T.C.
HATAY MUSTAFA KEMAL ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ
SİYASET BİLİMİ VE KAMU YÖNETİMİ ANA BİLİM DALI

ULUSAL VE ULUSLARARASI GÜVENLİK POLİTİKALARI TEMELİNDE DİJİTALLEŞME VE SİBER GÜVENLİK: HUKUKSAL VE YÖNETSEL BİR DEĞERLENDİRME

DOKTORA TEZİ

Hazırlayan
Mehmet Onur ÖZER

Tez Danışmanı
Prof. Dr. Mehmet Kahraman

Hatay – 2023

T.C.
HATAY MUSTAFA KEMAL ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ
SİYASET BİLİMİ VE KAMU YÖNETİMİ ANA BİLİM DALI

ULUSAL VE ULUSLARARASI GÜVENLİK POLİTİKALARI TEMELİNDE DİJİTALLEŞME VE SİBER GÜVENLİK: HUKUKSAL VE YÖNETSEL BİR DEĞERLENDİRME

DOKTORA TEZİ

Hazırlayan
Mehmet Onur ÖZER

Tez Danışmanı
Prof. Dr. Mehmet Kahraman

Hatay – 2023

ONAY

MEHMET ONUR ÖZER tarafından hazırlanan "***ULUSAL VE ULUSLARARASI GÜVENLİK POLİTİKALARI TEMELİNDE DİJİTALLEŞME VE SİBER GÜVENLİK: HUKUKSAL VE YÖNETSEL BİR DEĞERLENDİRME"*** adlı bu çalışma jüri tarafından lisansüstü öğretim yönetmeliğinin ilgili maddelerine göre değerlendirilip oybirliği / oyçokluğu ile ***SİYASET BİLİMİ KAMU YÖNETİMİ ANA BİLİM DALINDA DOKTORA TEZİ*** olarak kabul edilmiştir.

25/08/2023

Jüri Üyeleri	**İmza**
Prof. Dr. Mehmet KAHRAMAN (Tez Danışmanı – Başkan)	
Prof. Dr. Muharrem GÜNEŞ (Üye)	
Doç. Dr. Yıldız SAĞLAM ÇELİKÖZ (Üye)	
Dr. Öğretim Üyesi Ahmet BAĞRIAÇIK (Üye)	
Dr. Öğretim Üyesi Süleyman Emre ZORLU (Üye)	

Mehmet Onur ÖZER tarafından hazırlanan ***"Ulusal ve Uluslararası Güvenlik Politikaları Temelinde Dijitalleşme ve Siber Güvenlik: Hukuksal ve Yönetsel Bir Değerlendirme"*** çalışmasının yukarıda imzaları bulunan jüri üyelerince kabul edildiğini **onaylarım.**

Enstitü Müdürü

Doç. Dr. Sinan ERDOĞAN

ÖN SÖZ

İçinde bulunduğumuz yüzyıl içerisinde yaşadığımız hayatın her alanında kullanılan teknoloji, özellikle geçtiğimiz son yirmi yıl içerisinde internet teknolojisinin kullanımının yaygınlaşmasıyla birlikte gündelik bir alışkanlık hatta bir ihtiyaç haline gelmiştir. Bankacılık işlemlerinin, ticaretin, alışverişin, fatura işlemlerinin ve hatta birçok bürokratik işlemin internet üzerinden gerçekleştirilebildiği günümüzde, bilgisayarların, telefonların ve hatta evimizde kullandığımız birçok elektronik sarf malzemesinin de aynı şekilde internet teknolojisi ile kontrol edilebilir hale gelmesi güvenlik anlamında farklı tehditleri ortaya çıkartmaktadır. Bu anlamda sadece bireyler değil aynı zamanda devletlerin de teknolojiyi oldukça yaygın bir şekilde kullanıyor olması ortaya çıkan bu farklı güvenlik tehditlerinin devlet temelli ele alınmasını elzem hale getirmiştir.

Gelişen bilgi teknolojisi ve bilgisayar sistemleri devletlerin ulusal ve uluslararası güvenlik politikalarının oluşturulmasında oldukça önemli bir etkiye sahiptir. Devlet temelli değerlendirildiğinde günümüzde bilişim teknolojisi sadece kamu hizmetleri bağlamında e-devlet uygulamalarıyla sınırlı değildir. Devletlerin silahlı kuvvetlerinin kullandığı ileri teknoloji savunma sistemleri, elektrik ve su dağıtım şebekeleri, hava trafiği, barajlar, nükleer tesisler, demir yolu trafiği, bankacılık hizmetleri, finans sektörü ve enerji transferi gibi kritik altyapıların kontrolünün çok büyük bir kısmı otomatikleştirilmiş bilgisayar sistemlerinden oluşan merkezi denetleme kontrol ve veri toplama sistemleri aracılığıyla sağlanmaktadır. Bu noktada bu sistemlere dışarıdan yapılacak bir siber saldırı sadece devletlerin kritik altyapılarının çalışmasını engelleyerek güvenlik zafiyetleri oluşturup ekonomik kayıplara neden olmakla kalmayacak, aynı zamanda fiziki olarak da oldukça ciddi sonuçlar doğurabilecektir. Bu anlamda devletler bu tarz saldırıların önlenmesi amacıyla farklı önlemler alarak değişen güvenlik anlayışına ayak uydurmaya çalışmaktadır.

Bilişim teknolojilerinin bu denli gelişmesi ve internet ile daha çok cihazın birbiriyle bağlantılı hale gelerek sınırları ortadan kaldıran bir ağın ortaya çıkması mevcut fiziki alanlara ek olarak insan eliyle üretilmiş ve “Siber Uzay” olarak

adlandırılan dijital/sanal bir ortamın ortaya çıkmasını sağlamıştır. Siber uzayın durdurulamayan gelişimi ve önüne geçilemez etkisi devletler, kurumlar ve uluslararası örgütler tarafından 2000'li yıllar itibari ile tanınmış ve uluslararası ilişkilerin önemli aktörlerinin politika belirleyicileri tarafından bu alanın güvenliğinin sağlanması kritik ve öncelikli konular arasında yer almıştır.

Türkiye siber uzayın ve bu alanın güvenliğinin sağlanmasının önemini erken fark eden ve bu anlamda yasal düzenlemeler yapan ülkelerden bir tanesidir. İlk defa 1990'lı yılların başında Türk Ceza Kanunu'nda yapılan değişikliklerle siber uzayda gerçekleşebilecek tehditlere karşı önlem alınmış ve daha sonra özellikle 2000'li yıllarda gerek yasal gerekse yönetsel anlamda yapılan düzenlemelerle siber güvenliğin sağlanması ve siber uzayda caydırıcılığın kazanılması adına daha somut ve ciddi adımlar atılmaya başlanmıştır.

Bu çalışmada siber uzayın atarak devam eden kullanımı ile ortaya çıkan güvenlik tehditlerinin ulusal ve uluslararası temelde belirlenerek bu tehditlerin güvenlik politikalarına gerek kavramsal gerekse uygulama alanında yansımaları derinlemesine incelenmiştir. Ayrıca Türkiye'nin siber uzayda karşılaşabileceği tehditlere karşı gerek yasal zeminde gerekse de uygulamada izlemesi gereken yolun belirlenmesinde katkıda bulunmak amaçlanmıştır. Son olarak siber uzayın hukuksal ve yönetsel olarak nasıl düzenlendiği ve bu konuda ortaya çıkan temel sorunlar incelenmiştir. Bu bağlamda dünyada ve Türkiye'de konuyla ilgili yapılmış akademik çalışmalar ulusal güvenlik teorileri, uluslararası ilişkiler teorileri, yasal düzenlemeler, devletlerin ve kurumların yapmış olduğu çalışmalar, almış olduğu önlemler ve belirledikleri politikalar siber uzayda yaşanan somut olaylar çerçevesinde incelenerek ülkemizde yeni bir çalışma alanı olan siber güvenlik konusuna akademik olarak bir katkı sağlamak amaçlanmıştır.

Doktora çalışmam boyunca beni her konuda destekleyen, cesaretlendiren ve güvenen yol arkadaşım Melissa Meryem Özer'e hakkını hiçbir zaman ödeyemem. Ayrıca bu süreçte her aşamada yanımda bulunan, tecrübeleriyle yolumu aydınlatan ve cesaretlendiren değerli hocam ve ağabeyim Prof. Dr. Muharrem Güneş'e teşekkürü bir borç bilirim. Son olarak tez çalışmam boyunca beni her konuda destekleyen, anlayışını esirgemeyen, yaptığım her çalışmada sonsuz güven duygusunu hissettirerek beni cesaretlendiren ve teşvik eden, tecrübelerinden her daim faydalandığım ve

faydalanmaya devam edeceğim kıymetli hocam ve tez danışmanım Prof. Dr. Mehmet Kahraman'a şükranlarımı sunmayı bir borç bilirim. Kendisinin desteği ve güveni bu çalışmanın tamamlanmasındaki başat aktördür.

ULUSAL VE ULUSLARARASI GÜVENLİK POLİTİKALARI TEMELİNDE DİJİTALLEŞME VE SİBER GÜVENLİK: HUKUKSAL VE YÖNETSEL BİR DEĞERLENDİRME

Mehmet Onur ÖZER
Siyaset Bilimi ve Kamu Yönetimi Ana Bilim Dalı, Doktora Tezi, 2023
Danışman: Prof. Dr. Mehmet KAHRAMAN

ÖZET

Bilgi ve iletişim teknolojilerinin tahminlerin çok uzağında gelişmesi ve kullanım alanının yaygınlaşması ile yaşanan dijital dönüşüm gerçek hayatın normal akışı içerisindeki birçok alanda değişimlerin yaşanmasına neden olmuştur. Dijitalleşmenin yaygınlaşması ile ortaya çıkan siber uzay, sadece teknolojinin bileşenlerini barındıran bir kavram olmaktan çıkarak kara, hava, deniz ve uzaydan sonra beşinci muharebe alanı olarak kabul edilmiştir. Tamamen insan eliyle üretilmiş olan ve coğrafi olarak sınırları bulunmayan bu yeni alan beraberinde kendisine özgü, karmaşık ve sonuçları tahmin edilemeyecek boyutlara ulaşabilen tehditleri de getirmiştir.

Akıllı telefon teknolojisi ve internet kullanımının yaygınlaşması bilgisayar teknolojisini hemen her an bireylerin yanında taşıyabildiği bir boyuta dönüştürmüş ve sadece bireylerin birbirleri arasındaki ilişkilerini değil aynı zamanda devletle olan ilişkilerini de büyük bir dönüşüme uğratmıştır. Özellikle e-devlet uygulamalarının kullanım alanının artması vatandaşlar ve devlet ile olan ilişkileri de dijital bir hale dönüştürmüştür. Verilerin büyük oranda dijital ortamlarda işlenerek saklandığı, kamu kurumlarının iletişim ve veri akışlarını bilgi ve iletişim teknolojileri ile gerçekleştirdiği, kritik altyapıların ve üretim faaliyetlerinin bilgisayar teknolojileri ile kontrol edildiği ve ülkelerin savunma sistemlerinin yine aynı teknoloji üzerinden geliştirilerek kontrol edildiği günümüzde siber uzayda artan tehditler tüm bu yapıları risk altına sokmaya başlamıştır. Bu bağlamda ülkeler artık ulusal güvenlik

politikalarını belirlerken siber güvenlik politikalarının bir milli güvenlik meselesi olduğunun farkında olarak politika belirlemektedirler.

Türkiye, siber uzayın güvenliği konusunun erken farkına varan ülkelerden birisi olarak 1990'lı yılların başında siber uzayın düzenlenmesi adına yaptığı yasal düzenlemeler ve 2000'li yıllar itibari ile belirlediği politikalarla birlikte oluşturduğu kurumsal yapılanmalarla siber uzayın güvenliği konusunda çalışmalarını sürdürmektedir. Bu çalışma kapsamında siber güvenlik ve dijitalleşme kavramları teorik olarak irdelenecek ve Türkiye'nin bu alanın güvenliğinin sağlanması noktasında yaptığı yasal ve yönetsel düzenlemeler incelenerek siber uzaydaki mevcut durumu değerlendirilecektir.

ANAHTAR KELİMELER

Siber güvenlik, Siber Uzay, Dijitalleşme, Siber Tehdit, Siber Toplum, Siber Güvenlik Politikaları

DIGITALIZATION AND CYBERSECURITY BASED ON NATIONAL AND INTERNATIONAL SECURITY POLICIES: A LEGAL AND ADMINISTRATIVE ASSESSMENT

PhD Dissertation, Mehmet Onur ÖZER

Department of Political Science and Public Administration, 2023

Advisor: Prof. Dr. Mehmet KAHRAMAN

ABSTRACT

The rapid development and widespread use of information and communication technologies have led to significant changes in many aspects of everyday life, giving rise to digital transformation. The proliferation of digitalization has transformed the concept of cyberspace from simply encompassing the components of technology to being recognized as the fifth domain of warfare, following land, air, sea, and space. This newly created and geographically borderless realm, entirely constructed by humans, has brought about unique and complex threats with potentially unpredictable consequences.

The prevalence of smart phone technology and internet usage has transformed computer technology into a dimension that individuals can always carry with them, leading to a significant transformation in interpersonal relationships and interactions with the government. Particularly, the increasing use of e-government applications has digitized the relationships between citizens and the government. In today's world, where data is predominantly processed and stored in digital environments, public institutions communicate and manage data flow through information and communication technologies, critical infrastructures and production activities are controlled by computer technologies, and countries develop and control their defense systems through the same technology, the escalating threats in cyberspace have put all these structures at risk. Consequently, countries now recognize that formulating national security policies involves considering cyber security policies as matters of national security.

As one of the countries that early recognized the significance of cyber space security, Türkiye has been working on ensuring the security of cyberspace through legal regulations introduced in the early 1990s and the policies formulated since the 2000s. In this context, this study will theoretically analyze the concepts of cyber security and digitalization and evaluate the current state of cyberspace by examining the legal and administrative regulations implemented by Turkey to ensure the security of this domain.

KEY WORDS

Cyber Security, Cyber Space, Digital Transformation, Digitalization, Cyber Threat, Cyber Society, Cyber Security Policies

TÜRKİYE CUMHURİYETİ
HATAY MUSTAFA KEMAL ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ MÜDÜRLÜĞÜNE

Bu belge ile, bu tezde yer alan bilgilerin tamamının akademik kurallara ve etik ilkelerine uygun olarak toplanıp sunulduğunu beyan ederim. Söz konusu kural ve ilkelerin gereği olarak tezde yararlandığım eserlerin tamamına uygun bir şekilde atıfta bulunarak kaynak gösterdiğimi ayrıca beyan ederim. (25/08/2023)

Mehmet Onur ÖZER

İÇİNDEKİLER

İKİNCİ BÖLÜM

DİJİTALLEŞME İLE BİRLİKTE ORTAYA ÇIKAN YENİ GÜVENLİK ALGISI VE SİBER GÜVENLİK: TEORİK ÇERÇEVE

ÜÇÜNCÜ BÖLÜM

ULUSAL VE ULUSLARARASI BOYUTTA TÜRKİYE'DE DİJİTALLEŞME VE SİBER GÜVENLİK

DÖRDÜNCÜ BÖLÜM

TÜRKİYE'NİN SİBER GÜVENLİK ALANINDA YAPTIĞI ULUSLARARASI İŞ BİRLİKLERİ, ÇALIŞMALAR VE ANLAŞMALAR

TABLOLAR, ŞEKİLLER ve GRAFİKLER LİSTESİ

KISALTMALAR

AB : Avrupa Birliği

ABD : Amerika Birleşik Devletleri

AEP : Acil Eylem Planı

AK : Avrupa Komisyonu

AR : Artırılmış Gerçeklik (Augmented Reality)

AR-GE : Araştırma Geliştirme

ASELSAN : Askeri Elektronik Sanayi

ASSS : Avrupa Siber Suçlar Sözleşmesi

AYM : Anayasa Mahkemesi

BGYS : Bilgi Güvenliği yönetim Sistemi

BİLGEM : Bilişim ve Bilgi Güvenliği İleri Teknolojiler Araştırma Merkezi

BİT : Bilgi ve İletişim Teknolojileri

BK : Bakanlar Kurulu

BKK : Bakanlar Kurulu Kararı

BM : Birleşmiş Milletler

BTK : Bilgi Teknolojileri ve İletişim Kurumu

CCDCoE : NATO Müşterek Siber Savunma Mükemmeliyet Merkezi

CDDO : Cumhurbaşkanlığı Dijital Dönüşüm Ofisi

CIA : Amerikan Merkezi Haber Alma Ajansı

CMK : Ceza Muhakemesi Kanunu

ÇŞB : Çevre ve Şehircilik Bakanlığı

DHKP-C : Devrimci Halk Kurtuluş Partisi-Cephesi

DoD : Amerikan Savunma Bakanlığı (Department of Defense)

DPT : Devlet Planlama Teşkilatı

EGM : Emniyet Genel Müdürlüğü

FBI : Amerikan Federal Soruşturma Bürosu

FETÖ : Fettullahçı Terör Örgütü

FIRST : Siber Olaylara Müdahale Ekipleri Küresel Forumu

HAGB : Hükmün Açıklanmasının Geri Bırakılması

HAVELSAN : Hava Elektronik Sanayii

IoT : Nesnelerin İnterneti (Internet of the Things)

IP : Internet Protocol

IŞİD : Irak Şam İslam Devleti

JGK : Jandarma Genel Komutanlığı

KGM : Karayolları Genel Müdürlüğü

KHK : Kanun Hükmünde Kararname

KVKK : Kişisel Verilerin Korunması Kanunu

MC : Milletler Cemiyeti

Md. : Madde

MGK : Milli Güvenlik Kurulu

MİT : Millî İstihbarat Teşkilâtı

MÖ : Milattan Önce

NATO : Kuzey Atlantik Antlaşması Teşkilatı

NSA : Amerikan Ulusal Güvenlik Ajansı

ODTÜ : Orta Doğu Teknik Üniversitesi

SCADA : Merkezi Denetleme Kontrol ve Veri Toplama Sistemleri

SGE : Siber Güvenlik Enstitüsü

SMS : Kısa Mesaj

SSB : Savunma Sanayii Başkanlığı

SSCB : Sovyet Sosyalist Cumhuriyetler Birliği

SSİK : Savunma Sanayii İcra Komitesi

SSMDB : Siber Suçlarla Mücadele Daire Başkanlığı

SOME : Siber Olaylara Müdahale Ekibi

STM : Savunma Teknolojileri ve Ticaret A.Ş

TBMM : Türkiye Büyük Millet Meclisi

T.C. : Türkiye Cumhuriyeti

TCK : Türk Ceza Kanunu

TDK : Türk Dil Kurumu

TMK : Terörle Mücadele Kanunu

TSK : Türk Silahlı Kuvvetleri

TSKGV : Türk Silahlı Kuvvetlerini Güçlendirme Vakfı

TÜBİTAK : Türkiye Bilimsel ve Teknolojik Araştırmalar Kurumu

UAB : Ulaştırma ve Altyapı Bakanlığı

UDHB **:** Ulaştırma, Denizcilik ve Haberleşme Bakanlığı

UEKAE **:** Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü

URL **:** İnternet Alan Adı (Uniform Resource Locator)

USGS **:** Ulusal Siber Güvenlik Stratejisi

USOM **:** Ulusal Siber Olaylara Müdahale Merkezi

VPN **:** Sanal Özel Ağ (Virtual Private Network)

VR **:** Sanal Gerçeklik (Virtual Reality)

YÖK **:** Yüksek Öğretim Kurumu

YPG **:** Halk Koruma/Savunma Birlikler

GİRİŞ

Teknolojinin günümüzde geldiği nokta her ne kadar 1980'li yıllarda Geleceğe Dönüş filminde gösterildiği şekliyle uçan arabaların yaygın bir şekilde kullanıldığı seviyeye gelmemiş olsa da bilgisayar ve internet teknolojisi ilk kullanılmaya başlandığı günden bu yana tahmin edilemeyen boyutlara ulaşmıştır. Bilgisayarların, arabaların, küçük ev aletlerinin, insanların ve hatta devletlerin birbirlerine görünmez ağlarla bağlandığı günümüzde teknoloji, insan ilişkilerinden diplomasiye kadar geleneksel yapıyı dönüştüren bir etken haline gelmiştir. Tamamen insan elliyle üretilmiş, bilgisayarların, fiber optik kabloların, internetin, işletim sistemlerinin, akıllı cep telefonlarının ve her türlü teknolojik bileşenin oluşturduğu siber uzay, teknolojinin her bir bileşeninin dahil olduğu ve fiziki olarak sınırları olmayan yeni bir alan olarak gerçek hayatın bir parçası haline gelmiştir. İnternet bağlantısının olduğu her yer siber uzayda gerçekleştirilebilecek her türlü işlem için gereken ortamı sağlayabilecek kapasiteye sahiptir. Bu işlem kıtalararası bir telefon görüşmesi, bankalar arası para transferi, herhangi bir belgenin gönderilmesi veya alınması, fatura ödemesi, alışveriş, vergi bildirimi ya da uzaktan eğitimle anlatılan bir derse katılım sağlamak gibi işlem ve eylemler olabileceği gibi, bir ülkenin teknolojik altyapısına yapılacak bir saldırı, terör örgütlerinin yapacağı bir eylemin planlaması ve örgüt üyeleri arasında iletişimin sağlanması, bir ülkenin kritik altyapılarını kontrol eden bilgi ve iletişim sistemlerine yapılacak bir siber saldırı ya da bir bankanın sistemlerinin kontrolünün ele geçirilmesi ile haksız kazanç sağlama işlem ya da eylemleri de olabilmektedir. Dolayısıyla siber uzay, teknolojinin getirdiği imkanlarla sadece hayatı kolaylaştıran bir alan değil aynı zamanda yeni tehditlerin ortaya çıktığı ve bu tehditlerin sonucunda ortaya çıkabilecek sonuçlar itibari ile gerçek hayattan ayrılan karmaşık bir alan olarak karşımıza çıkmaktadır.

Teknolojinin hayatın hemen her alanına dokunduğu ve dönüştürdüğü günümüzde özellikle akıllı telefon ve internet teknolojisinin kullanımının yaygınlaşması, insanların hemen her yerde mobil ağlarla internete erişiminin bulunması ve gerçek hayattaki birçok şeyin teknoloji ile dijitalleşmesi sonucunda

geleneksel olan birçok kavram dönüşüme uğramıştır. Covid19 pandemisi ile ortaya çıkan yeni düzende tüm dünya siber uzayın en önemli bileşeni olan internet aracılığı ile birbirine bağlanmış ve zaten birçok şeyin dijitalleştiği dünyada insan ilişkileri, devletlerarası ilişkiler, eğitim, alışveriş, çalışma hayatı gibi birçok şey uzaktan ve internet aracılığı ile yapılır hale gelmiştir. Covid19 pandemisi gerçek hayatta yapılan birçok şeyin siber uzayda da gerçekleştirilebileceğini ispatlayan bir süreç olmuştur. "Siber" olgusu gelinen noktada artık bir sıfat görevi görmeye başlamış ve birçok kavramın önüne gelerek tanımlayıcı bir kavram haline dönüşmüştür. Siber uzay, siber diplomasi, siber teknoloji, siber terörizm, siber savunma, siber saldırı, siber dolandırıcılık, siber suç ve siber toplum gibi kavramlar hayatımıza girmekle kalmamış aynı zamanda günlük hayatın bir parçası haline de dönüşmüştür.

İnternet kullanımının oldukça yaygın hale gelmesi, bilgi ve iletişim teknolojilerinin internet teknolojisiyle bütünleşik olarak gelişmesi günlük hayatın rutini olan birçok iş ve işlemin internet üzerinden çok daha hızlı ve kolay bir şekilde gerçekleştirilmesine olanak sağlamaktadır. Gelinen noktada artık faturalar internet üzerinden ödenebilmekte, market alışverişi de dahil olmak üzere insanların ihtiyaç duyduğu hemen her şey internet üzerinden yapılan alışverişle temin edilebilmekte, e-devlet uygulamalarıyla birçok resmi işlem kurumlara gitmeden uzaktan halledilebilmekte, öğrenciler uzaktan eğitim uygulamalarıyla okula gitmeden eğitim hayatlarını sürdürebilmekte, insanlar sosyal medya platformları üzerinden tanışarak yeni ilişkiler ve bağlantılar kurabilmekte ve görüntülü arama teknolojisi ile hemen her yerde mesafe kavramı olmadan iletişim kurulabilmektedir. Artık evden çalışma denilen kavramın oldukça yaygınlaştığı günümüzde birçok işin fiziki bir çalışma ortamına gerek kalmadan halledilebildiği de bir gerçektir. Tüm bunların yanında üretim tesislerinin bilgi ve iletişim teknolojilerini üretim süreçlerine dahil etmesiyle daha verimli ve hızlı bir üretim sürecinin gerçekleştiği yeni bir sanayi sistemi de artık günümüzün bir gerçeği haline dönüşmüştür. Bu bağlamda internet üzerinden yapılan alışverişle insanların tüketim alışkanlıkları değiştiği gibi aynı zamanda üretim de dijital bir dönüşümle bambaşka bir boyuta ulaşmıştır. Büyük sanayi kuruluşları üretim süreçlerini artık geleneksel yöntemlerin dışında dijital bir hale dönüştürerek rekabet güçlerini artırmaya başlamış ve üretim süreçlerini bu sistemlerle çok daha verimli ve hızlı bir hale dönüştürmüştür.

Siber uzay sadece insanlar arasındaki ilişkileri, tüketim ve üretim alışkanlıklarını dönüştürmekle kalmamış aynı zamanda devletlerin teknolojiyi aktif olarak kullanmaya başlamalarıyla birlikte bürokrasiyi, siyaseti, savunmayı, diplomasiyi ve kamu politikalarını da büyük bir dönüşüme uğratmıştır. Birçok devletin aktif olarak kullandığı e-devlet uygulamaları ile devlet ve vatandaşları arasındaki ilişkilerin de dijitalleştiğini söylemek mümkündür. Artık vatandaşlar daha önce kamu kurumları ile olan ilişkilerinde fiziksel olarak kurumlara giderek hallettikleri iş ve işlemleri günümüzde e-devlet uygulamalarıyla bürokrasinin herhangi bir bileşeniyle etkileşime girmek zorunda kalmadan bilgisayar ya da akıllı telefonlarından halledebilir konuma gelmiştir. Siyasiler artık seçmenlere düzenledikleri mitingler aracılığıyla değil, sosyal medya platformları üzerinden ulaşmaya başlamışlardır. Dakikalar içerisinde oldukça büyük kitlelere ulaşabilme gücüne sahip olan sosyal medya kullanımı siyasetin de şeklini değiştirmiştir. Ülkeler artık siber uzayın güvenliğinin sağlanmasını bir ulusal güvenlik meselesi olarak kabul etmekle beraber ulusal güvenliğin tam olarak sağlanmasının ancak siber uzayda güvenliğin sağlanması ile gerçekleşebileceği gerçeğinin de farkına varmışlardır. Ülkelerin kullandığı ileri teknoloji savunma ve saldırı sistemlerinin büyük çoğunluğunun bilgi ve iletişim teknolojileriyle kontrol edildiği düşünüldüğünde bu alanın güvenliğini sağlıyor olmak bir ülkenin tüm savunma ve saldırı sisteminin güvenliğini sağlıyor olmak anlamına gelmektedir. Uluslararası ilişkilerde de geleneksel diplomasi yöntemlerini dönüştüren siber uzay, devletlerarası ilişkilerde önemli bir rol oynamaya başlamıştır. Toplumların dijitalleşmeye başlaması ile yaşam alanlarının da teknoloji ile bütünleşmesi, dünya nüfusunun büyük çoğunluğunun yaşadığı kentlerin de dijitalleşmesine neden olmuştur. Daha verimli, daha interaktif ve daha sürdürülebilir bir yönetim anlayışı çerçevesinde bilgi ve iletişim teknolojilerinin aktif olarak kullanıldığı akıllı kentler, kent yaşamını da değişime uğratmaktadır.

Siber uzayın bu kadar geniş bir yelpazede hayatın her alanına dokunması, bilgisayar ve internet teknolojilerinin kullanım oranlarının artması ve bilgi paylaşımının artık büyük oranda dijital ortamlarda gerçekleşiyor olması ise beraberinde yeni güvenlik tehditlerini de getirmiştir. Siber uzayda ortaya çıkan bu tehditler, münferit olarak bireyleri kişisel verilerin güvenliği başta olmak üzere birçok konuda risk altına sokuyor olmasının yanında siber uzayda ülkelerin kritik

altyapılarının işletim sistemlerine yapılacak bir siber saldırı olasılığı ile de aynı zamanda devletlerin ulusal güvenliğini de etkileyen bir unsur haline dönüşmüştür. Dolayısıyla bu bağlamda güvenlik kavramı da önemli bir dönüşümün içerisine girmiştir. Özellikle siber uzayın kara, hava, deniz ve uzaydan sonra beşinci muharebe alanı olarak kabul edilmesiyle birlikte güvenlik kavramı farklı bir boyut kazanmıştır. Artık devletler ve uluslararası örgütler insan eliyle üretilmiş bu yeni alanın güvenliğinin sağlanmasının ne kadar önemli olduğunun farkında olarak güvenlik politikaları üretmektedirler.

Türkiye siber uzayın güvenliği konusunun önemini erken fark eden ülkelerden birisidir. 1990'lı yılların başında, henüz bilgisayar teknolojisinin kullanımının oldukça düşük olduğu yıllarda, Türk Ceza Kanunu'nda yaptığı değişikliklerle siber uzayın yasal olarak düzenlenmesi adına ilk adımı atan Türkiye, geldiğimiz noktada birçok yasal düzenleme ve kurumsal yapılanmayla bu alanda güvenliğin sağlanması adına çalışmalar yürütmektedir. Siber uzayda güvenliğin sağlanması konusunun öneminin farkında olarak bu çalışma kapsamında Türkiye'de bu alanın güvenliğinin sağlanması adına yapılan yasal düzenlemeler ve yönetsel bağlamda oluşturulan kurumsal yapılanmalar detaylı bir şeklide incelenerek Türkiye'nin siber güvenlik alanında bugüne kadar yaptığı yasal düzenlemeler, oluşturduğu kurumlar ve bu kurumların siber uzayın güvenliği noktasında görev ve sorumlulukları irdelenmiştir. Ayrıca, siber uzay ve bu alanı oluşturan bileşenler ve bu alanda ortaya çıkan yeni tehdit algılamaları değişen güvenlik anlayışı çerçevesinde incelenerek değerlendirilmiştir. Fiziki olarak sınırları bulunmayan siber uzayın teorik olarak incelenmesinde uluslararası ilişkiler teorileriyle birlikte siyaset felsefesinin temelini oluşturan toplum sözleşmesi teorilerinden faydalanılmıştır.

Bu çalışmada siber uzayın atarak devam eden kullanımı ile ortaya çıkan güvenlik tehditlerinin ulusal ve uluslararası temelde belirlenerek bu tehditlerin güvenlik politikalarına gerek kavramsal gerekse uygulama alanında yansımalarını derinlemesine incelemek ve Türkiye'nin siber uzayda karşılaşabileceği tehditlere karşı gerek yasal zeminde gerekse de uygulamada izlemesi gereken yolun belirlenmesinde katkıda bulunmak amaçlanmıştır. Siber uzayın hukuksal ve yönetsel olarak nasıl düzenlendiği ve bu konuda ortaya çıkan temel sorunlar incelenerek bu bağlamda dünyada ve Türkiye'de konuyla ilgili yapılmış akademik çalışmalar ulusal güvenlik

teorileri, uluslararası ilişkiler teorileri, yasal düzenlemeler, devletlerin ve kurumların yapmış olduğu çalışmalar, almış olduğu önlemler ve belirledikleri politikalar siber uzayda yaşanan somut olaylar çerçevesinde incelenerek ülkemizde yeni bir çalışma alanı olan siber güvenlik konusuna akademik olarak bir katkı sağlamak bu çalışmanın bir diğer amacıdır. Konunun ulusal güvenlik anlamında önemi göz önünde bulundurulduğunda, bu çalışmanın sadece kapsamlı bir doktora tez araştırması olarak akademik alan yazınına katkı sağlamasının yanında aynı zamanda siber güvenlik bağlamında ulusal güvenlik politikalarının belirlenmesinde de yol gösterici bir çalışma olacağına olan inanç bu konunun seçilmesinin ana sebebidir.

Bu tez kapsamında "Siber uzay ve bileşenleri nelerdir? Siber uzayda güvenliğin sağlanması neden önemlidir? Ulusal ve uluslararası alanda Türkiye siber güvenlik ve dijitalleşme bağlamında neredeedir? Siber uzayın ortaya çıkardığı ulusal ve uluslararası güvenlik tehditleri nelerdir? Siber uzayın güvenliğinin sağlanması için atılması gereken adımlar, izlenmesi gereken politikalar nelerdir? Siber uzayın yasal olarak düzenlenmesi mümkün müdür?" sorularına cevap aranmıştır. Bu çalışmanın hipotezi ise "*Türkiye'de ulusal güvenliğin sağlanmasında siber uzay ve bileşenlerini hukuksal zeminde kontrol eden yasal düzenlemeler ve yönetsel zeminde kontrol eden kurumsal oluşumlar gerek ulusal gerekse uluslararası düzeyde yetersizdir."* temelinde oluşturulmuştur. Bu çalışmada nitel araştırma yaklaşımı çerçevesinde araştırma sorularının cevaplanması adına doküman incelemesi yöntemi kapsamında yerli ve yabancı yazının irdelenmesine ek olarak konuyla ilgili yasal ve yönetsel düzenlemeler bağlamında mevzuat incelemesi yapılmış ve teorik bir araştırma mantığında konuyla ilgili incelenen çalışmaların mantıksal bir çözümlemesi yapılmaya çalışılmıştır.

Bu çalışma dört bölümde incelenmiştir. Çalışmanın ilk bölümünde siber güvenlik kavramıyla ilgili olarak temel kavramlar, siber güvenliğin sağlanmasında karşılaşılan zorluklar, siber tehditler ve saldırı yöntemleri, siber suç, siber terörizm, siber savunma ve siber caydırıcılık kavramları derinlemesine incelenerek somut örnekler verilerek bu kavramlar açıklanmıştır. Siber uzay konusunun karmaşıklığı göz önünde bulundurularak konuyla ilgili terimlerin ve yaklaşımların birinci bölümde incelenmesi, siber güvenlik konusunun anlaşılması ve incelenen çalışma ve belgelerin mantıklı bir çözümlemesinin yapılabilmesi adına gerekli görülmüştür.

Çalışmanın ikinci bölümünde güvenlik kavramının dönüşümü ve açıklanması teorik olarak incelenmiş ve bu bağlamda siber güvenlik kavramının teorik altyapısı oluşturulmaya çalışılmıştır. Sınırları aşan, zamandan ve mekândan bağımsız olan siber uzayın güvenliği konusunun açıklanmasında bu bağlamda uluslararası ilişkiler teorilerinden ve aynı zamanda siyaset felsefesinin temelini oluşturan toplumsal sözleşme teorilerinden istifade edilmiştir. İdealizm, liberalizm, realizm ve neo-realizm temelinde ortaya koyulan güvenlik çalışmaları, siber uzayla birlikte ortaya çıkan siber güvenlik kavramıyla ilişkilendirilerek mantıksal bir çerçeve oluşturulmaya çalışılmıştır. Ayrıca dijitalleşme ile değişime uğrayan toplumsal yapı ve siber toplum kavramı açıklanarak toplumsal sözleşme teorileri kapsamında yeni bir "Siber Toplum Sözleşmesi" oluşturulmaya çalışılmıştır.

Çalışmanın üçüncü bölümünde Türkiye'de siber uzayın düzenlenmesi adına yapılan yasal düzenlemeler detaylı bir şekilde incelenmiştir. Bu kapsamda sadece kanunlarda siber uzayın güvenliğinin sağlanması adına yapılan düzenlemeler değil aynı zamanda kararlar, genelgeler, tebliğler, raporlar ve uluslararası anlaşmalar da incelenerek bir çözümleme yapılmıştır. Ayrıca Türkiye'nin siber güvenlik politikalarının belirlenmesinde önemli rol oynayan ve ilk defa 2013 yılında hazırlanan Ulusal Siber Güvenlik Stratejisi ve Eylem Planı belgeleri de detaylı bir şekilde incelenerek değerlendirilmiştir.

Tezin son bölümünde ise Türkiye'de siber güvenlik alanında oluşturulan kurumsal yapılanmalar, bu yapılanmaların görev ve sorumlulukları, siber güvenliğin sağlanmasında gerçekleştirdikleri faaliyetler ve ortaya koydukları projeler incelenmiştir. Türkiye'nin siber güvenlik anlamında oluşturduğu kurumsal yapılanma düzenleyici kurumlar, siber suçlarla mücadele eden kurumlar, ulusal siber güvenliğin sağlanmasında hizmet veren kurumlar ve siber güvenliğin sağlanmasında teknoloji geliştiren kurumlar olarak dört başlık altında incelenmiştir.

Çalışmanın sonuç kısmında ise incelenen yasal ve yönetsel düzenlemeler kapsamında Türkiye'de siber uzayın güvenliğinin sağlanması konusunda değerlendirmeler yapılmış ve bu alanın güvenliğinin sağlanması adına yapılan bu değerlendirmeler ışığında politika önerilerine yer verilmiştir. Ulusal güvenliğin tam anlamıyla sağlanabilmesi adına siber güvenliğin temin edilmesinin bir zorunluluk

olduğu gerçeği çerçevesinde yapılan değerlendirmeler ve önerilerin yol gösterici olması temenni edilmektedir.

BİRİNCİ BÖLÜM

TEMEL KAVRAMLAR VE YAKLAŞIMLAR ÇERÇEVESİNDE SİBER GÜVENLİK VE DİJİTALLEŞME

Güvenlik kavramı ve algısı geçmişten bugüne insanoğlunun yaşadığı çağın sosyal, ekonomik ve siyasal ortamının şartlarına göre farklılık göstermiş ve değişime uğramıştır. İlk kentlerin ortaya çıkmasından önce insanoğlunun doğadaki yaşamında doğal afetlerden ve yırtıcı hayvanlardan korunma temelinde oluşan güvenlik algısı, insanların bir arada yaşama eğilimi ile ortaya çıkan ilk insan toplulukları ve ilk kentlerin ortaya çıkmasıyla birlikte doğayla mücadele temelinden insanların birbirleriyle olan ilişkileri temeline evrilmiştir.

Güvenlik kavramı sosyal bilimler alanında diğer birçok kavramda olduğu gibi üzerinde anlaşma sağlanamamış tartışmalı kavramlardan birisidir. Güvenlik kavramı ile ilgili yapılan araştırmaların tek bir çatı altında toplandıkları nokta güvenliğin gerek bireysel gerekse toplumsal anlamda temel değerlere gelecek tehditlerden özgür olunması anlamında olduğudur. Güvenlik kavramı ile ilgili yapılan araştırmaların ayrıştığı nokta ise hangi temelde yapılması gerektiği sorunsalıdır. Ulusal, uluslararası ya da bireysel ölçeklerden hangisinin temel alınacağı, kavramla ilgili yapılan çalışmaların temel ayrışma noktası olarak karşımıza çıkmaktadır (Baylis, 2008: 73-74).

Dünyanın farklı coğrafyalarında insan topluluklarının farklı nedenlerle birbirleriyle olan mücadelesi ilk devletlerin ortaya çıkması ile devletlerarası bir mücadeleye dönüşmüş ve güvenlik olgusu çok daha geniş bir kapsamda ele alınmaya başlanmıştır. Ulus devletlerin tarih sahnesine çıkması ise güvenlik kavramını ulusal ve uluslararası düzeyde önem arz eden bir gerçeklik haline dönüştürmüştür. Dönemin siyasal ve ekonomik şartları ve ortaya çıkardığı etkiler ise güvenlik anlayışında anlamsal farklılıkların ortaya çıkmasına neden olmuştur. Bu anlamda güvenlik Birinci ve İkinci Dünya Savaşından sonra ülkelerin birbirlerine karşı sağladığı askeri tehdit

bağlamında ulusal güvenlik olarak, Soğuk Savaş döneminde ülkelerin birbirleriyle olan ilişkileri, stratejik dengeler ve nükleer caydırıcılık olarak, 2001'de gerçekleşen 11 Eylül saldırılarından sonra ise terörle mücadele şeklinde algılanmıştır (Booth, 2007: 185). Teknolojinin devletlerin ulusal ve uluslararası temelde güvenliklerinin sağlanmasında ne kadar önemli olduğu yirminci yüzyılda yaşanan iki dünya savaşı ve Amerika Birleşik Devletleri ile Sovyetler arasında uzun yıllar boyunca devam eden Soğuk Savaş döneminde daha da iyi anlaşılmıştır. Teknolojik olarak üstünlüğün geleneksel anlamda insan gücüne sahip olmaktan çok daha önemli olduğu bu süreçlerle ispatlanmıştır (Nye, 2011a).

İçinde bulunduğumuz 21. yüzyılda teknoloji, internet teknolojisinin kullanımının yaygınlaşmasıyla birlikte günlük yaşamın vazgeçilmez bir parçası haline geldiği söylenebilir. Bankacılık işlemlerinin, ticaretin ve alışverişin internet üzerinden kontrol edilebildiği günümüzde, bilgisayarların, telefonların ve hatta evimizde kullandığımız birçok elektronik sarf malzemesinin de aynı şekilde internet teknolojisi ile kontrol edilebilir hale gelmesi güvenlik anlamında farklı tehditleri ortaya çıkarmaktadır. Bu anlamda sadece bireyler değil aynı zamanda devletlerin de teknolojiyi oldukça yaygın bir şekilde kullanıyor olması ortaya çıkan bu farklı güvenlik tehditlerinin devlet temelli olarak da ele alınmasını gerekli hale getirmiştir.

Bilişim teknolojilerinin hemen her alanda oldukça sıklıkla kullanılmaya başlanmasıyla yeni ve sanal bir alan olan "*siber uzay*" ya da "*siber alan*" olarak adlandırılan dijital bir ortam ortaya çıkmıştır. Bu alanın güvenliğinin sağlanması ise son yıllarda devletlerin ve teknoloji geliştiren özel şirketlerin önceliği haline dönüşmüştür. İnsan eliyle üretilmiş bu yeni dijital ortamın hayatın her alanına nüfuz etmesiyle birlikte gerek birey gerekse devlet seviyesinde bu alanın kullanımı durdurulamaz ve aynı zamanda vazgeçilemez bir hal almıştır.

Bireylerin hayatın her noktasında teknolojiyi kullanır hale gelmesi ve devletlerin teknolojiyle birlikte birçok bürokratik hizmeti dijital olarak sunabilmesine ek olarak diğer birçok alanda teknolojiye ayak uydurarak dijitalleşmeye gitmesi, bu yeni alanda farklı güvenlik tehditlerinin ortaya çıkmasına neden olmuştur. Siber güvenlik denilen olgu ise bu tehditlerin artmasıyla birlikte ortaya çıkan ve özellikle devletler için henüz oldukça yeni ve anlaşılması oldukça karmaşık olan siber uzayda

güvenliğin tesis edilmesi adına dijitalleşmeye ayak uydurmanın bir tezahürü şeklinde ortaya çıkmıştır.

1. DİJİTALLEŞME, SİBER GÜVENLİK VE BİLEŞENLERİ

1.1. Dijitalleşme

Dijitalleşme kavramı bilgi ve iletişim teknolojilerinin kullanımının yaygınlaşmaya başlaması ve bu teknolojilerin özellikle gerek kamu sektöründe gerekse de özel sektörde mevcut sistemlere entegre edilmeye başlamasıyla ortaya çıkan yeni bir olgudur. Dijitalleşme, kurum veya kuruluşların ya da toplumların iş ve işleyişleriyle etkileşimlerinin bilgi ve iletişim teknolojileri kullanarak verimliliğini en üst seviyeye çıkartmayı amaçlayan bir kavramdır. Böylece mevcut verilerin analizi ile iş süreçlerinin bir otomasyon çerçevesinde gerçekleştirilmesi, iletişim ve iş birliği, dijital pazarlama, müşteri deneyimi geliştirme gibi alanlarda yenilikçi çözümler sunulması amaçlanmaktadır. Dijitalleşme ile kurum ve kuruluşlar küreselleşen dünyada rekabet güçlerini artırmayı hedeflemektedirler. Burada üzerinde durulması gereken bir diğer konu ise "dijitalleşme" ve "dijitalleştirme" kavramları arasındaki farktır. Dijitalleşme daha çok bilgi ve iletişim teknolojileri kullanarak mevcut süreçlerin verimliliğini artırma üzerine kullanılan bir terimdir. Dijitalleştirme ise var olan analog sistemlerin dijital teknolojilerle yer değiştirmesi anlamında kullanılmaktadır (Kneuer ve Milner, 2019: 7-10).

Dijitalleşme, fiziksel ortamlarda gerçekleşen iş süreçlerini dijital ortamlara taşır ve bu süreçleri daha hızlı, daha verimli ve daha etkili hale getirir. Örneğin, kâğıt tabanlı belgelerin dijital ortamda saklanması ve paylaşılması, iş süreçlerinin otomatikleştirilmesi ve veri analiziyle iş kararlarının daha iyi bilgiye dayalı olarak alınması dijitalleşmenin bir parçasıdır. Dijitalleşme, kurum, kuruluş ve toplumların rekabet gücünü artırmak gerek kamu sektöründe gerekse de özel sektörde müşteri taleplerine hızlı ve çözüm odaklı yanıt verebilmek, iş süreçlerinin verimliliğini artırmak ve yeni iş modelleri oluşturmak gibi birçok avantajı beraberinde getirmektedir. Ayrıca dijitalleşme, savunma, eğitim, sağlık, ulaşım, iletişim gibi birçok sektörde de iş ve işlemlerin yürütülmesi anlamında getirdiği yeniliklerle bu sektörlerde

çalışanlar ve hizmet alanlar bağlamında memnuniyet seviyesini artırmaktadır (Samoilenko, 2022: 6-7).

Dijitalleşme kavramı günümüzde hayatın her alanına sirayet eden bir gerçeklik haline dönüşmüştür. Devletlerin her alanda teknolojiyi kullanmaya başlamasıyla birlikte devlet seviyesinde dijitalleşme birçok alanda kendisini göstermeye başlamıştır. Özellikle bilişim teknolojilerinin devletlerin vatandaşlarına vermiş oldukları kamu hizmetlerinde getirdiği kolaylıklar dijitalleşmeye hız kazandırmıştır. Devlet seviyesinde dijitalleşme, bir ülkenin kamu hizmetlerini daha verimli, etkin ve erişilebilir hale getirmek için dijital teknolojilerin kullanımını içeren bir süreçtir. Devletler, dijitalleşmeyle birlikte vatandaşlara daha iyi hizmet sunmayı, kamu kaynaklarını etkin bir şekilde kullanmayı ve karar alma süreçlerini iyileştirmeyi hedeflemektedirler. Devletlerin kamu hizmetlerinde kullanmaya başladıkları e-devlet uygulamaları, kamu hizmetlerinin dijital ortamlarda sunulması ve vatandaşların bu hizmetlere mobil telefonları ya da bilgisayarları aracılığıyla erişmesini sağlamaktadır. Örneğin, vergilerin internet üzerinden kolayca ödenebilmesi, araç tescil ve plaka işlemlerinin ya da abonelik işlemlerinin e-devlet üzerinden yapılabilmesi, kamu hizmetlerine erişim, elektronik oy kullanma gibi uygulamalar devlet seviyesinde dijitalleşmenin bir parçası olarak kabul edilebilir. Ayrıca kamu kurum ve kuruluşlarının dijitalleşmesi ile bu kuruluşlar arasında veri paylaşımı sağlanarak bilgi akışı ve iletişim daha etkili, daha verimli ve kolay bir hale gelmektedir. Bu sayede kamu kurum ve kuruluşlarında yapılan her türlü iş ve işleme ait bilgiler ilgili diğer kurum ve kuruluşların da entegre olduğu sistem içerisinde saklanmakta ve benzer işlemler için bir başka kurumda yeniden bilgi girişi ya da belge ihtiyacı büyük oranda önlenebilmektedir. Bu durum özellikle kamu kurum ve kuruluşlarında belgelerin düzenlenmesi veya veri girişi işlemlerinde harcanan zaman konusunda önemli bir avantaj sağlamaktadır.

Bunun yanında devletler, dijitalleşme ile yüksek hızlı internet erişimi ve fiber optik ağlar gibi altyapıları ülkelerinde geliştirmektedirler. Bu sayede vatandaşlar ve kurumlar arasında hızlı iletişim ve veri transferi sağlanması hedeflenmektedir. Ayrıca kamu kurumları, dijital ortamlarda verdiği hizmetlerden elde ettiği verilerin analizini gerçekleştirerek karar alma süreçlerini iyileştirmekte ve hizmetlerin kişiselleştirilmesini sağlayabilmektedirler. Devlet seviyesinde dijitalleşme,

hükümetlerin vatandaşların ihtiyaçlarına daha iyi yanıt vermesini, hizmet kalitesini artırmasını ve toplumun refahını iyileştirmesini amaçlamaktadır.

Dijitalleşme hayatın her alanında geleneksel alışkanlıkları dönüşüme uğratmaktadır. Kullanımı artan e-devlet uygulamalarıyla kamu hizmetleri büyük oranda dijitalleşmiştir. Sanayide dijitalleşme ile üretim yöntemleri büyük bir dönüşüme uğramış, daha kolay ve daha hızlı bir hale gelmiştir. İnternet teknolojisinin kullanımının yaygınlaşması ve internete erişimin oldukça kolay hale gelmesiyle insan hayatının en önemli ve uzun parçası olan eğitim süreci de büyük değişikliğe uğramıştır. Eğitim hayatına başladıkları ilk günden dijital dünyanın getirdiği kolaylıklarla öğrenme sürecine başlayan öğrenciler, artık okullarda hazırlanan sunum kağıtlarını duvara yansıtan tepegöz teknolojisinden her öğrenciye ücretsiz olarak dağıtılan tabletlerin olduğu, akıllı tahtalarla tebeşir ve kalemin birçok okulda tarihe karıştığı ve anlatılan içeriğin görsel olarak sunulmasında projektör ve bilgisayar teknolojisinin kullanıldığı dijital bir eğitim sistemi dönemine girmiştir. Covid19 pandemisinin beraberinde getirdiği dijital dönüşüm ise eğitimin birçok alanda fiziksel olarak binalara ihtiyaç duymadan bilgisayar ve internet teknolojisi ile uzaktan da gerçekleştirilebileceğini tüm dünyaya kanıtlamıştır. Uzaktan eğitim modelleri ile üniversitelerin çevrimiçi bölümleri yaygınlaşmış ve yüksek öğrenimde dijital modelin yaygınlaşmaya başladığı yeni bir döneme girilmiştir.

İnternet üzerinden satış yapan sitelerin yaygınlaşmasıyla tüketim alışkanlıkları da oldukça büyük bir dönüşüme uğramıştır. Artık birçok kişi mağaza veya market alışverişini internet üzerinden gerçekleştirmektedir. Sağlık sektörü, siyaset ve daha birçok farklı alanın günden güne dijitalleştiği günümüzde gerçek hayatta yapılan faaliyetlerin önemli bir bölümü dijital dünyada yerini almış ve bilgisayar teknolojisinin getirdiği kolaylıklarla sürekli değişen ve dönüşen bir sürece girilmiştir.

1.1.1. Dijitalleşen Yaşam: Akıllı Kentler ve Dijital Toplum

Dijital toplum kavramı, dünya nüfusunun %56'sının yaşadığı kentlerin (Dünya Bankası, 2023) dijitalleşmeye başlaması ve "akıllı kent" kavramının ortaya çıkmasıyla birlikte içerisinde bulunduğu dijital dönüşüm ile daha belirgin ve anlamlı hale gelmiştir. Dünya Bankası'nın mevcut verileri ve tahminlerine göre 2050 yılına kadar dünya nüfusunun %70'inin kentlerde yaşayacağı öngörülmektedir. Dolayısıyla

kentlerin durdurulamayarak artan nüfus oranı ve dijitalleşmenin toplumların hayatına getirdiği olumlu ve olumsuz değişimler göz önünde bulundurulduğunda, kentleşme denilen olgunun dijitalleşme ve akıllı kentler kavramlarıyla birlikte yeni bir sürecin içerisine girdiği söylenebilir. Kentlerde artan nüfus oranları beraberinde yeni ihtiyaçları da getirmektedir. Kent altyapılarının artan nüfusa bağlı olarak yenilenmesi zorunluluğu, artan enerji ihtiyacı, toplu taşıma olanaklarının artan nüfusla birlikte oluşan talebi karşılayamaz hale gelmesi, hava kirliliği, elektrik, su ve doğalgaz gibi günlük hayatın en doğal ihtiyaçları haline gelen enerji kaynaklarının dağıtımında yaşanan sorunlar bilgisayar teknolojisinin getirdiği dijital yönetim sistemlerinin kentlerde aktif bir şekilde kullanılmasını zorunlu hale getirmiştir. Dolayısıyla dijitalleşme kavramı, ortaya çıkarttığı tüm dönüşüm süreçleriyle birlikte toplumların yaşamına olan etkisi bağlamında incelendiğinde kent temelli olarak da incelenmesi gereken bir kavramdır.

İlk ortaya çıktıkları günden bu yana sürekli değişen ve dönüşen kentler, teknolojinin günümüzde geldiği nokta ile yeni bir dönüşüm süreci olan dijitalleşme süreci içerisine girmiştir. Kentlerin dijitalleşmeye başlaması ise bilgi ve iletişim teknolojilerinin kentlerin yönetiminde daha aktif bir şekilde kullanılmaya başlanması ve kent yönetiminin daha verimli ve etkin bir hale getirilmeye çalışılması ile "akıllı kentler" kavramını ortaya çıkartmıştır. Kentlerde artan nüfus ve bununla beraber ortaya çıkan yeni ihtiyaçlar, küreselleşmeyle ortaya çıkan yeni ekonomik düzen ve dijital toplumun bu yeni ekonomik ve toplumsal düzene adaptasyon süreci, kentlerde yaşayan toplumların ihtiyaçlarının karşılanmasında sürdürülebilirlik, yönetilebilirlik ve verimliliğin sağlanması amacıyla yeni teknolojilerin ve yönetim sistemlerinin kullanılmasını bir ihtiyaç haline getirmiştir. Akıllı kent kavramının birçok farklı tanımı yapılmıştır. Çevre ve Şehircilik Bakanlığı'nın (ÇŞB) yaptığı tanıma göre akıllı kent, "*Paydaşlar arası işbirliği ile hayata geçirilen, yeni teknolojileri ve yenilikçi yaklaşımları kullanan, veri ve uzmanlığa dayalı olarak gerekçelendirilen ve gelecekteki problem ve ihtiyaçları öngörerek hayata değer katan çözümler üreten daha yaşanabilir ve sürdürülebilir şehirler*." olarak tanımlanmıştır (ÇŞB, 2019). Avrupa Komisyonu (AK) ise akıllı kentleri geleneksel ağlar ve hizmetlerin dijital çözümler kullanılarak kent sakinleri ve işletmeleri için daha verimli hale getirildiği bir yer olarak tanımlamaktadır. AK'ye göre akıllı kentler daha iyi kaynak kullanımının

olduğu ve emisyonun azaltıldığı dijital teknolojilerin ötesinde bir kavramdır. Akıllı kent kavramı, daha akıllı kentsel ulaşım ağları, güncellenmiş su temini ve atık bertaraf tesisleri ve binaları aydınlatma ve ısıtma konusunda daha verimli yöntemlerle donatılmış kentleri ifade etmektedir. Ayrıca, daha etkileşimli ve duyarlı bir kent yönetimi, daha güvenli kamusal alanlar ve yaşlanan nüfusun ihtiyaçlarının karşılamasını da içeren akıllı kent kavramı, teknoloji ve yenilikçi çözümlerin kent yönetiminin her alanında kullanılması anlamına gelmektedir (AK, 2023).

Akıllı bir kent, işletme verimliliğini artırmak, halkla bilgi paylaşımını sağlamak ve daha iyi bir yönetim hizmeti sunmak ve kent sakinlerinin refah seviyesini artırmak amacıyla bilgi ve iletişim teknolojilerini kullanır. Akıllı bir kentin temel amacı, akıllı teknolojiler ve veri analizi kullanarak kent fonksiyonlarını optimize etmek, ekonomik büyümeyi teşvik etmek ve aynı zamanda vatandaşların yaşam kalitesini iyileştirmektir. Akıllı kentlerin işlevselliği mevcut teknoloji miktarından ziyade bu teknolojinin nasıl kullanıldığındadır. Bir kentin akıllılığı teknolojiye dayalı altyapı, çevresel girişimler, etkili ve yüksek işlevli toplu taşıma, güvenilir ve ilerici kent planları, insanların şehirde yaşamasını ve çalışmasını ve kaynaklarını kullanmasını sağlama gibi karakteristik özellikler temelinde değerlendirilir (TWI-Global, 2023).

İnsanlar yaklaşık 6.000 yıl önce şehirlerde yaşamaya başladıklarından beri hijyen, suç, vergi toplama, kamusal tesislerin bakımı ve acil hizmetler gibi sürekli aynı sorunlarla uğraşmak zorunda kalmışlardır. Teknolojinin geldiği nokta ile ortaya çıkan yenilikler ise altyapıların güncellenmesini ve yeni altyapıların inşasını gerektirmektedir. Elektrik şebekesi, telefon ve cep telefonu ağları, internet, fiber optik kablo ağları, su ve atık arıtma, çöp ve geri dönüşüm, halka açık parklar ve rekreasyon alanları, raylı sistemler, hafif raylı sistemler ve otomobil yolları, yollar, ana arterler ve kullanım hakları gibi konular günümüz kentlerinin yönetiminde öne çıkan meselelerdir. Bugün kentler sürekli olarak sakinlerini ve altyapıyı izleyerek sunulacak olan hizmetlerin iletimi ve kalitesinin iyileştirilmesini sağlamak için "daha akıllı" hale gelmektedir. Bu durum ise büyük ölçüde otomasyona, internete teknolojisine ve "Nesnelerin İnterneti (IoT)" olarak adlandırılan kavrama dayanmaktadır. Nesnelerin İnterneti, kontrol edilebilen veya kontrol bilgisi gönderilebilen cihazların internete bağlanması anlamına gelen ve günümüzde özellikle dijitalleşmeyle birlikte ortaya

çıkan oldukça önemli bir gerçekliktir. Bu durumda akıllı kentler, insanlardan ve kenti oluşturan altyapılardan elektronik veri toplamak için binlerce sensörün kullanıldığı ve elde edilen verilerin analizleri çerçevesinde oluşturulan politikalarla kentlerde verimliliğin ve yaşam kalitesinin artırılmasının amaçlandığı yapılanmalardır (National Geographic, 2020).

1.1.2. Kent Kuramları Bağlamında Dijitalleşen Kentler ve Toplum

Kentlerin ortaya çıkmasına neden olan ekonomik ve toplumsal değişimler genellikle kırsaldan kente daha iyi yaşam şartları, güvenlik, eğitim veya sağlık gibi nedenlerle insanların münferit ya da toplu halde göç etmesiyle sonuçlanan bir süreçtir. Ortaya çıkan göç hareketleri ise kentlerde nüfusun artması ve beraberinde getirdiği yeni yönetim sorunlarına neden olmuştur. Günümüzde gelişen bilgi ve iletişim teknolojilerinin kent yönetiminde aktif olarak kullanılmaya başlanması ve daha verimli bir yönetim oluşturulmaya çalışılması ise akıllı kentler denen kavramın ortaya çıkmasına neden olmuştur. İlk ortaya çıktıkları zamanlardan bu yana kentlerin boyutları, nitelikleri ve işlevleri köklü değişikliklere uğramış olsa da kent yaşamını tanımlayan nitelikler genellikle aynı kalmıştır. MÖ 3000 yılının öncesinde Ortadoğu ve Mısır topraklarında doğan ilk kentler, daha sonraları bu coğrafyalardan Orta Asya ve İndus vadisine (günümüz Afganistan, Pakistan ve Hindistan coğrafyası) doğru bir yayılma göstermiştir (Huot, Thalman ve Valbelle, 2000). Kentlerin ortaya çıkması ile birlikte doğan kentleşme olgusu ise en basit anlamıyla kent sayısının artmasını ve bu kentlerde yaşayan nüfus hareketlerini anlatan bir olgudur. Dar anlamda bakıldığında demografik bir anlam taşıyan kentleşme olgusunu açıklayabilmek için demografik hareketlere sebep olan ekonomik ve toplumsal değişimlerin de göz önünde bulundurulması gerekir (Keleş, 2012). Dijitalleşme ve akıllı kentler ise bu demografik hareketlere sebep olan ekonomik ve toplumsal değişimlerin sayısal olarak anlamlandırılması ve yenilikçi çözümlerin bulunarak daha verimli bir kent yönetiminin oluşturulmasına yardımcı olmaktadır.

Kentlerin daha akıllı bir hale gelmesi ve dijitalleşmesi ile toplumların dijitalleşme süreci de hız kazanmıştır. Özellikle akıllı telefonların kullanım oranının yaygınlaşması, kent yönetiminde kullanılan sistemlerle alakalı olarak kent sakinlerine akıllı telefonlar aracılığı ile sürekli bilgi ve güncelleme gönderilmesi dijital toplumun

akıllı kentlerle bütünleşmesini kolaylaştırmıştır. Toplu taşımada otobüs veya trenlerin nerede olduğunu ve ne zaman geleceğini takip etmeye yarayan mobil uygulamalar, kentlerde oldukça sıklıkla karşılaşılan altyapı çalışmalarının son durumları ile ilgili bilgilendirmeler ya da hanelerin kullandığı elektrik, su ve gaz gibi temel ihtiyaçların kullanım oranlarının elektronik sayaçlarla ölçülerek anlamlandırılması ve verilerin oluşturulmasıyla daha verimli ve tasarruflu kullanımın sağlanması akıllı kentlerle birlikte oluşan dijital toplumun bu dönüşüm içerisinde kendisine yer bulmasını sağlamaktadır. Kentlerin dijitalleşmesi ile ortaya çıkan yeni toplumsal yapının anlaşılması ise akıllı kent kavramının anlaşılması adına oldukça önemlidir. Kentlerin toplumsal yapılarının anlaşılmasının önemli olduğu düşüncesinin ise feodalizmden kapitalizme geçişle birlikte ortaya çıktığı söylenebilir. Nüfusun artması, üretim tarzının değişmesi, kırsaldan göçlerin artmasıyla birlikte birçok düşünür yeni sistemi açıklamaya yönelmiştir. Bu bağlamda kent; kapitalist üretim güçlerinin yansıması olan toplumsal ilişkilerin açıklanması ve öngörülerde bulunulmasını sağlayabildiği oranda ele alınmış ve incelenmiştir (Pınarcıoğlu, Kanbak ve Şiriner, 2010: 72). Dijitalleşme ile ortaya çıkan yeni kent yaşamında ise elde edilen veriler yardımıyla bu öngörülerin yapılabilmesi bilgi ve iletişim teknolojileriyle çok daha kolay bir hale gelmektedir.

Akıllı kent kavramı özellikle büyük dünya metropollerinde uygulanmaya başlanmış ve bu metropollerin barındırdığı büyük nüfusların daha verimli bir şekilde yönetilmesi amaçlanmıştır. Özellikle büyük metropol kentlerin kendilerine has sorunları akıllı kent uygulamalarıyla çözüme ulaştırılmaya çalışılmaktadır. Kıta Avrupası'nda kentleşmenin beraberinde getirdiği toplumsal sorunları gündeme getiren klasik kent kuramcılarından Georg Simmel, metropol kentlerinin özelliklerini aktarırken kente özgü bir yaşam tarzının olduğunu belirtmiş ve bunu çok net bir şekilde açıklamıştır. Kenti toplumsal bir inşa ve yaşam biçimi olarak algılayan Simmel'e (2009: 321) göre kentin kendine özgü bir yaşam biçimi, kentli olmanın da getirdiği bazı özellikler vardır. İlişkilerin anonimleştiği; mesafeli etkileşimlerin gündelik hayatın büyük bir kısmını belirlediği metropolde, insanlar arası ilişkileri bir kayıtsızlık tavrı ya da ihtiyatlı olma hali belirler. Metropolün gerektirdiği sayısız etkileşim içinde kişinin ayakta kalabilmesi için gerekli olan sadece kendini düşünme veya bireyselleşme hali kent kültüründen kaynaklanır ve cemaat kültürüne alışık kırsala soğuk gözükür (Al-Rebholz, 2017: 142). Dolayısıyla kentliliğin kendiliğinden oluşan

içselleştirilmiş kuralları vardır. Dijitalleşme ve akıllı kentlerle birlikte bu içselleştirilmiş kurallarında yeni bir dönüşüm içerisine girdiğini söylemek mümkündür. Artık büyük metropollerde trafik akışını ve yoğunluğunu, toplu taşıma programlarını, hava durumunu, etkinlikleri, altyapı çalışmalarını ve kentle ilgili her türlü güncellemeyi akıllı telefonlar aracılığı ile takip etmek kent sakinleri için yazılı olmayan bir kural haline gelmiştir.

Örneğin Singapur şehir devleti, tam anlamıyla akıllı kentler yaratma yarışında öncülerden biri olarak kabul edilir. Nesnelerin interneti teknolojisini barındıran kameralarıyla kamusal alanların temizliği, kalabalık yoğunluğu ve kayıtlı araçların hareketi sürekli olarak izlenmektedir. Singapur, enerji kullanımını, atık yönetimini ve su kullanımını gerçek zamanlı olarak takip etmek için oluşturduğu sistemlere sahiptir. Ayrıca, otonom araç testleri ve yaşlıların sağlık ve refahını sağlamak için bir izleme sistemleri bulunmaktadır. Amerika Birleşik Devletleri'nin (ABD) Kansas eyaletinde bulunan Kansas City, akıllı sokak lambaları ve şehrin büyük bir kısmını donatan ücretsiz internet ağıyla akıllı kentler içerisinde yerini almaktadır. Park yeri detayları, trafik akışı ölçümü ve yayaların sık kullandığı bölgeler, şehrin veri görselleştirme uygulaması aracılığıyla sakinlere sunulmaktadır. Yine ABD'nin California eyaletinde bulunan San Diego şehrinde ise trafik akışını ve park etmeyi optimize etmek ve kamu güvenliğini ve çevre farkındalığını artırmak adına 3.200 akıllı sensör kurulmuştur. Elektrikli araçlar, güneşten elektriğe şarj istasyonlarıyla desteklenmekte ve bağlantılı kameralar trafik sorunları ve suçları izlemektedir. Dubai'de de trafik izleme sistemleri bulunmaktadır. Ayrıca akıllı sağlık çözümleri, akıllı binalar, hizmetler, eğitim ve turizm seçenekleri de mevcuttur. Barcelona da otobüs duraklarında ücretsiz internet ve USB şarj portları sunan akıllı ulaşım sistemlerine, bisiklet paylaşım programına ve çevrimiçi ödeme seçeneklerini içeren akıllı bir otopark uygulamasına sahiptir. Sıcaklık, kirlilik ve gürültü, nem ve yağışı ölçen sensörler ise sürekli veri akışı sağlamaktadır (TWI-Global, 2023).

20. yüzyılın ikinci yarısından sonra çoğu kent bilimci mekân kavramını hem toplum tarafından oluşturulan ve dönüştürülen hem de toplumu dönüştüren yapay çevre olarak kabul etmeye başlamıştır. Harvey (1985), bu anlamda kentin sadece coğrafyacılara bırakılmayacak kadar önemli bir oluşum olduğunu belirtmiştir. Mekân, bir fiziksel üretim nesnesidir; somut olarak üretilen, kullanılan, tüketilen bir nesnedir.

Kuşkusuz aynı zamanda da toplumsal olayların içinde geçtiği sosyal bir olgudur. Harvey'e (2006: 287) göre mekân ontolojik bir kategori değildir ve hem insanı biçimlendiren hem de insan tarafından biçimlendirilen toplumsal bir boyuta sahiptir. Dolayısıyla Harvey, hiçbir mekân politikasının toplumsal ilişkilerden bağımsız olmayacağını savunur. Mekânsal biçimleri, cansız nesneler olarak değil, toplumsal süreçlerle bütünleşmiş olarak görmek gerekir. Aynı şekilde bu görüşün önemli savunucularından Castells (1977: 126), toplumsal yapının bir ifadesi olarak mekânı analiz etmenin onun ekonomik, politik ve ideolojik sistemin unsurları ve bunların kombinasyonları etrafında olması gerektiğini belirtir. Bu bağlamda toplumların ve kentlerin dijital dönüşüm süreci birbiri içerisine geçmiş ve birbirini şekillendiren süreçler olarak algılanmalıdır. Toplumların dijitalleşme sürecinde bilgi ve iletişim teknolojileri ile olan ilişkileri kentlerin dijitalleşme süreçlerini de şekillendirmiştir. Özellikle bireylerin internet kullanım oranlarının artışı ve akıllı telefonların yaygınlaşması, kentlerin dijital dönüşümlerinde bu teknolojilerin aktif olarak kullanıldığı bütünleşik bir dönüşüm halinde gelişmiştir. Kent sakinlerinin oluşturulan uygulamalarla yaşadıkları mekâna ait özellikleri, toplu taşımayı, trafik güncellemelerini, güvenlik uyarılarını, hava kirliliğini ya da etkinlikleri anlık olarak takip edebildiği bu dönüşüm, toplumun ve kentlerin dijitalleşmesinin en iyi örneklerinden bir tanesidir.

Kentleşme kavramının anlaşılmasında önemli teorisyenlerden birisi olan Adna Ferrin Weber (1899), sanayi sektöründeki ücretlerin cazibesi ve diğer iş olanaklarının insanların kırsaldan kentlere doğru göç hareketini hızlandırdığını belirtmiştir. Weber, kentsel büyümenin toplumsal nedenleri üzerinde özellikle durmuş ve bu nedenleri kentlerin sunduğu bazı avantajlara dayandırmıştır. Kentlerde bulunan eğitim, eğlence, yaşam standardı, entelektüel kuruluşlar gibi olanakların kentlere olan nüfus hareketinin nedenleri olarak gösteren Weber, aynı zamanda kent yaşamına dair bilginin yayılmasının da bu hareketi etkilediğini belirtmiştir. Weber'in 1899'da kaleme aldığı kentleşmenin toplumsal nedenleri günümüzde hala geçerliliğini korumaktadır. Buna ek olarak dijitalleşme ile artan kitle iletişim araçlarının kullanımının toplumun her kesiminde artışı ve sosyal medyanın artık herkes tarafından kullanılıyor olması ise kentlerle ilgili bilginin oldukça kolay bir şekilde ulaşılmasına olanak sağlamaktadır.

Önemli kent kuramcılarından birisi olan David Harvey (2012) Asi Şehirler *(Rebel Cities)* adlı kitabında Robert Park'ın kentin doğuşu ile ilgili düşüncelerine atıf yaparak kendisinin "*Şehir Hakkı*" olarak tanımlayabileceğimiz fikrini açıklamaktadır. Park (aktaran Harvey, 2012: 3-4), insanoğlunun inşa ettiği şehir, aslında içinde yaşadığı dünyadır ve bu şehri inşa ederken dolaylı olarak ve farkında olmadan insan kendisini de yeniden inşa etmiştir demektedir. Toplumların günden güne daha fazla dijitalleşmesi, inşa edilen şehirlerin de bu dijitalleşmeye ayak uydurarak daha akıllı hale gelmelerine neden olmaktadır. Bireylerin günlük hayatının vazgeçilmez bir parçası haline dönüşen bilgi ve iletişim teknolojileri, akıllı telefonlar ve internet teknolojisi, kentlerin yönetiminin de bir parçası olmaya başlamıştır. Burgess'in (1925) kentlere gerçekleşen göç hareketleri sonrası kent yaşamına ayak uydurmaya çalışan bireyin kent yaşamına dâhil oluş ve kenti şekillendiren süreç ile yakından ilgili olan bu düşünce, Harvey'nin geliştirdiği şehir hakkı kavramının temelini oluşturur. Harvey (2012: 4), eğer Park haklı ise, nasıl bir kent istiyoruz sorusunun, nasıl insanlar olmak istiyoruz, ne tür sosyal ilişkiler geliştiriyoruz, doğa ile nasıl bir ilişkiye değer veriyoruz, ne tür bir hayat tarzını arzuluyoruz, hangi estetik değerlere sahibiz sorularından ayrı bir şekilde düşünülemeyeceğini söyler ve bu yüzden şehir hakkının bireylerin ya da grupların kentlerin bünyesinde barındırdığı kaynaklara erişiminden çok daha ötede, şehirleri arzuladığımız gibi değiştirme hakkı olduğunu anlatır. Şehir hakkı bireysel bir hak olmayıp, kolektif bir hak olarak karşımıza çıkar. Bu bağlamda dijitalleşme temelinde değerlendirildiğinde ise sonraki bölümlerde açıklanacak olan siber toplum ya da dijital toplum temelinde yeni toplumsal düzenin akıllı kentlerin ortaya çıkma sürecine doğrudan etki ettiği söylenebilir.

1.2. Siber, Sibernetik ve Siber Uzay

"Siber" kelimesi genellikle tek başına kullanılmayan bir kavramdır. Bilgi ve iletişim teknolojileri ile ilişkili olarak bu teknolojileri oluşturan her türlü bileşeni ifade etmek için kullanılan bu kelime, bilgisayar teknolojileri, veri güvenliği, verinin saklanması, verinin işlenmesi, verinin transferi, internet teknolojileri gibi kavramları çağrıştıracak şekilde kullanılan bir kavramdır. Bu kavramın oluşturduğu iki boyuttan söz edilebilir. Bunlardan ilki fiziksel boyut diğeri ise bu fiziksel boyutun ortaya çıkardığı sanal boyut (internet teknolojisi) olarak ele alınmaktadır. Bu iki boyutun birleşimi ile ortaya çıkan alan ise "Siber Uzay" olarak adlandırılmaktadır. Siber uzayı

oluşturan fiziksel sistem ise fiziki ve bilgisayar bileşenlerin bir araya gelmesiyle oluşmaktadır. Fiziki bileşen doğada var olan biyolojik yapıları oluşturan sistemler ile insan yapımı sistemlerin (ulaşım ağları, enerji üretim sistemleri gibi) bir araya gelmesiyle ortaya çıkan bir bileşendir. Bu bileşen, kendi içerisinde belirli ya da devam eden bir zaman diliminde kendisini oluşturan diğer bileşenlerle ilişki içerisinde varlığını sürdürmektedir. Fiziki bileşenin diğer boyutunu oluşturan bilgisayar teknolojisi ise işlem, iletişim ve kontrol teknolojilerini içerisinde barındırmaktadır. Bu bileşenler ise kendi içerisinde yazılımlara eklenen algoritmalar ve dijital sistemler ile ortaya çıkan bir iletişim ağını oluşturur (Sanfelice, 2016: 3).

Siber uzay ortamı oynaklık, belirsizlik, karmaşıklık ve öngörülemezlik kavramları ile karakterize edilebilir. Siber uzay elektromanyetik enerjiyi bilgisayar ortamında kodlanmış sinyallere dönüştürmek amacıyla özel olarak tasarlanmış teknoloji, yazılım ve donanım programları kullanılarak oluşturulan insan eliyle üretilmiş bir alan olması bakımından kara, hava, deniz ve uzay alanlarıyla bağlantılı olmasının yanında bu alanlardan oldukça farklı yeni bir alan olarak karşımıza çıkmaktadır (Scherrer ve Grund, 2009: 9).

Günümüzde bilişim teknolojileri tahmin edilemeyen boyutlarda gelişimlerini sürdürmektedirler. Bu gelişim ve internet teknolojisinin gelmiş olduğu seviye ile daha çok cihazın birbiriyle bağlantılı hale gelerek sınırları ortadan kaldıran bir ağın ortaya çıkması mevcut fiziki alanlara ek olarak daha önce de belirtilen ve insan eliyle üretilmiş sanal bir ortamı yaratmıştır. "Siber uzay" (cyberspace) ya da "siber alan" olarak adlandırılan bu alanın küresel anlamda kabul görmüş bir tanımlaması yoktur. İnsan ve hayvanlarda kontrol ve iletişimi konu alan çalışma alanı olarak tanımlanan "*sibernetik"* kavramından (Wiener, 1948) üretilen siber uzay kavramı, ilk defa bir bilim kurgu romanı yazarı olan William Gibson tarafından 1984 yılında *Neuromancer* isimli kitabında kullanılmıştır (Singer ve Friedman, 2014, s.12). Gibson siber uzay kavramını şu şekilde tanımlamıştır:

> "*Matematiksel kavramların öğretildiği çocuklar tarafından her milletten milyarlarca meşru operatörün tecrübe ettiği, her gün yaşanan içgüdüsel ve tepkisel bir halüsinasyon. İnsan sistemindeki tüm bilgisayarlardan edinilmiş verilerin grafiksel gösterimi. Akla hayale sığmaz bir karmaşıklık. Aklın mekansızlığında, veri kümelerinde ve takımyıldızlarında gezinen ışık çizgileri. Şehrin ışıkları gibi, uzaklaşan…*" (Gibson, 1994: 43)

Amerikan Savunma Bakanlığının yayınladığı Askeri Terimler Sözlüğünde siber uzay, bilgi teknolojisi altyapıları ve yerleşik verilerin birbirine bağlı ağları, internet, telekomünikasyon ağları, bilgisayar sistemleri ve yerleşik işlemciler ve denetleyicileri de kapsayan bilgi ortamında küresel bir alan olarak tanımlanmıştır (DoD, 2017).

Genellikle internet ve internet hizmetinin kullanıldığı bilgisayarlarla ilişkilendirilerek tanımlanan siber uzay kavramını sadece internete indirgeyerek açıklamak doğru olmayacaktır. Birbirinden bağımsız şekilde idare edilen binlerce ağdan oluşan internetin siber uzayın sadece bir parçası olduğunu söyleyen Nye (2014), devletlerin ve devlet dışı aktörlerin bu karmaşık alanda hem iş birliği hem de çatışma içerisinde olduklarını belirtmiştir (Nye, 2014: 5-6). Siber uzayı fiziksel ve sanal varlıkların emsalsiz bir kombinasyonu olarak tanımlayan Libicki (2007) ise, siber uzayın fiziksel, sözdizimsel (sentaktik) ve anlamsal (semantik) katmanlardan oluştuğunu söylemektedir. (Libicki, 2007: 5-12). Deibert (2016) ise siber uzayın küresel dijital elektronik telekomünikasyon ortamını ifade ettiğini belirterek internetten daha geniş bir anlamda siber uzayın ağa bağlı bilgi ve iletişim sistemleri ile cihazlardan oluşan, her yere nüfuz eden ve durmadan gelişen bir alan olduğunu ifade etmiştir. Siber uzay günümüzde devletler, özel sektör ve sivil toplum tarafından toplumun, ekonominin ve siyasetin her alanına dokunan kritik bir altyapı olarak tanınmıştır. Bu noktada sadece bir dakikalığına da olsa ağ bağlantılarının çalışmaması büyük ekonomik kayıpların yaşanmasını tetikleyebileceği gibi hassas kamu hizmetlerinin aksamasına da neden olabilecektir. Dolayısıyla siber uzayın güvenliği yirmi birinci yüzyılın en önemli sorunlarından birisi olarak karşımıza çıkmaktadır (Deibert, 2016: 3-8).

Siber uzayın hayatın her alanına nüfuz eden hızlı ve önüne geçilemez etkisi devletler, kurumlar ve uluslararası örgütler tarafından 2000'li yıllar itibari ile tanınmış ve uluslararası ilişkilerin önemli aktörlerinin politika belirleyicileri tarafından bu alanın güvenliğinin sağlanması kritik ve öncelikli konular arasında yer almıştır (Wilner, 2020). Bu anlamda Amerika Birleşik Devletleri Savunma Bakanlığı 2015 yılında yayınladığı "Siber Strateji" belgesi ile siber uzayı kara, deniz, hava ve uzaydan sonra beşinci muharebe alanı olarak tanımış ve siber uzayın güvenliğinin sağlanması noktasında hangi stratejileri izleyeceğini ilan etmiştir (DoD, 2015). Dünyanın en güçlü askeri ittifakı olan NATO ise siber uzayın güvenliği konusunu ilk defa 2002 yılında

Prag Zirvesinde siyasi ajandasına almış, 2007 yılında birlik üyesi olan ülkelerden Estonya'ya Rusya tarafından yapıldığı iddia edilen siber saldırılar sonrasında (Cutts, 2009: 69) 2008 yılında siber savunma politikasını kabul etmiştir. 2016 yılında gerçekleşen Varşova Zirvesinde ise siber uzay NATO'nun kara, hava ve denizden sonra dördüncü muharebe alanı olarak birlik üyesi ülkeler tarafından kabul edilmiştir (NATO/Varşova Zirvesi, 2016). Ayrıca NATO'nun kurucu anlaşmasına göre üye ülkelerden birisinin ulusal güvenliğine yapılan bir saldırı sonucu ittifak üyesi ülkelerin saldırıya uğrayan ülkenin yanında yer alacağını bildiren 5. maddenin bir siber saldırı sonucunda devreye sokulabileceği sonucuna da varılmıştır (Schmitt ve Vihul, 2017).

1.3. Dijitalleşme ile Ortaya Çıkan Siber Güvenliğin Bileşenleri

Dijitalleşme günden güne toplumun ve ekonominin gelecekteki gelişimi için bir temel olma yolunda ilerlemektedir. Günümüz dünyasında insanlar, cihazlar ve makineler teknolojik manada birbirleriyle kablolu ya da kablosuz bir şekilde bağlanmış durumdalardır. Çağımızın içerisinde bulunduğumuz bu döneminin bir internet ve akıllı telefonlar dönemi olarak kabul edildiğini düşündüğümüzde akıllı telefonlar aracılığı ile hemen her an yanımızda taşıdığımız internet teknolojisinin insanoğlunun hayatının her noktasına temas ettiğini söylemek abartılı olmayacaktır. İnternet teknolojisi, çalışmak, alışveriş yapmak, sinemaya gitmek, insanlarla iletişim kurmak, müzik dinlemek, yemek sipariş etmek, faturaları ödemek, yeni arkadaşlıklar edinmek gibi birçok günlük aktivitenin dahi icra edilme şekillerini değiştirmiştir. Buna bağlı olarak internet kullanıcılarının her an her dakika ne yaptığını ne konuştuğunu ya da nereye gittiğini takip etmek mümkün hale gelmiştir. Geldiğimiz bu noktada insanların internet kullanmasını durdurmasını beklemek olası değildir (Prasad ve Rohokale, 2019). Dijitalleşme sadece bireylerin hayatının her alanına nüfuz etmemiş aynı zamanda devletler nezdinde de oldukça etkin kullanılmaya başlamıştır.

Devletleri oluşturan yapıların giderek teknolojiyi daha aktif kullanması ve dijitalleşmeye gitmesi bu alanın güvenliğinin sağlanması zorunluluğunu bir öncelik haline getirmiştir. Özellikle bilgi ve belge yönetiminin gün geçtikçe dijital ortamlarda yapılmasını sağlayacak teknolojilerin devletlerin hemen her biriminin vazgeçilmez bir parçası haline gelmesi ise bu durumu ulusal güvenliğin vazgeçilmez bir parçasına

dönüştürmüştür. Bu noktada siber güvenliği oluşturan bileşenler devletlerin siber uzaydaki güvenliğinin sağlanması amacıyla ayrı birimler olarak ele alınmaktadır.

1.3.1. Siber Güvenlik Bileşenleri

Oldukça karmaşık bir yapıya sahip olan siber uzay ve bu alanın güvenliği farklı yaklaşımlar temelinde ele alınabilmektedir. Bu anlamda sınırları belli olmayan bu alanın güvenliğinin sağlanması bu alanı oluşturan üç temel bileşenin tam anlamıyla güvenliğinin sağlanması yoluyla gerçekleştirilebilir. Siber güvenliği oluşturan bileşenler üç ana başlık altında incelenebilir. Bunlar "teknoloji, altyapı ve insan unsuru" olarak sıralanabilir.

Teknoloji siber güvenliğin en temel bileşenidir. Siber uzay ve bu alanı oluşturan bütün bileşenlerin temelini oluşturan teknoloji ile anlatılmak istenen şey ise bilgisayar teknolojisi ve bu teknolojinin kullanılmasını sağlayan bütün bileşenleri ifade etmektedir. Bu noktada yazılım, bu yazılımların geliştirilmesi için gerekli olan bütün bileşenler, iletişim sistemleri, internet teknolojisini oluşturan vericiler, kablolar, bilgisayar ana kartları, bilgisayar işletim sistemleri gibi birbirleriyle bağlantılı olan bütün teknolojik unsurlar teknoloji bileşenini oluşturmaktadır. Siber güvenliğin sağlanmasında teknoloji unsurunun önemi ise devletlerin bahsi geçen teknolojiyi üretim kapasiteleri ile alakalıdır. Bu noktada bahsi geçen teknolojik altyapıyı oluşturan cihazların oldukça büyük bir bölümünün dünyada Microsoft, Apple, IBM gibi çok uluslu şirketlerin ürettiğini ve bu konuda bir tekel oluşturduklarını düşündüğümüzde devletlerin siber uzayın güvenliğini sağlamalarında kendi teknolojilerini üretebiliyor olmalarının önemi ortaya çıkmaktadır. Başka bir ülkeden alınan bir bilgisayar işletim sisteminin içerisine eklenmiş olan korsan bir yazılım ile kritik bilgilerin internete bağlı olan cihazlar üzerinden aktarılması oldukça kolay bir hale gelebilmektedir (Lehto ve Neittaanmäki, 2018).

Siber güvenliği oluşturan bir diğer bileşen ise bir ülkenin siber uzayını oluşturan teknolojinin altyapısıdır. İletişimi sağlayan telefon hatları, mobil internet teknolojisinde hizmet sağlayıcı operatörler, fiber optik kablo ağları ve uydular gibi sistemler siber uzayın en temel altyapısını oluşturmaktadır. Ülkelerin bu altyapılarda ne kadar güçlü oldukları siber güvenliğin sağlanmasıyla doğru orantılı bir etkiye

sahiptir. Ayrıca, bu altyapıların geleneksel olarak güvenliğinin sağlanması ise siber güvenliğin bir diğer boyutu olarak karşımıza çıkmaktadır. Bir ülkenin kritik altyapılarına yapılabilecek bir siber saldırının haricinde fiber optik kabloların geçtiği bir hatta düzenlenecek olan bir terör saldırısı da oldukça önemli sonuçlara yol açabilecek türden bir saldırıdır. Siber uzayın önemli bir katmanını oluşturan altyapı bileşeni, bu alanın coğrafi olarak sınırsızlığı ya da sanallığı noktasında farklılık göstermektedir. Dolayısıyla siber uzayı oluşturan altyapı, bölgesel olarak yerleşmiş olmakla birlikte fiziki ve siyasi coğrafyayla da yakından bağlantılıdır. Bu bağlamda diğer bileşenlerden farklı olarak bu bileşenin ulusların siber uzayı nasıl algıladığı, hukuki olarak bu alanı nasıl düzenlediği, bu alanın mülkiyeti ve bağımsızlığı anlamında haritalandırılabilir (Douzet, 2016)

Siber güvenliğin sağlanmasında gerekli olan tüm bileşenlerin içerisinde insan unsuru bulunmaktadır. İnsan unsuru içerisinde kullanıcı, yönetici, bilgisayar işletmeni, yazılımcı, mühendis, operatör, tasarımcı, geliştirici, güvenlik görevlisi gibi rolleri üstlenmektedir ve dolayısıyla siber güvenlik sürecinde doğrudan etkili olabilmektedir. İnsan unsuru kapsamında yapılacak bir hatanın ya da gösterilecek bir zafiyetin güvenlik bağlamında ne tür sonuçlar doğurabileceği ve bu sonuçların sistemin düzgün işleyebilmesi açısından ne kadar önemli olabileceği bilinci siber güvenlik farkındalığını tanımlamaktadır (Bostan ve Şengül, 2018: 146). İnsan unsuru, siber uzayın doğrudan ya da dolaylı olarak mutlak bir bileşenidir. Siber uzayda kullanıcı olarak bir sistemden faydalanan ya da sistemi tasarlayan veya işleten rolleriyle insan, siber sistemlerle sürekli etkileşim içerisindedir. Güvenlik sistemlerindeki çok katmanlı ve hiyerarşik yapı genellikle güvenlik zinciri olarak adlandırılır ve bu zinciri oluşturan halkaların birbiriyle bağlantılı olarak çalışması güvenliğin eksiksiz olarak sağlanması için vazgeçilmezdir. Bu halkalardan birisinde gerçekleşecek olan zayıflık bütün güvenlik zincirini etkileyecek ve sistemin çalışmasını durduracaktır (Booth, 2007). Bu zincirin halkalarından birisini oluşturan insan unsuru ise yapılan çalışmalarda genellikle zincirin en zayıf halkası olarak değerlendirilmektedir. Siber güvenlik ile ilgili yaşanan vakaların incelenmesinde insan kaynaklı zafiyetler diğer zafiyetlere oranla en büyük oranı oluşturmaktadır. Dolayısıyla siber güvenliği oluşturan bileşenlerden insan unsuru zincirin en zayıf halkası olarak değerlendirilmektedir (Bostan ve Şengül, 2018: 147). Ülkelerin siber güvenlik altyapılarını geliştirmek için

daha fazla nitelikli insan gücüne ihtiyaçları ortadadır. Dolayısıyla ülkeler siber güvenlik eğitim faaliyetlerine gün geçtikçe daha büyük yatırımlar yapmaktadırlar. Türkiye bu anlamda son yıllarda gerek kurumlar nezdinde başlattığı eğitim faaliyetleri ve farkındalık çalışmaları gerekse de üniversiteler bünyesinde açılan yeni bölümler ve birimler ile siber güvenlik alanında insan unsurunu güçlendirme çalışmalarına devam etmektedir.

1.4. Siber Uzayın Güvenliği ve Karşılaşılan Zorluklar

Siber uzay ve bu alanın güvenliği beraberinde birçok kavramın ortaya çıkmasını da sağlamıştır. "Siber güvenlik, siber savaş, siber savunma, siber caydırıcılık, siber terörizm, siber istihbarat, siber suçlar, siber saldırı, siber dolandırıcılık ve siber diplomasi" bu kavramların sadece bir kısmını oluşturmaktadır (Nye, 2005, 2007, 2011a; Libicki, 2006, 2007, 2009; Schmitt ve Vihul, 2017; Ermiş, 2015; Kostopoulos, 2018; Kremer ve Müller, 2014; Wiemann, 2015 vd.). Tüm bu kavramlar içerisinde siber güvenlik kavramı ise siber uzayda yaşanabilecek ve siber uzaydan gelebilecek tehditleri kapsayan bir kavramdır (Deibert ve Rohozinski, 2010). Siber güvenlik, siber uzayı oluşturan bütün ağ ve bu ağı oluşturan bilgisayarlar, kablo alt yapıları, yazılımlar gibi bileşenlerin güvenliğini ifade etmektedir. Tüm bu ağlar ve bileşenleri ise bireyler, kurumlar ve devletler tarafından çeşitli amaç ve fonksiyonlarda kullanılmaktadır. Dolayısıyla siber güvenlik bireyleri, kurumları ve devletleri kapsayan oldukça geniş bir çalışma alanı olmakla birlikte birçok devlet, uluslararası örgüt ve önemli ağ teknolojisi firmaları tarafından bir ulusal öncelik olarak kabul edilmektedir (Güntay, 2019).

Siber uzayın gün geçtikçe genişlemesi ve siber uzayda gerçekleşen faaliyetlerin artması ülkelerin güvenliğinden sorumlu birimler için yeni zorlukların ortaya çıkmasına neden olmuştur. Siber uzayda ortaya çıkan tehditler sadece çok daha karmaşık bir hale gelmemiş aynı zamanda daha güçlü ve spesifik hedeflere yönelebilen tehditlere dönüşmüştür. Siber uzay bir bakıma, devletler, kişiler, siyasi oluşumlar, suç örgütleri ve terörist gruplar tarafından istihbarat toplama, toplum üzerinde etki oluşturma, bilgi edinme ve kritik altyapıların işletim sistemlerine yapılan siber saldırılarla bu yapıları işlevsiz hale sokma gibi amaçlarla kullanılır hale gelmiştir. Coğrafi olarak sınırları olmayan ve insan eliyle üretilmiş bu alanda gerçekleştirilen

saldırılar, saldırıyı gerçekleştiren için maliyetinin konvansiyonel saldırılarla kıyaslandığında oldukça düşük olması ve belirli bir mekâna ya da coğrafyaya bağlı olmadan gerçekleştirilebiliyor olmasına ek olarak risk boyutunun oldukça düşük olması nedeniyle oldukça cazip bir saldırı yöntemine dönüşmüştür (Libicki, 2012).

Yeni bir mücadele ve çatışma ortamına dönüşen siber uzayın güvenliği bu anlamda oldukça karmaşıktır. Kara, hava, deniz ve hatta uzay ile kıyaslandığında doğal olmayan bu yeni çatışma alanı, ülkelerin ulusal güvenlikleri açısından önemli tehditler oluşturmaktadır. 2007 yılında Estonya da gerçekleşen ve ülkenin bütün iletişim sistemlerine yapılan siber saldırı kamu hizmetlerinin aksamasına neden olmuş, devlet kurumlarının kullandığı sistemler işlemez hale gelmiş, bankacılık sistemleri durmuş ve ülkede ciddi bir krize neden olmuştur. Estonya'da gerçekleşen bu saldırı siber güvenliğin sağlanmasında yaşanabilecek zorlukları tüm dünyada gün yüzüne çıkartmakla kalmamış aynı zamanda ülkelerin bu alanın güvenliğinin sağlanması noktasında da yeni önlemler almasına neden olmuştur. Her ne kadar Rusya bu saldırıdan sorumlu tutulmuş olsa da failler hala gün yüzüne çıkmamıştır.

Siber uzayda gerçekleştirilecek olan bir saldırının her an her saniye dünyanın herhangi bir coğrafyasından gelebileceği göz önünde bulundurulduğunda durumun karmaşıklığı daha da belirgin hale gelmektedir. Ayrıca siber uzayda gerçekleşen saldırılarla mücadelede uluslararası bağlamda kabul görmüş yasal bir zemin bulunmamaktadır. Ülkelerin iç hukuklarında yaptıkları düzenlemeler bu saldırıları gerçekleştiren faillerin kendi ülke sınırları içerisinde yakalanması durumunda uygulanabilecek düzenlemelerdir. Lakin bir ülkeye dünyanın başka bir coğrafyasından yapılan bir siber saldırının ortaya çıkartacağı fiziki sonuçların hangi yasal düzenlemeyle hukuki bir yaptırıma maruz kalacağı büyük bir belirsizliktir. Tüm bunlara ek olarak bir ülkeye gerçekleştirilen bir siber saldırının bir savaş sebebi sayılıp sayılmayacağı hala uluslararası hukukun çözüm bulamadığı ve ülkelerin kendi iç hukuk düzenlemeleriyle üstesinden gelmeye çalıştığı bir konudur (Douzet, 2018).

Siber uzay kavramının tanımlanması ise bu alanın güvenliğinin ve yönetiminin sağlanması adına bir diğer zorluk olarak karşımıza çıkmaktadır. Valeriano ve Maness siber uzayın tanımlanmasında İngilizce *"fog"* yani "sis" kelimesini kullanmaktadırlar. Bu kavram siber uzayın tanımının yapılmasında kapsamlı ve detaylandırılmış bir

çerçevenin oluşturulmasında yaşanan zorlukları ve tehditlerin algılanmasında ortaya çıkan zorlukları yansıtmaktadır (Valeriano ve Maness, 2012). Farklı anlamlara da gelebilen bu kelime siber uzayla ilişkilendirildiğinde "belirsizlik, bulanıklık, karartı, pus" şeklinde de algılanabilir. Siber uzayın karmaşıklığı ve kompleks yapısı düşünüldüğünde oldukça yerinde olan bu kavram, insan eliyle ortaya çıkmış ve coğrafi olarak herhangi bir sınırı olmayan bu alanın algılanması adına oldukça yerinde bir kullanımdır. Diğer birçok kavramda olduğu gibi siber uzay kavramı için de üzerinde uzlaşı sağlanmış bir tanım mevcut değildir. Bunun yerine farklı aktörler tarafından benimsenmiş ve dolayısıyla siber uzay bağlamında farklı görüşlerin ortaya çıkmasına neden olan onlarca farklı tanım mevcuttur. Sadece Amerikan Savunma Bakanlığı Pentagon'un geçtiğimiz yıllarda yayınladığı ondan fazla siber uzay tanımlaması mevcuttur. (Douzet, 2018: 3).

Siber uzayın her noktasında görülen özel sektör ise bu alanın güvenliğinin sağlanması ve yönetiminde karşılaşılan diğer zorluklardan birisidir. Dünya üzerindeki internet altyapılarının çoğu özel kuruluşlar tarafından geliştirilmiştir ve aynı zamanda bu kuruluşlar tarafından yönetilmektedir. Dünya üzerindeki bilgisayarların neredeyse yüzde 90'ı Microsoft firmasının işletim sistemiyle çalışmaktadır. Dolayısıyla Microsoft ve ona bezer diğer kuruluşlar (Apple, Symantec v.d.) bu alanın güvenliğinin sağlanması, şüpheli hareketlenmelerin tespiti ve saldırıların önlenmesi bağlamında önemli bir role sahiptirler. Bu kapsamda düşünüldüğünde devletlerin tek başına siber uzayın güvenliğini sağlayabilmeleri mümkün değildir. Siber uzayın sürekli gelişime açık yapısı ve artan kullanımına ek olarak devletlerin özel kuruluşlara bağımlılığı bu anlamda devlet-özel sektör iş birliğini kaçınılmaz kılmaktadır.

Siber uzayda gerçekleşen saldırıların karmaşıklığı ve saldırının kaynağının belirlenmesinde yaşanan zorluklar ise siber uzayın güvenliği noktasında ortaya çıkan bir diğer önemli zorluktur. Fransız haber kanalı TV5 Monde'ye 2015 yılında gerçekleştirilen ve terör örgütü IŞİD/DAEŞ ile ilişkilendirilen saldırılar ve yine aynı yıl Fransa'da yaşanan terör saldırıları oldukça büyük siyasi ve sosyal etkiler ortaya çıkartmıştır. Fransız yetkililer tarafından 2014 yılında yaşanan siber saldırıların IŞİD tarafından gerçekleştirildiği ve bunun bir terör eylemi olduğu açıklanmıştır. Lakin sonrasında yapılan araştırmalarda saldırıyı gerçekleştirenlerin IŞİD ile organik olarak

herhangi bir bağının bulunmadığı ve saldırganların büyük olasılıkla Rusya'dan oldukları değerlendirilmiştir (BBC, 2016).

2. SİBER GÜVENLİK TEHDİTLERİ

2.1. Siber Saldırı: Yöntemleri ve Çeşitleri

Siber güvenlik, ağların, bilgisayarların ve programların güvenliğiyle birlikte kötü amaçlı yazılımlara, saldırılara, hasara ve yetkisiz erişime karşı becerilerin, tekniklerin, süreçlerin ve uygulamaların bir toplamı olarak karşımıza çıkmaktadır. Bilgi ve iletişim teknolojilerindeki (BİT) ilerleme ve gelişim 5G teknolojisi ve buna bağlı olarak mobil iletişim teknolojisinin oldukça ileri ve hızlı bir seviyeye gelmesini sağlamış ve durum kaçınılmaz bir hale gelmiştir. Bu durumun olumsuz tarafı ise bu teknolojilerin kullanımının artmasıyla birlikte ortaya çıkan yeni tehditlerin oldukça güvensiz bir ortam yaratmasıdır. BİT her gün saldırılara maruz kalmakta ve bu saldırılar para, özel bilgiler, istihbarat sağlama ya da siyasi motivasyonla yapılmış saldırılar olarak ortaya çıkabilmektedir (Prasad ve Rohokale, 2020).

Siber saldırılar farklı yöntemlerle bilgisayar işletim sistemlerine yasal olmayan bir şekilde sızarak bilgi çalma, sistemin doğru çalışmasını engelleme ya da sistemin tamamen durdurulmasını amaçlayan saldırılardır. Üretim faaliyetlerini, bankacılık hizmetlerini, kamu ve özel sektör hizmetlerini, askeri sistemleri ve hatta operasyonları etkileyebilecek nitelikte olan bu saldırılar birçok farklı yöntemle yapılabilmektedir (Westberg, 2017: 275). Elektrik, doğalgaz, su gibi insanların günlük hayatlarında elzem olan enerji ihtiyaçları, bankacılık hizmetleri, ulaşım, üretim, sağlık, seyahat gibi insan hayatının günlük bir parçası haline gelen her türlü etkinliğin yapılan çalışmalar sonucunda siber saldırılar tarafından etkilenebildiği görülmüştür (Prasad ve Rohokale, 2020: 16).

Siber suçların sayısı ve sıklığı internet teknolojisinin kullanım yaygınlığının artması ve teknolojinin daha erişilebilir hale gelmesiyle artmaktadır. Dolayısıyla bir bilgisayar sistemi bu saldırıları düzenleyen taraf olabildiği gibi aynı zamanda bu saldırılara maruz kalan taraf da olabilmektedir. Siber saldırılar birçok farklı kategori ve bu kategorilerin alt saldırıları şeklinde incelenmektedir. Bu saldırıların en

bilinenleri ise zararlı yazılımlar kullanarak bilgisayar sistemlerine sızmayı sağlayan *"kötü amaçlı yazılım"* (malware), aktif ya da pasif olarak bilgisayar ve ağ bağlantılarını izleyen *"ağ saldırıları"* (network attacks), bilgisayar ağlarına izinsiz bir şekilde girmeyi tanımlayan *"ağ ihlali saldırıları"* (network intrusion attacks), insan doğasında bulunan zayıf noktaları tespit ederek farklı yöntemlerle insanların düşüncelerine yön verme amacıyla yapılan *"sosyal mühendislik saldırıları"* (social engineering attacks), bireylerin ya da kuruluşların bilgi işletim sistemlerine sızarak yasal olmayan bir şekilde bilgileri aktarmayı tanımlayan "siber espiyonaj" (cyber espionage), devletlerin özellikle kritik altyapılarını kontrol eden işletim sistemlerine yapılan "siber terörizm" (cyber terrorism) saldırıları ve son dönemde gerek ulusal gerekse uluslararası hukuku meşgul eden "siber savaş" (cyber warfare) saldırıları şeklinde kategorize edilebilir (Prasad ve Rohokale, 2020: 15-17).

2.1.1. Kötü Amaçlı Yazılımlar (Malware)

Kötü amaçlı yazılımlar (malware) siber saldırı yöntemleri içerisinde en çok kullanılan yöntemlerin başında gelmektedir. Bu tür yazılımlar spesifik olarak bir hedefe karşı kullanılan ve bilgisayar sistemlerine karşı gerçekleştirilen saldırılardır. Birçok alt kategoriyi içerisinde barındıran kötü amaçlı yazılımlar aracılığıyla yapılan saldırılar oldukça karmaşık bir hale gelebilmekle birlikte kullanıcıların çoğu zaman farkına bile varmadan bilgisayar sistemlerinin içerisine sızabilmektedirler (McAfee, 2023).

Reklam görünümlü yazılımlar (adware), casus yazılımlar (spyware), virüsler (virüs), truva atı (Trojan), işletim sisteminde arka planda çalışan gizli program ya da programlar grubu (rootkit), arka kapı saldırıları (backdoor), tuş kaydedici yazılımlar (key loggers), sahte antivirüs yazılımları (rogue security spftware), kullanıcıların programa giriş yapabilmesi için belirli bir fidye tutarı ödeyene kadar kullanıcının bilgisayarını etkisiz hale getiren yazılım (ransomware) ve son olarak sahte internet tarayıcıları aracılığıyla hırsızlık yapılmasını sağlayan yazılımlar (browser hijacker) kötü amaçlı yazılımlar aracılığıyla yapılan saldırıların alt kategorileri olarak sıralanabilir (Prasad ve Rohokale, 2020: 28).

Yukarıda bahsi geçen kötü amaçlı yazılımlarla yapılabilen saldırılar bilgisayar ya da akıllı telefon kullanan ve internete erişimi olan herkesin gün içerisinde

karşılaşabileceği türden saldırılardır. Özellikle kullanıcıların dikkatini çeken ürünlerin reklamları şeklinde öne sürüldüğünde oldukça kolay bir şekilde sisteme girmeyi sağlayabilmektedir. Teknoloji kullananların her gün kullandığı internet tarayıcılarının kullanıcıların karşısına çıkarttığı reklam içerikleri bu anlamda kötü amaçlı yazılımların bilgisayar sistemlerinin içerisine sızabilmesi için iyi bir fırsattır.

Bahsi geçen saldırı yöntemleri genel olarak birbirleriyle bağlantılı bir şekilde kullanılabilmektedir. Kullanıcıların dikkatini çeken bir reklam yazılımı üzerinden sisteminize indirdiğiniz fakat farkında olmadığınız bir tuş kaydedici yazılım (key logger) internet aracılığı ile yapılan tüm alışverişlerde ya da oldukça kritik bilgilerinizi sakladığınız e-mail adreslerinize erişimde ya da şifresi ve kullanıcı adı olan herhangi bir sistemde tüm bilgilerinizi kaydederek bu sistemi kötü amaçlı kimselerin kullanımına oldukça kolay bir şekilde açabilme kapasitesine sahiptir.

2.1.2. Ağ Saldırıları (Network Attacks)

Ağ saldırıları aktif ya da pasif bir şekilde bilgisayar ve ağ bağlantılarını hedef alan saldırılardır. Ağ saldırıları birçok farklı şekilde yapılabilmektedir. Ağ saldırıları spesifik olarak bir kuruma ya da organizasyona ait bir ağa yetkisiz bir şekilde erişim sağlanarak veri hırsızlığı yapma amaçlı gerçekleştirilen saldırılardır. Bu saldırılar kullanıcı adları, şifreler, banka hesap numaraları gibi kritik belgelerin ele geçirilerek sonrasında bu bilgilerle yasa dışı gelir elde etme ya da bir kuruma ait hassas bilgilerin ele geçirilmesi amacıyla yapılan saldırılar şeklinde karşımıza çıkmaktadır. Ağ saldırılarının en bilinenleri sazan avlama (phishing) (Cisco, 2022) ve sahte e-posta ya da başka bir ağa saldırı düzenleyen kişinin kendisini saldırıyı düzenlediği ağın yetkili bir kullanıcısı olarak gösterdiği (spoofing)saldırı yöntemidir (Kaspersky, 2022b).

Sazan avlama yöntemi ağ saldırılarında en çok karşılaşılan yöntemlerden birisidir. Bu saldırıda saldırgan kullanıcıların sürekli kullandığı web sitelerinin birebir aynısını yaparak kullanıcının farkında olmadan bu web sitesi üzerinden kritik bilgilerini ele geçirmesi şeklinde gerçekleşir. Kullanıcıların farkı anlamalarının oldukça güç olduğu bu tür saldırılarda saldırgan birebir kopyasını yaptığı bir bankanın web sitesini ya da e-posta hizmeti sağlayıcısının web adresini kullanıcıya ulaştırdıktan sonra kullanıcının her zaman olduğu gibi kullanıcı adı ve şifresini bahsi geçen sahte adrese hesabına erişim için girmesini bekler. Sahte web sitesi üzerinden hesabına

erişim sağlamaya çalışan kullanıcın bilgileri saldırganın eline geçtikten sonra ise saldırgan bu bilgileri istediği gibi değiştirerek kullanabilme imkanına sahiptir (IBM, 2021).

2.1.3. Sosyal Mühendislik Saldırıları (Social Engineering Attacks)

Siber uzayda gerçekleşen saldırı yöntemlerinin en popülerlerinden birisi olan sosyal mühendislik saldırıları aslında bakıldığında birçok farklı alanda kullanılan bir saldırı yöntemi şeklinde karşımıza çıkmaktadır. Sosyal mühendislik saldırıları geçtiğimiz on yıl içerisinde o kadar yaygınlaşmıştır ki sosyal mühendisliği geldiğimiz noktada güvenlik, yönetim, eğitim, psikoloji, sosyoloji, askeri ve diğer birçok farklı alanda görmek mümkün hale gelmiştir. Maliyeti düşük, riski az olan sosyal mühendislik saldırılarının ortaya çıkartabileceği potansiyel etki ise oldukça büyüktür. Bir sosyal mühendisin ana amacı hedefin düşünmeden karar vermesini sağlayarak kendi amacına uygun hareket ettirmektir (Kaspersky, 2022a).

Bir başka tanıma göre sosyal mühendislik etik olmayan ve teknik bilgi gerektirmeyen bir saldırı türü olarak tanımlanmaktadır. Sosyal mühendislik bu tanıma göre bir kişiyi yanlış yönlendirmelerle önemli bilgileri elde etmeyi amaçlamaktadır. Saldırganın insan zihninden faydalanarak önemli bilgileri ele geçirmesi ve bu bilgilerle aslında erişimi olmayan mecralara ulaşarak bu durumdan fayda elde etmesi şeklinde ortaya çıkmaktadır. Sosyal mühendislik insan doğasında var olan yardım etme güdüsü, güven ya da korku gibi içgüdüsel davranışlardan faydalanmaktadır (Graves, 2010: 48-49). Bilgi güvenliği açısından oldukça büyük bir tehdit oluşturan sosyal mühendislik saldırıları, siber uzayda gerçekleştirilen ve yüksek seviye teknik bilgi gerektiren saldırılara eş değer seviyede bir tehdit olarak algılanmalıdır. Teknolojinin kullanımından çok insan doğasında bulunan zayıf noktaları hedef alan bu tür saldırılar güvenlik zincirinin en zayıf halkasının insan olduğu düşünüldüğünde bilgi güvenliği açısından büyük bir tehdit oluşturmaktadır.

Sosyal mühendislik saldırıları insan temelli sosyal mühendislik ve bilgisayar temelli sosyal mühendislik olmak üzere iki temel kategoride incelenmektedir (Prasad ve Rohokale, 2020; Salahdine ve Kaabouch, 2019; Hadnagy: 2018). İnsan temelli sosyal mühendislik saldırıları farklı yöntemlerle gerçekleştirilebilmektedir. Bunlar arasında en bilinenleri bir başkası gibi davranarak karşıdakini kandırma yöntemi

(impersonating), önemli bir kişi ya da kullanıcı gibi davranarak karşıdaki kişiyi kandırıp önemli bilgileri elde etme, saldırganın kendisini teknik servis elemanı olarak tanıtıp yardım olmayan bir sorunu çözmek adına bilgi hırsızlığı yapması, bir kişinin kullanıcı adı ve şifre gibi kişisel bilgilerini o fark etmeden ele geçirme olarak adlandırılan omuz sörfü (shoulder surfing) ve bir kullanıcının artık ihtiyacı olmadığını düşündüğü ve bir kenara attığı CD, belge, harici bellek, kullanılmayan bir bilgisayar ya da cep telefonu gibi şeylerin karıştırılarak değerli bilgi elde etme eylemi olan çöp karıştırma (dumpster diving) teknikleri insan temelli sosyal mühendislik saldırı yöntemleri olarak değerlendirilmektedir (Prasad ve Rohokale, 2020; Salahdine ve Kaabouch, 2019; Hadnagy, 2018; Graves, 2010).

Bilgisayar temelli yapılan sosyal mühendislik saldırıları da insan temelli yapılan saldırılar gibi insan mantığını temel alarak teknolojik aygıtları bu yönde kullanmaya dayalıdır. Bilgisayar ve internet teknolojisinin geldiği nokta hayatın birçok alanında insanlara kolaylık ve lüks sağlamaktadır. Buna bağlı olarak bu teknolojilerin artan kullanımı artık bir bağımlılık seviyesine gelmiştir. Dolayısıyla hemen herkesin kullandığı kişisel bilgisayarlar ve cep telefonları bilgisayar temelli yapılan sosyal mühendislik saldırıları için bir araç olarak kullanılmaktadır. Mobil iletişim teknolojisi ile hedefe yaklaşımın çok daha kolay, masrafsız ve risksiz hale gelmesi siber uzayı sosyal mühendislik saldırıları anlamında oldukça uygun bir ortam haline sokmuştur.

Bilgisayar temelli gerçekleştirilen sosyal mühendislik saldırıları da farklı yöntemlerle yapılabilmektedir. Bu kimi zaman standart bir e-postaya eklenen ve farkında olmadığımız bir dosya olabildiği gibi sazan avlama (phishing) tekniğinde olduğu gibi sahte web siteleri üzerinden de yapılabilmektedir. İnternette gezinirken karşımıza bir anda çıkan sayfalar (pop-up Windows), kimlik bilgilerinin sanal ortamda ele geçirilmesi, sahte alışveriş siteleri, sahte e-posta adresleri ile gönderilen belgeler gibi yöntemler siber uzayda en sık karşılaşılan sosyal mühendislik saldırılarıdır (Deibert, 2016: 324).

Sosyal mühendislik alanında önemli çalışmaları olan Hadnagy bu alanda gerçekleştirilen saldırıları dört temel kategoride değerlendirmektedir. Bunlar SMS yani kısa mesajlar ile yapılan saldırılar, telefon aramaları ile yapılan saldırılar, sazan

avı/oltalama (phishing) saldırıları ve bir başkası gibi davranarak hedefi kandırma yöntemi (impersonation) ile yapılan saldırılardır (Hadnagy, 2018: 18-19).

Mobil teknoloji ile hayatımıza giren SMS yani kısa mesaj aracılığı ile yapılan oltalama saldırılardır. Bu tip saldırılarda kullanıcın cep telefonuna gelen bir kısa mesajla bir bankanın önemli bir güvenlik uyarısı gönderdiği ve bunun için mesajda verilen bir internet uzantısı bağlantısı (link) olabileceği gibi hedefin önemli bir soruşturmada adının geçtiği ve acilen mesajda verilen numarayı araması gerektiği belirtilebilir. Numarayı arayan hedefe kimlik bilgilerinin doğrulanması adına sorulan sorularda hedefin bilgileri elde edilir. Telefon aramaları ile gerçekleşen saldırılarda ise saldırgan kendisini bir kamu görevlisi, teknik servis yetkilisi ya da banka görevlisi gibi tanıtarak hedefin kritik bilgilerini ele geçirmeye çalışmaktadır. Bunlara ek olarak bu tarz saldırıların en popüler olanları bazı devlet kurumları tarafından kendilerine ödeme yapılacağı bilgisini içeren sms mesajlarının içerisine eklenen linkler üzerinden kişisel verilerin hedef alındığı saldırılardır. Bahsi geçen tüm bu saldırı yöntemleri aslında daha önce de belirtilen sazan avlama/oltalama (phishing) yönteminin farklı versiyonları şeklinde gerçekleştirilmektedir. Ülkemizde son dönemlerde oldukça sıklıkla karşılaşılan bu tür saldırılar kendisini asker, polis, savcı gibi kamu görevlisi olarak tanıtan ya da bir bankadan arıyormuş gibi kişisel bilgileri ele geçirmeye çalışan saldırganların yaptığı uygulamalardır. Ayrıca bu durum devlet kurumlarında kritik pozisyonlarda çalışan kişilerin bilgilerini ele geçirerek oldukça gizli bilgi ve belgeleri ele geçirmek adına bir istihbarat faaliyeti olarak da karşımıza çıkabilmektedir. Güvenlik birimlerinin vatandaşlara bu tür aramalar ve mesajlara itibar etmemelerini gerektiren uyarı mesajları ve sosyal medya paylaşımları ise bu tarz saldırıların ne kadar popüler hale geldiğinin bir göstergesidir.

2.1.4. Siber Espiyonaj ve Siber İstihbarat

Siber uzayın güvenliği ile ilgili ele alınması gereken bir diğer konu ise ulusal güvenliğin sağlanmasında hayati rol oynayan istihbarat faaliyetlerinin dijitalleşme ile içerisine girdiği dönüşümdür. İstihbarat, bireylerin ve devletlerin bilgi teknolojilerini her alanda oldukça yoğun bir şekilde kullanmalarına bağlı olarak siber uzayda da önemini artırmıştır. Teknolojinin bu kadar yaygın kullanılmaya başlamasıyla birlikte geleneksel istihbarat yöntemleri de bu değişime ayak uydurarak büyük bir dönüşüm

içerisine girmiştir. Bilginin büyük oranda dijital ortamlarda saklandığı ve işlendiği düşünüldüğünde bu ortamlara sızarak yapılan bilgi toplama faaliyetleri ülkelerin istihbarat birimleri tarafından maliyeti düşük ve riski az bir istihbarat edinme yöntemi olarak karşımıza çıkmaktadır. İstihbarat kavramı işleme tabi tutulmuş, değerlendirilmiş bilgi (Tezsever, 1999: 106), sahip olunan verilerin en verimli şekilde kullanılması ve bilginin gücü (Bal, 2006: 67) şeklinde farklı tanımlara sahiptir. Bu tanımlardan da anlaşılacağı gibi istihbarat sadece bilgi toplama ve haber alma faaliyetleri olarak değil aynı zamanda elde edilen verilerin doğru bir şekilde işlenerek doğru bilgi üretilmesi şeklinde algılanmalıdır.

Siber uzayda gerçekleştirilen istihbarat faaliyetleri ise birçok farklı yöntemle gerçekleştirilmektedir. Bunlardan en bilinenleri ise "teknik istihbarat, sinyal istihbaratı, ölçüm ve iz istihbaratı" olarak literatürde yerini almaktadır (Roberts, 2011: 3). İnternet kullanımının tahmin edilemeyen boyutlarda artması, özellikle sosyal medya kullanımın oldukça yaygınlaşmasıyla birlikte bireyler hakkında edinilebilecek bilgiye ulaşımın çok daha kolay hale gelmesi, açık kaynakların artması ve bilginin işlendiği ve saklandığı dijital ortamların internet ile olan bağlantısı istihbaratı bu ortamlarda daha az personel, daha az maliyet ve çok daha az riskle yürütmeyi mümkün kılmaktadır.

Siber istihbarat yöntemleri ülkelerin sahip oldukları bilgi toplama kapasitelerine bağlı olarak farklılık gösterebilir. Genel olarak bakıldığında bilinen en yaygın siber istihbarat yöntemleri ise "siber elektronik istihbarat, siber açık kaynak istihbaratı ve sosyal ağlara dayalı siber istihbarat" şeklinde üç ana başlık altında incelenebilir.

Siber elektronik istihbarat bu işte uzman kişiler ya da geliştirilen yazılımlar aracılığı ile bir işletim sistemine kullanıcının izini ve bilgisi olmadan sızma işlemi gerçekleştirerek bilgi edinme olarak tanımlanabilir (Bayraktar, 2014: 131). Teknoloji alanında yaşanan gelişmeler ve devletlerin bu noktada özellikle istihbarat alanında yaptığı çalışmalar siber uzayı devletler ve birçok diğer kuruluş için bir bilgi kaynağı haline getirmiştir. Daha önce bahsi geçen ağ saldırıları, kötü amaçlı yazılımlar ya da sosyal mühendislik saldırıları bu saldırıları gerçekleştiren kişilerin devlet desteği alarak kapasitelerini artırmasıyla birlikte oldukça güçlü bir istihbarat toplama yöntemi

haline dönüşebilmektedir. Elektronik istihbarat sadece devletlerin ulusal çıkarları için elzem olan bilginin toplanması adına kullanılan bir yöntem olarak algılanmamalıdır. Aynı zamanda farklı sektörlerde faaliyet gösteren kuruluşların aralarındaki rekabette bir diğerine avantaj sağlayacak ticari sırların ele geçirilmesi adına da oldukça sıklıkla kullanılan bir yöntem olarak karşımıza çıkmaktadır (Singer ve Friedman, 2014).

Siber açık kaynak istihbaratı ise internet ortamında oldukça hızlı bir şekilde yayılan haberlerin doğru şekilde analiz edilerek istihbarata dönüştürülmesidir. Bu bağlamda siber uzay, istihbarat örgütleri için sınırsız bir bilgi kaynağı olarak değerlendirilebilir. Medya kuruluşlarının haricinde sosyal medya aracılığıyla artık her bir bireyin bir medya organı haline dönüşebildiği günümüzde bilgi oldukça akışkan ve ulaşılabilirliği yüksek bir olgudur. Dünyanın her yerinde dijital ortamda yayın yapan medya kuruluşlarının haberleri istihbarat örgütlerinin kritik gördüğü konularda bilgi edinmesini sağlayacak önemli kaynaklardır. Bir ülkenin siyasi durumu, iç politikada neler yaşandığı, askeri kapasitesi gibi önemli konular hakkında bilgi edinebilmeyi sağlayan açık kaynak istihbaratı tamamen maliyetsiz bir yöntem olması açısından oldukça önemlidir.

Sosyal ağlara dayalı siber istihbarat ise daha önce de bahsi geçen siber sosyal mühendislik saldırıları ile oldukça yakından ilgilidir. Hemen herkesin kullandığı sosyal medya ağları istihbarat örgütlerinin yayılmasını istediği bilginin oldukça kısa süreler içerisinde milyonlara ulaşmasını sağlayacak platformlardır. Bu bağlamda halkın kışkırtılması, propaganda ya da psikolojik hareketler gibi örtülü operasyonlar için oldukça müsait bir ortamdır (Bayraktar, 2014: 137-138). Dünyada internet kullanımı ile ilgili istatiksel araştırmalar yapan önemli kuruluşlardan birisi olan DataReportal'ın 2022 yılında yayınladığı rakamlara göre dünya nüfusunun yüzde 58,7'si sosyal medya kullanmaktadır. Yine aynı kuruluşun verilerine göre Türkiye'de sosyal medya kullanan kişi sayısı ise nüfusun yaklaşık yüzde 82'sini oluşturmaktadır (DataReportal, 2022). Bireylerin hayatıyla ilgili hemen her detayı paylaştığı bu platformlar bilgi toplama adına önemli kaynaklar olmakla birlikte herhangi bir bilginin ya da haberin milyonlarca kişiye dakikalar içerisinde ulaştırılabilmesi adına oldukça büyük önem taşımaktadır. 2010 yılında Tunus'ta başlayarak Tüm Kuzey Afrika ülkelerine ve oradan da Ortadoğu ülkelerine yayılan Arap Baharı hareketi, yayıldığı ülkelerde rejim değişikliklerine giden etkilere sahip olmuştur. İnsanların ülkelerindeki

yönetimden duydukları rahatsızlıkları ve sorunları protesto etmek için meydanlarda toplandığı bu hareketin bu kadar büyük bir etkiye sahip olmasındaki en büyük kaynak ise sosyal medya platformlarında vatandaşların örgütlenerek bir araya gelmesiyle olmuştur. Bu etki göz önünde bulundurulduğunda sosyal medyanın gücü ülkeler içerisinde halkların bir amaç etrafında toplanarak farklı güçlerin amaçlarına hizmet edecek hareketlenmelere yol açabilmesi adına her zaman göz önünde bulundurulması gereken bir gerçekliktir.

2.1.5. Siber Terörizm

Terörizm çalışmaları öngörülebilirlik bakımından değerlendirildiğinde en karmaşık çalışma alanlarından birisi olarak karşımıza çıkmaktadır. Terör örgütleri veya terörle ilintili olan yapılanmalar yaşam süreleri boyunca sabit bir yol izlemekten kaçınmaya meyilli bir şekilde hareket etmektedirler (Shapiro, 2013: 17). Bu yapılanmalarla mücadele eden birimler ortaya çıkabilecek potansiyel tehditlerin önüne geçebilmek ve bu yapılanmaların karşısına çıkabilecek fırsatları ortadan kaldırabilmek adına oldukça büyük çaba harcamaktadırlar. Bu bağlamda değerlendirildiğinde terörist yapılanmalar bu çalışmaların önüne geçebilmek ve amaçlarına ulaşabilmek adına yaratıcılıklarını, teknik ve operasyonel kapasitelerini geliştirmek zorunda olduklarının farkında olarak her geçen gün bilgi birikimlerini geliştirmektedirler (Torres-Soriano ve Toboso-Buezo, 2019: 49).

Siber uzay, internet teknolojisinin kullanımının yaygınlaşması ve hemen her yerde erişimin mümkün hale gelmesiyle birlikte terör örgütleri için vazgeçilmez bir araç haline gelmiştir. Yeni bir muharebe alanı olarak kabul edilen siber uzay, terör örgütleri için sadece yeni bir eylem alanı değil aynı zamanda konvansiyonel olarak yapmaya devam ettikleri eylem ve etkinlikleri için de yeri geldiğinde bir eğitim ve finans sağlama aracı, yeri geldiğinde oldukça kolay bir iletişim ve propaganda alanı ve aynı zamanda kendilerine para harcamadan yeni sempatizanlar bulabilecekleri masrafsız bir mecra haline dönüşmüştür. Terörist gruplar siber araçları oldukça aktif bir şekilde kullanmaya başlamışlardır. Terör faaliyetlerinin siber uzayda da gerçekleştirilebileceği ya da siber uzayın kolaylıklarından faydalanarak bu tarz faaliyetlerin gerçekleştirilebileceğinin anlaşılmasıyla birlikte siber uzay ve terörizm kavramları yan yana gelmeye başlamıştır. Bu kavramların bir arada kullanılmasıyla

birlikte ortaya çıkan siber terörizm kavramı günümüzde halen uluslararası kabul görmüş bir tanıma sahip değildir. İlk defa 1980'li yıllarda Barry Collin tarafından kullanılan kavram üzerine tıpkı terörizm kavramında olduğu gibi birçok farklı tanım yapılmıştır. Siber terörizm kavramı bu yıllarda ABD'de devlet kurumlarına ya da ekonomiye gerçekleştirilebilecek olan bilgisayar temelli saldırıları tanımlamak maksadıyla kullanılmaya başlanmıştır. Collin siber terörizm kavramıyla alakalı olarak o yıllarda fiziksel ve sanal olan varlıkların terörizm kavramının bazı özellikleriyle nasıl birleşebileceğini işaret etmiştir (FBI, 2011).

Siber terörizm kavramının tanımına geçmeden önce terörizm kavramının tanımıyla başlamak faydalı olacaktır. Bilindiği üzere terörizm kavramı üzerine uluslararası anlamda anlaşma sağlanmış tek bir tanım bulunmamaktadır. Her devletin ve uluslararası kuruluşun farklı bir şekilde tanımladığı terörizm kavramı üzerine yapılan çalışmaların kesiştiği ve hepsinin belirlediği ortak nokta ise terörist faaliyetlerde kullanılan şiddetin siyasi bir amaca ulaşmak adına kullanıldığı ve toplumda korku ve panik yaratma maksadının olduğudur. Ülkemizde terör tanımlaması 3713 sayılı Terörle Mücadele Kanunu'nda (TMK) oldukça detaylı ve genişletilmiş bir şekilde yapılmıştır. TMK terör kavramını şu şekilde tanımlamaktadır:

> "*Terör cebir ve şiddet kullanarak; baskı, korkutma, yıldırma, sindirme veya tehdit yöntemlerinden biriyle, Anayasada belirtilen Cumhuriyetin niteliklerini, siyasî, hukukî, sosyal, laik, ekonomik düzeni değiştirmek, Devletin ülkesi ve milletiyle bölünmez bütünlüğünü bozmak, Türk Devletinin ve Cumhuriyetin varlığını tehlikeye düşürmek, Devlet otoritesini zaafa uğratmak veya yıkmak veya ele geçirmek, temel hak ve hürriyetleri yok etmek, Devletin iç ve dış güvenliğini, kamu düzenini veya genel sağlığı bozmak amacıyla bir örgüte mensup kişi veya kişiler tarafından girişilecek her türlü suç teşkil eden eylemlerdir.*" (TMK, 1991: Md. 1)

Siber terörizm kavramı, tıpkı terör ve terörizm kavramında olduğu gibi, tanım konusunda uluslararası kabul görmüş bir tanıma sahip değildir. Farklı kaynaklar bu kavramı sanal ve fiziksel faktörler arasında bir denge bulmaya çalışarak bu faktörlerin dahil olduğu biçimde farklı biçimlerde tanımlamaktadırlar (Riglietti, 2017: 15). Siber terörizm kavramı ortaya çıktığından bu yana oldukça hızlı bir şekilde yayılmış ve akademisyenler, devlet kurumları, yasal uygulamalar ve medya tarafından farklı olaylarla ilişkilendirilerek kullanılmaya başlanmıştır. Fakat artan bu kullanımın her zaman doğru bir şekilde yapıldığını söylemek mümkün değildir. Örnek olarak, bilgi

teknolojileri altyapılarına yapılan siber saldırılar ve buna benzer eylemler de kimi zaman siber terörizm olarak değerlendirilmektedir. Aslında bu tarz saldırılar daha çok siber suçlar olarak değerlendirilebilir. Buradaki karışıklık, siber suçlular ve siber teröristlerin kullandığı yöntemlerin aynı olmasından kaynaklanmaktadır. Bir siber saldırı olayının siber suç ya da siber terör kapsamında değerlendirilmesinde ortaya çıkan ayrım, gerçekleştirilen saldırının amacı noktasında birbirinden ayrılmaktadır. Bu noktada daha önce de belirtildiği üzere literatürde bulunan birçok farklı terör tanımının ortak noktası olan şiddet ve siyasi amaç faktörleri ayırt edici faktörler olarak karşımıza çıkmaktadırlar. Konuyla ilgili uzmanların yaptığı çalışmalarda siber terörizm ve siber suç kavramlarının ayırt edilmesinde gerçekleştirilen eylemin içeriği en önemli faktör olarak karşımıza çıkmaktadır. Her ne kadar benzer teknikler suçlular ve teröristler tarafından kullanılıyor olsa da saldırıyı gerçekleştirenlerin siyasi amaçlarla fiziksel bir zarara yol açma maksadı en ayırt edici özellik olarak değerlendirilmektedir (InfoSec, 2012).

Siber terörizm farklı kaynaklar ve araştırmacılar tarafından farklı yönleri ele alınarak tanımlanmaktadır. Amerikan Federal Soruşturma Bürosu (FBI) tarafından yapılan tanıma göre siber terörizm, ulus altı gruplar veya yasadışı ajanlar tarafından siyasi bir motivasyonla önceden tasarlanarak bilgi, bilgisayar sistemleri ve verilere yapılan ve muharip olmayan hedeflere karşı şiddetle sonuçlanan saldırılar şeklinde tanımlanmaktadır (Denning, 1999). 1997 yılında bir FBI çalışanı tarafından yapılan bu tanım, o yıllarda her ne kadar doğru olsa da teknolojinin geldiği nokta düşünüldüğünde siber terörizm kapsamı mevcut gelişmelere bağlı olarak oldukça detaylandırılabilir. Bu bağlamda FBI seneler içerisinde siber terörizm tanımını defalarca değiştirmiştir. Yapılan tanımlarda siber terörizm sadece bilgi teknolojileri altyapılarına yapılan saldırıları kapsayan bir tanımdan çok daha geniş aktiviteleri kapsayan tanımlara evrilmiştir. Amerikan Merkezi Haber Alma Ajansı'na (CIA) göre siber terörizm ileri teknolojinin kullanılması yoluyla siyasi, dini veya ideolojik amaçların elde edilmesi maksadıyla kritik altyapıların devre dışı bırakılması veya verilerinin silinmesiyle sonuçlanan saldırılardır (Riglietti, 2017: 16). Yapılan bir başka tanımda ise siber terörizm Mahir Terzi tarafından "*siyasal içerikli olup siber ortamda, insanların da bir parçası olduğu siber sistemlere karşı bozma, sızma veya ihlal etmenin gerçekleşmesi veya gerçekleştirme tehdidi gibi bir hareketin neden olduğu engellenme sonucu,*

milyonların davranışını etkilemek ve günlük yaşamın gidişatını bozmak" şeklinde tanımlanmaktadır (Terzi, 2018: 92).

Siber terörizmi farklı bir bakış açısından inceleyen Awan (2014) siber terörizmle ilgili olarak iki farklı yönü karşılaştırmaktadır. İlk olarak bilgisayarı ana silah olarak ele alan Awan, ikinci olarak bilgisayar olgusunu genişleterek bu silahın radikalleşme, patlatıcı yapımı hakkında tariflere ulaşma gibi amaçlarla kullanılabileceğinin üzerinde durmuştur. Yazara göre siber uzayda gerçekleşen terör eylemlerinin çoğunun ikinci hipoteze daha çok uyduğunu söylemektedir. Yapılan araştırmalara göre bilgisayar teknolojisiyle yapılan saldırılar sonucunda can kaybının yaşanması ya da ciddi bir fiziksel zararın ortaya çıkması olasılığı hala oldukça düşüktür. Fakat bu durum gelecekte terörist yapıların siber uzayda gerçekleştirebileceği daha karmaşık saldırılar sonucu bu tarz sonuçlara ulaşamayacağı anlamına gelmemektedir (Awan, 2014: 5-9).

Siber uzayın kullanımının geldiği nokta göz önünde bulundurulduğunda yapılan siber terörizm tanımları her ne kadar kapsayıcı olsa da teknolojinin günden güne değişen yapısı bu tanımların güncellenmesi gerekliliğini de ortaya çıkartmaktadır. Bireylerin teknoloji kullanımının artışı ve internet teknolojisinin akıllı telefonlardan evlerdeki basit sarf malzemelerinin kontrolüne kadar günlük hayatın bir parçası haline gelmesi siber uzayda büyük toplulukları etkileyebilecek saldırıların da önünü açmış ve bireysel sonuçlar doğurabilecek tehditler ortaya çıkartmıştır. 2019 yılında STM'nin[1] yayınladığı Siber Tehdit Durum Raporuna göre akıllı ev sistemleri ve akıllı cihazlara yapılacak koordineli bir saldırı insanların yaşam kalitesini ve hatta sağlığını olumsuz yönde etkileyebilir. Birçok kişinin kullandığı akıllı ses sitemlerine yapılacak akustik bir saldırı insanlar üzerinde basit göz atması şeklinde bir etki doğurabileceği gibi aynı zamanda işitme kaybı gibi oldukça ciddi sağlık sorunlarına da yol açabilmektedir (STM, Siber Tehdit Raporu, 2019).

Devletlerin enerji, ulaşım ve iletişim gibi kritik altyapılarının kontrolünü sağlayan sistemlerinin dijital ortamlarda gerçekleştirilmesi ise bu alanda tehdit

[1] STM Savunma Teknolojileri Mühendislik ve Ticaret A.Ş Türk Silahlı Kuvvetleri (TSK) ve Savunma Sanayii Başkanlığı'na (SSB) sistem mühendisliği, teknik destek, proje yönetimi, teknoloji transferi, lojistik destek hizmetleri; görevlerini gerçekleştirmek amacıyla Savunma Sanayii İcra Komitesi (SSİK) kararı ile 1991 yılında kurulmuştur. Detaylı bilgi için bkz. http://www.stm.com.tr

potansiyelini daha fazla artırmaktadır. Günümüzde bilişim teknolojisi sadece kamu hizmetleri bağlamında e-devlet uygulamalarıyla sınırlı değildir. Devletlerin silahlı kuvvetlerinin kullandığı ileri teknoloji savunma sistemleri, elektrik, doğal gaz ve su dağıtım şebekeleri, hava trafiği, barajlar, nükleer tesisler, demir yolu trafiği, bankacılık hizmetleri, finans sektörü ve enerji transferi gibi kritik altyapıların kontrolü merkezi denetleme kontrol ve veri toplama sistemleri (Supervisory Control and Data Aqusition Systems-SCADA Systems)[2] aracılığıyla sağlanmaktadır (Van Long Do vd., 2017). Bu sistemlere yapılacak bir siber terör saldırısı oldukça ciddi sonuçlar doğurabilecek etkilere sahiptir.

Siber uzayın gerek bireyler gerekse toplumlar arasındaki iletişimi getirdiği nokta ise son on yılda hayal edilemez seviyelere ulaşmıştır. Dolayısıyla siber terör sadece bu alanda kritik altyapılara ya da bilgi teknolojileri sistemlerine yapılacak saldırılarla kısıtlanamaz. Terör örgütlerinin propaganda, finans sağlama, eğitim ve örgütlerine yeni sempatizanlar kazandırma gibi faaliyetleri siber uzayda çok daha kolay ve masrafsız hale gelmiştir. Bu bağlamda siber terörizmin tanımı yapılırken bu tarz faaliyetlerin de tanıma dahil edilmesi elzem bir hal almıştır. Bu minvalde bir siber terörizm tanımı yapmak gerekirse siber terörizm siyasi, dini veya ideolojik bir motivasyonla yasa dışı oluşumlar ya da bireyler tarafından toplumda korku ve panik yaratan, sonuçları fiziksel bir zarara yol açabilecek potansiyele sahip, siber uzayı oluşturan bileşenlere yapılacak saldırılar ve bu bağlamda yapılan her türlü propaganda, eğitim, finans sağlama ve yeni sempatizanlar elde etme eylemleri şeklinde tanımlanabilir.

2.1.5.1. Siber Terörizm Kapsamında Değerlendirilebilecek Eylem ve Yapılanmalar

Ekonomi Barış Çalışmaları Enstitüsünün (Institute for Economy & Peace, IEP) yaşanan olaylar, can kayıpları, yaralanmalar ve ortaya çıkan zarar üzerinden yaptığı analize göre yayınladığı Küresel Terörizm İndeksi (Global Terrorism Index) listesinde 2021 yılında terörizmden en çok etkilenen ülkelerin başında Afganistan gelmektedir.

[2] SCADA sistemleri ile ilgili daha detaylı bilgi için bkz. Van Long Do, Fillatre, L., Nikiforov, I., & Willett, P. (2017). Security of SCADA systems against cyber-physical attacks. *IEEE Aerospace and Electronic Systems Magazine*, *32*(5), 28–45. https://doi.org/10.1109/MAES.2017.160047

Afganistan'dan hemen sonra ise sırayı Irak, Somali, Burkina Faso, Suriye ve Nijerya almaktadır. Türkiye ise terörizmden en çok etkilenen ülkeler listesinde 23. sırada yer almaktadır (IEP, 2022, Global Terrorism Index: 8). Bu listeye göre Türkiye terörizm riski bakımından yüksek riskli ülkeler kategorisinde yer almaktadır.

Aynı raporun elde edilen verilere göre yaptığı sıralamada ise IŞİD (Irak ve Şam İslam Devleti)[3], El Şabab, Taliban ve El Nusra örgütleri en tehlikeli ve aktif terörist organizasyonlar olarak gösterilmektedir (IEP, 2022, Global Terrorism Index: 15). Bahsi geçen bu terör grupları içerisinde Taliban ve IŞİD internet teknolojisini en aktif şekilde kullanan örgütler olarak karşımıza çıkmaktadırlar. Bu bağlamda Taliban internet ortamında oldukça ciddi oranlarda bilgi ve belge paylaşımı yapmakta ve buna ek olarak propaganda amaçlı videolar ve ses kayıtları yayınlamaktadır. Yapılan bu paylaşımlar ise Taliban tarafından kontrol edilen web siteleri aracılığıyla gerçekleştirilmektedir. Her ne kadar bu web sitelerinin kapatılması ve yayından kaldırılması noktasında ulusal ve uluslararası güçler mücadele ediyor olsa da her seferinde yeni adreslerle ortaya çıkan bu siteler Taliban örgütünün kullandığı önemli bir propaganda aracıdır. Farsça, Peştuca, Darice, Urduca, İngilizce ve Arapça yayınlar yapan Taliban sosyal medya platformlarını, forum sitelerini ve e-posta yoluyla haberleşme kaynaklarını oldukça aktif bir şekilde kullanmaktadır (Riglietti, 2017: 18).

Taliban, Facebook, Twitter ve YouTube gibi sosyal medya platformlarını bir propaganda aracı olarak kullanmakla birlikte örgüte finans sağlayacak muhtemel yatırım kaynaklarının da bu sayede dikkatini çekmeye çalışmaktadır. Sahip olduğu hesaplarla oldukça kolay ve kısa sürede milyonlarca insana ulaşabilme kapasitesine sahip olan örgüt bu hesaplar aracılığıyla daha çok dini mesajlar paylaşmaktadır. Taliban her ne kadar internet teknolojisini oldukça aktif bir şekilde kullanıyor olsa da kayıtlara geçmiş fiziksel bir zararla sonuçlanan ya da herhangi bir kayba yol açan herhangi bir siber saldırıları söz konusu değildir. Bunun yerine örgütsel olarak büyüme hedeflerini gerçekleştirmek, yapacak oldukları saldırıları koordine etmek ve daha önce de belirtildiği üzere propaganda yapmak için bilgisayar teknolojilerini aktif olarak kullanmaktadırlar (The New York Times, 2021).

[3] Bahsi geçen örgüt farklı isimlerle de anılmaktadır. Ayrıca farklı coğrafyalarda da etkinlik gösteren örgüt özellikle yabancı yazında İngilizce olarak kısaca "Islamic State" yani "İslam Devleti" şeklinde kabul görmüştür.

En tehlikeli terör örgütleri listesinde başı çeken IŞİD siber uzayı oldukça aktif bir şekilde kullanan örgütlerden bir tanesidir. İnternet ortamında gönderdikleri mesajlarda, yayınladıkları bilgi ve belgelerde ve videolarda kendilerini "Siber Halifelik" olarak tanıtan örgüt bu alanı kendilerine sempati duyan kişi ve oluşumları aynı çatı altında toplamayı hedeflemektedir. Siber uzayda örgütün çatısı altında faaliyet gösteren farklı gruplar bulunmaktadır. Birleşik Siber Halifelik (United Cyber Caliphate), Halife Ordusunun Çocukları (The Sons of Caliphate Army), Siber Halifelik Ordusu (The Cyber Caliphate Army), ve Kalaşnikof e-Güvenlik Takımı (The Kalashnikov E-Security Team) bunlardan bazılarıdır. Örgüt özellikle kendi kurdukları web siteleri, sosyal medya platformları ve forum siteleri üzerinden oldukça yoğun bir şekilde propaganda yapmaktadır. Bunlara ek olarak birçok farklı siber saldırı gerçekleştiren örgüt özellikle Amerikan devlet kurumları ve çalışanlarını hedef alarak kritik bilgileri ele geçirmeye çalışmaktadır (CCRS, 2017, Cyber Terrorism Insurance Futures: 25).

Türkiye terörizm sorunuyla uzun yıllardır mücadele eden bir ülke olarak son yıllarda siber uzayın terör örgütleri tarafından aktif bir şekilde kullanılmaya başlanması ile birlikte terörle mücadele kapsamını bu alanda da genişletmeye çalışan ve bu bağlamda önemli çalışmalar yürüten bir ülkedir. 1980'li yıllardan itibaren kendilerini kürdistan işçi partisi olarak tanımlayan terör örgütü PKK'nın (Partiya Kakeren Kurdistane) ayrım gözetmeksizin yaptığı eylemlerle mücadele eden Türkiye, son yıllarda Fettullahçı Terör Örgütü (FETÖ), IŞİD, Halk Koruma/Savunma Birlikleri (YPG)[4] ve Devrimci Halk Kurtuluş Partisi-Cephesi (DHKP-C) gibi terör örgütlerine karşı da mücadele vermektedir.

Türkiye'nin mücadele ettiği terör örgütleri de diğer örgütler gibi eylem ve faaliyetlerini siber uzayda da sürdürmektedirler. Her ne kadar bugüne kadar fiziksel olarak bir zarara yol açan bir siber terör saldırısına maruz kalınmamış olsa da bu örgütler özellikle propaganda yapmak, finans sağlamak, örgüte üye sayısını artırmak ve sempatizan toplamak, iletişim ve planlama gibi birçok faaliyeti bilgisayar teknolojilerini kullanarak gerçekleştirmektedirler. Bunun en büyük örneğini 2016

[4] YPG Türkiye tarafından ülke içerisinde faaliyet gösteren PKK terör örgütünün Suriye kolu olarak kabul edilmektedir.

yılında FETÖ tarafından gerçekleştirilen başarısız darbe girişiminden sonra ortaya çıkartılan örgüt üyelerinin haberleşme aracı olarak kendi ürettikleri kriptolanmış bir iletişim programı olan ByLock oluşturmaktadır. Örgüt üyeleri arasında iletişimin sağlanmasında kullanılan bu yazılım, darbe girişiminin planlanmasında oldukça önemli bir rol oynamıştır.

2015 yılında kendilerini Suriye Elektronik Ordusu (Syrian Elctronic Army) olarak tanımlayan bir grup tarafından bakanlıklar ve devlet kurumlarına yapılan siber saldırılarda grup saldırı düzenledikleri kurumlara ait e-posta adreslerini ele geçirdiklerini açıklamıştır (AlJazeera Turk, 2015). Ele geçirdikleri bilgilerin tamamen önemsiz ve eski bilgiler olduğu ortaya çıkmış olsa da bu durum terör örgütlerinin siber uzaydaki saldırı kabiliyetlerinin günden güne arttığını bize göstermektedir.

2018 yılında Türk Silahlı Kuvvetleri'nin (TSK) Suriye'deki PKK ve YPG hedeflerine karşı düzenlemiş olduğu Zeytin Dalı Harekâtı sırasında Rusya merkezli bir siber saldırı grubu olan Ananymous, PKK ve YPG örgütlerine destek amacıyla bir sosyal medya platformu olan Twitter'da "#OpTurkey" etiketi ile başlattığı geniş spektrumlu siber saldırılarda birçok devlet kurumunun web sitesini hedef almıştır (STM, 2018, Siber Tehdit Durum Raporu: 6-7).

2021 yılında Ankara Emniyet Müdürlüğü Terörle Mücadele Şube Müdürlüğü PKK terör örgütünün siber saldırılar gerçekleştirmek amacıyla kurmuş olduğu ve kendilerini Mezopotamya Hackers olarak tanımlayan yapılanmaya karşı yapmış olduğu operasyonlarda bu yapılanmaya ait olduğu tespit edilen 9 ayrı grubun 2020 ve 2021 yıllarında kamu kurum ve kuruluşlarının kullandıkları internet sayfaları ve tüzel kişilerin kullandıkları internet sitelerine yetkisiz erişim sağladıkları belirlenmiştir. Yapılan saldırılarda toplamda 2754 Türk kamu-özel internet sitelerine yetkisiz erişim saldırısı yaptıkları belirlenen gruba üye olduğu belirlenen 26 kişi göz altına alınarak tutuklanmıştır (AA, 2021).

2.1.6. Siber Suç

21. yüzyıl suçluları günden güne gelişen teknolojiye daha fazla güvenerek ve bu teknolojinin getirdiği imkanları kullanarak suç faaliyetlerini artan bir şekilde sürdürmeye devam etmektedirler. Bu suçlular, siber uzayın ortaya çıkarttığı ve

hayatımızın artık vazgeçilmez bir parçası olan interneti oldukça aktif bir şekilde kullanarak geleneksel anlamda işlenen suçları daha kolay bir şekilde işleyebilmektedirler. Dijital dünyanın getirdiği her türlü nimetten faydalanan suç dünyası, uyuşturucu dağıtımı, hırsızlık, evrakta sahtecilik, kişisel verilerin ele geçirilmesi, çocuk pornografisi, ticari sırların çalınması, devlete ait kritik bilgilerin ele geçirilmesi gibi suçları internet teknolojisi ile çok daha kolay ve düşük riskle gerçekleştirebilmektedir. Dolayısıyla daha derinden bakıldığında siber suçların diğer suçlara nazaran sadece ekonomik değil aynı zamanda ulusal güvenliği tehdit eden önemli bir tarafının olduğu gerçeği siber uzayda işlenen suçlarla ilgili olarak ülkelerin daha sıkı tedbirler alması gerekliliğini ortaya çıkartmaktadır.

İnternet teknolojisinin kullanımın artmasıyla birlikte ortaya çıkan siber suç olgusunun kavramsallaştırılması bu olguyla mücadelede bir gereklilik haline gelmiştir. Ancak hala oldukça yeni sayılabilecek bu olgunun kavramsallaştırılması sosyal bilimlerin tartışmalı olan diğer birçok konusu gibi oldukça karmaşıktır. Özellikle siber suç olgusunun tanımında ortaya çıkan farklılıklar ve ülkelerin hukuk sistemlerinde konuyla ilgili yapılan farklı düzenlemeler bu olgunun her kesim tarafından farklı olarak algılanmasına neden olmaktadır.

Siber suç olgusunun kavramsallaştırılmasında göz önünde bulundurulması gereken farklı ana faktörler vardır. Bunlardan bir tanesi siber uzayda işlenen bir suçun geleneksel ya da gerçek dünyada işlenen suçların dijital versiyonları olabileceğidir. Bu suçlar eğer siber uzayı oluşturan bileşenlerinden bir tanesi ile alakalı değilse geleneksel ya da gerçek dünya suçları olarak kabul edilebilir. Bu noktada özellikle hukuki yaptırımların dijital dünya ile uyum sağlaması adına ortaya çıkan zorluklar nedeniyle siber uzayda işlenen bir suç dahi olsa çoğu zaman failler yakalandığı takdirde geleneksel hukuk kurallarına göre yargılanmaktadırlar. Siber uzayda gerçekleşen suçları diğer suçlardan ayırırken göz önünde bulundurulan bir diğer önemli faktör ise suçu işleyen kişinin motivasyonun ne olduğudur. Siber uzayda işlenen bir suçun hangi motivasyonla gerçekleştiğini ayırt edebiliyor olmak bu suçun kategorize edilmesinde oldukça önemlidir. Her ne kadar bazı durumlarda siber suçlar ve diğer yasa dışı eylemlerin sorumluları benzer temellerde suçlar işliyor olsalar da suç niyetinin ve motivasyonun ne olduğunun bilinmemesi, işlenen suçun bir adi suç mu ya da başka kategoride bir suç mu olduğu değerlendirmesini yapmak noktasında

karmaşıklığa neden olmaktadır. Özellikle siber uzayda gerçekleşen yasa dışı bir faaliyetin bir siber suç mu yoksa daha önce detaylarıyla açıklanan siber terör olgusu bağlamında değerlendirildiğinde bir terör eylemi mi olduğu ayrımını yapmak bu noktada oldukça güç hale gelmektedir. Son olarak işlenen suçun niteliği de siber suç olgusunun kavramsallaştırılmasında oldukça önemli bir faktördür. Suç işleyen aktörün motivasyonuyla birlikte ele alınması gereken diğer bir olgu da işlenen suçun niteliği bağlamında suçu işleyen aktörün hangi kaynakları kullanarak bu suçu işlediği, herhangi bir oluşuma bağlı olarak ya da bireysel olarak bu suçu işleyip işlemediği konusu da oldukça önemlidir (Finklea ve Theohary, 2015).

Siber suç olgusunun uluslararası anlamda üzerine uzlaşı sağlanmış genel bir tanımı yoktur. Akademisyenler, araştırmacılar, uluslararası kuruluşlar, devletlerin hukuk sistemleri, bilişim sektöründe faaliyet gösteren birçok kuruluş bu kavramı farklı şekilde tanımlamaktadır. Dünyanın önde gelen yazılım ve bilişim şirketlerinden birisi olan bilişim alanında antivirüs programları geliştiren Kaspersky, siber suçu bir bilgisayarı, bilgisayar ağını ya da ağa bağlı bir cihazı hedef alan suç faaliyeti olarak tanımlamaktadır (Kaspersky, 2023a). Britannica sözlüğüne göre ise siber suç dolandırıcılık, çocuk pornografisi fikri mülkiyetlerin dağıtımı, kimlik hırsızlığı ya da mahremiyetin ihlali gibi yasadışı faaliyetleri gerçekleştirebilmek için bilgisayarın işlenen suçun bir enstrümanı olarak kullanıldığı suç faaliyetleri olarak tanımlamaktadır (Britannica, 2023). Yazılım güvenliği alanında faaliyet gösteren dünyanın en büyük şirketlerinden birisi olan Avast ise siber suçu bilgisayar ya da internet kullanarak yapılan tüm yasadışı aktiviteler olarak tanımlamaktadır (Avast, 2022).

Siber suç, illegal aktiviteler ve içerisinde başka amaçlar barındırmayan eğilimlerden farklı olarak daha geniş ve kapsamlı bir anlama sahiptir. Bu bağlamda siber suç kişi veya kuruluşların fayda sağlamak amacıyla bilgiyi ele geçirmesi ya da bir durumu manipüle etmek amacıyla teknolojinin bir suç aracı olarak kullanılması şeklinde tanımlanabilir (Wall, 2007: 10).

Emniyet Genel Müdürlüğü (EGM) Siber Suçlarla Mücadele Daire Başkanlığı ise siber suçu bilişim sistemlerini hedef alan ya da bu sistemlere ait bilgileri veya kullanıcılarını tehdit eden ve bilişim sistemleri kullanılarak işlenen suçlar olarak tanımlamaktadır (EGM, 2019)

Türkiye'nin de taraf olduğu ve 2001 yılında Budapeşte'de imzalanarak 2004 yılında yürürlüğe giren "Avrupa Siber Suçlar Sözleşmesi" ya da diğer adıyla "Sanal Ortamda İşlenen Suçlar Sözleşmesi" ise siber suçun tanımını oldukça geniş bir şekilde Maddi Ceza Hukuku kapsamında yapmıştır. Sözleşmenin siber uzayda işlenen suçlarla mücadelede hazırlanan ilk uluslararası sözleşme olması ve sözleşmeyi imzalayan ülkelerin kendi iç hukuklarında sözleşmenin yükümlülüklerini yerine getirecek değişiklikler yapması bakımından oldukça önemlidir. Sözleşme siber suçu *"Bilgisayar verilerinin ve sistemlerinin gizliliğine, bütünlüğüne ve erişilebilirliğine yönelik suçlar."* başlığı altında *"yasadışı erişim, yasadışı araya girme, verilere müdahale, sisteme müdahale, cihazların kötüye kullanımı, bilgisayarla bağlantılı sahtecilik, bilgisayarla bağlantılı dolandırıcılık, çocuk pornografisiyle bağlantılı suçlar, telif hakkı ve bununla bağlantılı hakların ihlaline ilişkin suçlar"* kategorileri altında incelemiştir (Council of Europe Budapest Convention, 2004). Siber suçlarla mücadele Türk Ceza Kanunun 20. Maddesinde "Bilişim Alanında Suçlar" başlığı altında asıl olarak incelenmiş olsa da kanunun diğer ilgili maddeleri Avrupa Siber Suçlar Sözleşmesi'nde bahsi geçen suçlarla alakalı önemli düzenlemelere gitmiş ve bu düzenlemeler kapsamında hukuki mücadeleye yer verilmiştir. İlgili maddeler tezin Türkiye'de siber uzayın yasal düzenlemelerini içeren diğer kısımlarında detaylı olarak incelenecektir.

Siber suç olgusunun kavramlaştırılarak üzerine uluslararası anlamda kabul görmüş bir tanımın belirlenmesi bu suçlarla mücadelede ve bu suçların geleneksel anlamda işlenen suçlardan ayrımının yapılabilmesinde oldukça önemli bir rol oynamaktadır. Lakin bunun gerekliliği konusunda da tartışmaların olduğunu belirtmek gereklidir. Finklea ve Theohary tanımın hangi amaçla yapıldığına bağlı olarak bunun değişkenlik gösterebileceğini savunmaktadırlar. Eğer siber suç olgusunun tanımının yapılmasının amacı çeşitli birçok suçun siber suç şemsiyesi altında araştırılması ve soruşturmasının yürütülmesi ise bunun öneminin çok kritik olmadığı ve işlenen spesifik suçların geleneksel anlamda işlenen suçlar ya da bir siber suç olup olmadığına bakılmaksızın tanımlarının yapılmasının daha zorunlu olduğu söylemektedirler. Diğer taraftan ise eğer devlet kurumları ve özel kuruluşlar siber suçla mücadelede strateji geliştirme yoluna gideceklerse siber suç olgusunun açık bir tanımının yapılmasının faydalı olacağını savunmaktadırlar. (Finklea ve Theohary, 2015: 16).

Siber suç olgusunun açık bir tanımının bu suçlarla mücadele eden kuruluşların izleyeceği yöntemler anlamında önemli olduğu açıktır. Dolayısıyla özellikle siber uzayı yasal olarak düzenleyen kanun maddelerinde siber suçların neler olduğu ya da geleneksel anlamda işlenen suçların bilgisayar ya da bilgisayar teknolojileri kullanılarak işlendiğinde ortaya çıkartacağı sonuçlara bağlı olarak gerekli düzenlemelerin yapılması siber uzayda gerçekleşecek olan suçlarla mücadelede elzemdir.

3. SİBER UZAYDA CAYDIRICILIK KAVRAMI

3.1. Siber Caydırıcılık Kavramı

Caydırıcılık kavramı özellikle Soğuk Savaş döneminde Amerika Birleşik Devletleri (ABD) ve Sovyetler Birliği (SSCB) arasında ortaya çıkan silahlanma yarışında bir denge unsuru olarak değerlendirilebilecek olan nükleer caydırıcılık kavramı ile oldukça önemli bir gerçeklik haline dönüşmüştür. Devletlerin siber uzayı artan bir şekilde özellikle kritik altyapıların kontrolünün sağlanması adına kullanımı ise siber caydırıcılık kavramını ortaya çıkartmıştır. Özellikle olası bir saldırı durumunda oldukça büyük sonuçlar doğurabilecek kritik altyapıların siber uzayda güvenliğinin sağlanması konusu önemli bir ulusal güvenlik konusu haline dönüşmüştür. Ulaşım, enerji, haberleşme, finans, endüstri ve sağlık sektörleri gibi kritik altyapılar olarak değerlendirilen bu alanların kontrolünün SCADA sistemleri ile gerçekleştiriliyor olması bu altyapıları potansiyel siber saldırılara açık hale getirmektedir.

Her devletin farklı bir şekilde tanımladığı kritik altyapılar genel olarak bakıldığında potansiyel bir saldırı sonucu ulusal güvenliği tehdit altında bırakabilecek, toplumun hayati ve sosyal fonksiyonlarının aksamasına neden olacak, ekonomik faaliyetlerin durma noktasına getirebilecek altyapılar olarak tanımlanabilir. ABD kritik altyapıları, çalışmalarının durması ya da yok edilmeleri halinde fiziksel veya ekonomik güvenliği veya halk sağlığını tehlikeye sokacak hayati önemi bulunan fiziksel ve sanal sistemler olarak tanımlamaktadır (Cybersecurity&Infrastructure Security Agency, CISA). Ülkemizde kritik altyapılar 2013 yılında Ulaştırma,

Denizcilik ve Haberleşme Bakanlığı'nın[5] yayınladığı 28818 sayılı tebliğde "*işlediği bilginin gizliliği, bütünlüğü veya erişilebilirliği bozulduğunda, can kaybına, büyük ölçekli ekonomik zarara, ulusal güvenlik açıklarına veya kamu düzeninin bozulmasına yol açabilecek bilişim veya endüstriyel kontrol sistemlerini barındıran altyapılar*" olarak tanımlanmıştır (Resmî Gazete, 2013). Buna ek olarak Ulaştırma ve Altyapı Bakanlığı'nın hazırlamış olduğu 2020-2023 Ulusal Siber Güvenlik Stratejisi ve Eylem Planında kritik altyapı sektörleri "Elektronik Haberleşme, Enerji, Finans, Ulaştırma, Su Yönetimi ve Kritik Kamu Hizmetleri" olarak belirlenmiştir (UAB, 2020).

Kritik altyapıların kontrolü ve işletilmesi devletlerin yönetim şekillerine bağlı olarak değişiklik göstermektedir. Bu yapılar tamamen devlet eliyle ya da tamamen özel sektör tarafından kontrol edilebildiği gibi devlet ve özel sektör iş birliğinin yapıldığı şekilde de kontrol edilebilmektedir. Serbest piyasa ekonomisi temelinde bir yönetim anlayışına sahip olan ülkemizde kritik altyapıların kontrolü ve işletimi devlet ve özel sektör iş birliği temelinde sağlanmaktadır. Kritik altyapıların siber uzaydaki güvenliğinin sağlanması devlet ve özel sektör arasında güçlü bir bilgi paylaşım sisteminin sağlanarak potansiyel tehditlerin belirlenip önceden önlem alınmasıyla sağlanabilmektedir (Ermiş, 2015: 81). Alınacak bu önlemler ve bu önlemlerin alınabilmesi için gerekli olan teknolojik altyapının ve insan gücünün oluşturulması ise siber caydırıcılık kavramının ilk adımı olarak değerlendirilebilir.

3.1.1. 21.yüzyılda Siber Tehditler Nükleer Silahların Yerini mi Alıyor?

Caydırıcılık kavramı daha önce de belirtildiği üzere soğuk Savaş döneminde ABD ve SSCB'nin giriştiği nükleer silahlanma yarışında nükleer caydırıcılık temelinde uluslararası siyasetin önemli bir konusu haline dönüşmüştür. SSCB'nin dağılmasıyla birlikte ortaya çıkan yeni dünya düzeninde nükleer caydırıcılık kavramının önemini yitirdiği söylenemez. Lakin 1962 yılında Türkiye'nin de önemli bir rol oynadığı Küba Krizi sürecinde olduğu gibi bir dehşet dengesi oluşturacak boyutlardan uzaklaştığını söylemek mümkündür. İçerisinde bulunduğumuz

[5] Ulaştırma, Denizcilik ve Haberleşme Bakanlığı'nın adı Cumhurbaşkanlığı Hükümet Sistemi'ne geçilmesiyle, 10/07/2018 tarihli ve 30474 sayılı Resmî Gazetede yayımlanan 1 No'lu Cumhurbaşkanlığı Teşkilatı Hakkında Cumhurbaşkanlığı Kararnamesi ile "Ulaştırma ve Altyapı Bakanlığı" olarak değiştirilmiştir.

21.yüzyılın ise birçok araştırmacı ve devlet adamı tarafından siber tehditler dönemi olduğu ve bu tehditlerin nükleer silahların yerini alacağı tespiti yapılmaktadır. Caydırıcılık teorisinin karşı tarafın gerçekleştirebileceği potansiyel bir saldırıyı bu saldırının oluşturabileceği sonuçlar bakımından değerlendirildiğinde başarıya ulaşma ihtimalinin olmaması ya da fayda-maliyet temelinde zararla sonuçlanabileceğini eldeki kapasitelerle saldırı gerçekleşmeden durdurmak temeline dayanmaktadır. Ayrıca oluşabilecek potansiyel bir saldırıya karşı gerçekleştirilecek misilleme kapasitesi bu noktada oldukça önem teşkil etmektedir (Mazarr, 2018: 3-7). Konvensiyonel olarak sahip olunan kapasite üzerinden devletlerin sahip olduğu caydırıcı gücün siber uzayda da sağlanıp sağlanamayacağı konusu ise halen tartışılmaktadır.

Siber caydırıcılık çalışmalarında önemli isimlerden birisi olan Libicki (2009), bu kavramı birçok farklı açıdan ele almıştır. Siber caydırıcılığın nükleer caydırıcılık ya da konvansiyonel askeri caydırıcılık olgusundan farklı olduğunu aktaran Libicki, bu farklılıkların bir politika olarak siber caydırıcılığın aleyhine çalıştığını ve bu bağlamda siber caydırıcılık kavramının oldukça problemli olabileceğini aktarmaktadır. Soğuk Savaş döneminde ortaya çıkan nükleer caydırıcılık kavramı simetriktir. Yani caydırıcılık olarak nitelendirilebilecek konvansiyonel güce kimin ne kadar sahip olduğu konusunda taraflar genellikle bilgi sahibidir. Buna bağlı olarak potansiyel bir saldırı durumunda bu saldırının fayda maliyet analizini yapmak mümkün olabilir. Saldırı gerçekleştirmeyi düşünen taraf karşı tarafın misilleme gücünü göz önünde bulundurarak ortaya çıkacak olan etkinin analizini yaptıktan sonra saldırıyı gerçekleştirme ya da durdurma kararı alabilir. Nükleer caydırıcılık, kullanıldığında karşı tarafı ve hatta insanlığı ortadan kaldırabilecek etkiler doğurabilmektedir. Siber caydırıcılık kavramı ise bu noktada nükleer caydırıcılıktan ayrılmaktadır. Siber caydırıcılıkta tehlikenin kimden geleceğini önceden kestirmek ve potansiyel bir siber saldırıya taraf olan aktörleri belirlemek mümkün olmayabilir. Siber uzay, sadece devletlerin değil, aynı zamanda devlet dışı aktörlerin ve hatta kimi zaman bireylerin kendi başına oldukça aktif olabildikleri bir ortam olarak değerlendirilebilir. Dolayısıyla ortaya çıkabilecek büyük bir siber saldırı tek bir ülkeden gelebileceği gibi herhangi bir devlet dışı aktör ya da birden fazla aktörün bir araya gelerek oluşturduğu bir oluşumdan da gelebilmektedir (Libicki, 2009: 23-39).

Soğuk Savaş dönemi boyunca ABD ve Sovyetler arasında gerçekleşen nükleer gerilim sürecinde elde edilen verilere göre siber caydırıcılık mümkün olarak görülmektedir. Bu bağlamda Libicki nükleer caydırıcılık ve siber caydırıcılık arasındaki farkları ortaya koymak adına 3 temel ve 6 destekleyici soru sormaktadır. Sorduğu ilk temel soru *"Kimin yaptığını biliyor muyuz?"* sorusudur (Libicki, 2009: 39). Özellikle caydırıcılık kavramının temelini oluşturan misilleme durumunda saldırının kimden geldiği ve misillemenin kime karşı yapılacağının bilinmesi elzemdir. Bu bağlamda değerlendirildiğinde siber uzayda gerçekleşen saldırıların kaynağının belirlenmesinin oldukça güç olması siber caydırıcılığı problematik yapan unsurlardan bir tanesi olarak değerlendirilebilir.

Libicki'nin sorduğu diğer iki temel soru ise *"Karşı tarafın varlıkları risk altında tutulabilir mi?"* ve *"Bu durum tekrarlanabilir mi?"* sorularıdır (Libicki, 2009: 39). Caydırıcılık gelebilecek potansiyel bir saldırıyı eldeki varlıkların karşı taraf harekete geçmeden durdurma etkisi yaratmasıyla mümkün olabilir. Dolayısıyla saldırı gerçekleştirme planı içerisinde olan herhangi bir taraf saldırıyı gerçekleştireceği tarafın yapacağı misilleme sonucu elindeki varlıkları riske atabilecek bir durum oluşma tehlikesini ve bu misillemeyi tekrarlayabilme kapasitesini bilirse saldırıyı harekete geçirmeden durdurabilir. Çünkü yapacağı saldırı sonucunda karşı tarafa vermeyi planladığı zararın kendisinde açacağı zarardan çok daha az olması böyle bir girişimde bulunmanın faydadan çok zarara yol açabileceğini gösterdiğinden bu riske girmenin anlamsız olacağını bilecektir. Bu bağlamda siber caydırıcılığın varlığından söz edebilmek için misilleme ve bunun tekrarını yapabilecek kapasiteye sahip olmak gereklidir.

Libicki'nin sorduğu diğer 6 destekleyici soru ise *"1. Eğer misilleme caydırıcı olmazsa en azından karşı tarafı silahsızlandırabilir mi? 2. Üçüncü taraflar çatışmaya dahil olacaklar mı? 3. Misilleme kendi tarafımıza doğru mesajı gönderir mi? 4. Vereceğimiz karşılık için bir sınırımız var mı? 5. Durumu tırmandırmaktan kaçınabilir miyiz?"* ve son olarak *"6. Saldırgan karşılık vermeye/saldırmaya değer mi?"* sorularıdır (Libicki, 2009: 39). Libicki'nin sorduğu bu sorular oluşabilecek potansiyel bir siber saldırıya karşılık verilen misilleme durumunda sorulan sorulardır. Libicki'nin bu soruları değerlendirildiğinde konvansiyonel caydırıcılık için sorulması gereken sorulardan çok da farklı olmadığı değerlendirilebilir. Lakin siber uzayda

gerçekleştirilecek bir saldırının maliyetinin konvansiyonel anlamda gerçekleştirilecek saldırılardan çok daha düşük olması ve ortaya çıkartacağı etkilerin nükleer bir saldırının ortaya çıkartabileceği etkilerden oldukça farklı olması, siber caydırıcılık kavramını farklı bir yere koymaktadır.

Libicki'ye benzer şekilde Joseph Nye (2011) siber teknoloji ile nükleer teknoloji arasında oldukça büyük farklar olduğunu vurgulamaktadır. (Nye, 2011a: 22). Nye'ın bahsettiği bu farklılıkları Libicki, bir siber sistemin zarar görmesinin ya da bağlantısının kesilmesinin bir anda ekonomileri oldukça büyük zararlara uğratabileceğini belirtmekle beraber nükleer bir saldırının ortaya çıkartabileceği etkileri vurgulamak adına büyük bir nükleer savaşın insanlığı yeniden taş devrine döndürebileceğini söylemektedir (Libicki, 2009: 48). Nükleer tehditten farklı olarak siber tehditler varlığı belli olan tehditler değillerdir. Dolayısıyla siber uzayda caydırıcılık kavramı oldukça karmaşık bir olgu olmakla birlikte sadece misillemeden ibaret değildir. Caydırıcılık olgusu ile ilgili nükleer silahlanma yarışının arttığı Soğuk Savaş döneminde ortaya çıkan görüşler bu olgunun görece basit ve nükleer bir saldırıya karşı yapılacak misillemeye bağlı olduğu üzerine kurulmuştur. Misilleme kapasitesi Soğuk Savaş boyunca caydırıcılık olgusunun temelini oluşturmuştur. Lakin daha sonraları yapılan araştırmalarda ve ortaya çıkan teorilerde caydırıcılık olgusunun özellikle gücün kullanılması bağlamında değerlendirildiğinde öngörülenden daha karmaşık bir kavram olduğu kanısına varılmıştır. Ayrıca nükleer caydırıcılık, konvensiyonel güçler, açıklayıcı politikalar, uyarı düzeyi seviyelerinin değişikliği ve kuvvet hareketleri ile desteklenmiştir (Nye, 2011a: 33).

Nye'a göre araştırmacıların caydırıcılık olgusunun nitelik bakımından siber uzayda işe yaramayacağına dair görüşleri yanlış ve oldukça basittir. Devletlerarası caydırıcılık, karşılılık ve sınırlama bağlamında değerlendirildiğinde yetersiz niteliğe rağmen hala varlığını sürdürmektedir. Kaynağı belli olmayan bir saldırı karşısında diğer hükümetler kendilerini bir anda ters etki yaratan ve birbirine bağlı ilişkilerin olduğu bir ağın içerisinde bulabilirler. Örnek olarak Soğuk Savaş döneminde ABD ve Sovyetlere bağlı olarak tek düze karşılıklı bir askeri bağımlılığın olmasına rağmen ABD, Çin ve diğer ülkeler farklı ağların içerisinde yer almışlardır. Dolayısıyla ABD ekonomisine zarar verecek büyük bir saldırıda Çin'de büyük kayıplara uğrayabilecek

bir pozisyonda bulunmuştur. Bu durum tam tersine de gerçekleşebilir (Nye, 2011a: 34).

Nye, siber uzayda gerçekleşecek olan saldırıların maliyet avantajları üzerinde önemle durmuştur. Diğer konvensiyonel güçlerin muharebe alanlarında hakimiyet sağlamaları ve kontrolü ele geçirmeleri oldukça maliyetlidir. Bunun aksine siber uzayın maliyet etkinliği göz önünde bulundurulduğunda devlet dışı aktörlerin ve konvensiyonel olarak kapasitesi düşük devletlerin de bu alanda etkili olabilmesi mümkün hale gelmektedir. Nye aynı zamanda siber uzayda üstünlüğün savunmadan çok saldırı ile gerçekleşebileceğini savunmaktadır (Nye, 2010, 2011a).

2000'li yıllar itibari ile yaşanan teknolojik gelişmeler ve internet teknolojisinin geldiği nokta daha önce de üzerinde durulduğu üzere sadece bireyleri değil aynı zamanda devletler ve devlet dışı aktörleri de siber uzayın bir parçası haline getirmiştir. Siber uzayın karmaşıklığı bu alanda gerçekleşen saldırıların tespitini oldukça zor bir hale sokmaktadır. Ayrıca bu saldırıların niteliği bakımından hangi amaçla yapıldığının belirlenmesi de bir başka zorluk olarak değerlendirilebilir. Dolayısıyla yaşanan bir saldırıda verilecek olan karşılığın saldırının kimin tarafından gerçekleştiği sorunsalı üzerinden değerlendirildiğinde ölçülülük ilkesi bağlamında durum daha da karmaşık bir hale gelmektedir. Yaşanan bir siber saldırının hangi düzeyde olduğu, saldırıyı gerçekleştiren aktörün bir devlet mi, devlet dışı bir aktör mü ya da bireysel bir saldırı olup olmadığının tespiti oldukça zor ve kimi zaman imkânsız olabilmektedir (Nye, 2010: 16). Dolayısıyla verilecek olan karşılığın niteliğini belirlemek oldukça zordur. Verilecek olan karşılık eğer ölçülülük ilkesine uymaz ya da yanlış bir tarafa verilirse bunun sonuçları savaşla sonuçlanabilecek bir çatışmaya dönüşebilir. Saldırının kim tarafından yapıldığının belirlenmesi ve kapasitesi noktasında ortaya çıkan zorluklar siber uzayda caydırıcılık kavramını oldukça karmaşık ve hassas bir durum haline sokmaktadır. Caydırıcılık kavramı potansiyel saldırganın karşı tarafın kapasite ve kabiliyetlerine bağlı olarak ortaya koyabileceği karşı misillemenin muhtemel sonuçlarından çekinmesi ile saldırıyı gerçekleştirmekten vazgeçmesi temeline dayanmaktadır. Siber uzayın belirsizliği ve karmaşık yapısı ise bu alanda caydırıcılık kavramının mümkünlüğü sorunsalını ortaya koymaktadır (Libicki, 2009: 65-67).

3.1.2. Siber Uzayın Yasal Olarak Düzenlemesi Bağlamında Caydırıcılık

Siber uzayın karmaşık yapısı devletlerin insan eliyle üretilmiş bu alanda ulusal güvenlik bağlamında caydırıcı niteliklere sahip olmasını zorlaştırmamakla birlikte aynı zamanda siber uzayın yasal olarak düzenlenmesi ile oluşturulacak bir sistemde bu alanda oluşabilecek suçların önlenmesi adına hukuki caydırıcılığın oluşturulmasını da oldukça güç bir hale getirmektedir. Hukukta caydırıcılık kavramı ceza hukukunun bir uzantısı şeklinde tartışılmaktadır. Bu konuda gerek yerli gerekse yabancı yazında birçok farklı teoriye rastlamak mümkündür. Genel olarak suçla mücadelede caydırıcılık kavramı işlenen suça karşılık verilecek cezanın niteliğiyle alakalı olarak değerlendirilmektedir. Bu noktada hukukta caydırıcılık kavramının "cezanın caydırıcılığı" olarak incelendiğini söylemek yanlış olmayacaktır. Suçla mücadelede özellikle caydırıcı cezanın ağır cezadan geçtiğini kabul eden görüşler oldukça yaygın olmakla birlikte hukukta caydırıcılık kavramı sadece cezanın ağırlığı ile ilgili değil aynı zamanda bir ülkede bulunan ceza adalet sisteminin bütünü ile alakalı olarak incelenmesi gereken bir konudur (Orhan, 2021: 65). Dolayısıyla siber uzayın yasal olarak düzenlenmesi ile bu alanda ortaya çıkabilecek suçların önlenmesi adına oluşturulacak caydırıcılık, bu alanda işlenen suçlara verilecek olan cezaların açık bir şekilde kanunlarla belirlenmesinden ve uygulanabilir olmasından geçmektedir.

Ceza adalet sisteminin işlenecek suçlara karşı önleyici ve caydırıcı nitelikte olabilmesi için kanunda açıkça belirtilmiş suçlara karşı verilecek cezaların uygulanabilirliği anlamında bazı ilkelerin olması gereklidir. Bu ilkeler cezaların kesinliği, hızlılığı ve şiddetliliğidir. Cezaların kesinliği ilkesi kanun önünde herkesin eşit bir şekilde yargılanmasını ve herhangi bir suç işlenmesi durumunda suça karşılık gelen cezanın mutlak surette er ya da geç uygulanmasını ifade etmektedir. Hızlılık ilkesi ise suç ortaya çıktıktan sonra suçluların en kısa sürede yakalanarak soruşturma, kovuşturma ve muhakeme süreçlerinin gerçekleştirilip cezanın kesinleştirilmesi anlamına gelir. Cezaların şiddetliliği ise işlenen suça bağlı olarak verilecek cezanın orantılı olmasını ifade etmektedir. Bu üç ilkenin olmaması durumunda ise cezaların caydırıcılığını yitirecektir (Dolu, Büker ve Uludağ, 2012: 72-73).

Türkiye'de ceza adalet sisteminin belkemiğini oluşturan Türk Ceza Kanunu (TCK) ise siber uzayın güvenliğinin sağlanması, bu alanda işlenecek suçların

önlenmesi bağlamında caydırıcılığın oluşturulması için en önemli düzenlemedir. Siber uzayın yasal olarak TCK'da ilk defa düzenlenmesi 1991 yılında yapılmıştır. Daha sonra 2004 yılında yapılan değişikliklerle daha kapsamlı hale gelen bu düzenleme siber uzayın hukuksal anlamda caydırıcılığını güçlendirmiştir.

2001 yılında imzalanarak 2004 yılında yürürlüğe giren ve Türkiye'nin 2010 yılında taraf olduğu Avrupa Siber Suçlar Sözleşmesi ile de Türkiye siber uzayda işlenen suçların cezaları ile ilgili bu sözleşmeye uygun olarak TCK'da önemli uyum çalışmaları yapmış ve yeni düzenlemeler getirmiştir.

3.1.2.1. Türk Ceza Kanunu'nda Caydırıcılık Bağlamında Siber Uzayın Yasal Düzenlenmesi

Türkiye siber uzayın ve bu alanın güvenliğinin sağlanmasının önemini erken fark eden ve bu anlamda yasal düzenlemeler yapan ülkelerden bir tanesidir. 1990'lı yılların başında konunun öneminin farkına varan Türkiye, siber alan ile ilgili olarak ilk defa 6 Haziran 1991 tarihinde 3756 Sayılı 756 sayılı Türk Ceza Kanunu'nun Bazı Maddelerinin Değiştirilmesine Dair Kanun ile siber uzayda işlenen suçlar bağlamında bir düzenlemeye gitmiştir. Bu kanunun 20. maddesinde "Bilişim Alanında Suçlar" başlığı altında bilgileri otomatik işleme tabi tutulmuş bir sistemden programların, verilerin veya diğer unsurların hukuka aykırı olarak ele geçirilmesi veya bunların başkasına zarar vermek üzere kullanılması, nakledilmesi veya çoğaltılması yasayla ceza unsuru olarak kabul edilmiş ve bu cezanın hükümleri düzenlenmiştir (Resmî Gazete, 1991). 2000'li yılların başına gelindiğinde ise siber uzayın kullanımının yaygınlaşması ile Türkiye siber güvenliğin sağlanması ve siber uzayda caydırıcılığın kazanılması adına daha somut ve ciddi adımlar atmaya başlamıştır.

Türkiye'de siber uzayda işlenen suçların düzenlenmesi adına oluşturulmuş tek bir kanun bulunmamaktadır. Siber uzayda bilişim alanında işlenen suçların düzenlenmesi mevcut kanunlara ilgili hükümlerin eklenmesiyle düzenlenmiştir. Bu anlamda 1991 yılında yapılan düzenlemeden çok daha kapsamlı olarak 2004 yılında siber suç kavramının kanunla tanımının yapıldığı ve "Bilişim Alanında Suçlar" başlığıyla 5237 sayılı Türk Ceza Kanunun (TCK) onuncu bölümünde bilişim sistemine girme, sistemi engelleme, bozma, verileri yok etme veya değiştirme ile banka ve kredi kartlarının kötüye kullanılması konularında düzenleme yapılmıştır. Bahsi geçen bu

düzenlemeler TCK'nın 243., 244. ve 245. maddelerinde bağımsız olarak düzenlenmiştir (5237 Sayılı TCK). Ayrıca 2001 yılında Budapeşte'de imzalanan Avrupa Siber Suçlar Sözleşmesi'nin (Budapeşte Sözleşmesi olarak da anılır) 2012 yılında Türkiye Büyük Millet Meclisi'nin (TBMM) onaylamasıyla bu sözleşmeye taraf olan Türkiye, TCK'da bu sözleşmenin hükümlerine uygun olarak düzenlemelere gitmiştir.

TCK'nın Bilişim Alanında Suçlar başlığı altında 243. maddesi bilişim sistemine girme suçunu düzenlemiştir. Bu madde uyarınca bir bilişim sisteminin bütününe ya da bir kısmına hukuka aykırı olarak giren kişiler hakkında bir yıla kadar hapis ya da adli para cezası uygulanması hükme bağlanmıştır. Yine aynı maddenin ikinci fıkrasında ise birinci fıkrada tanımlanan eylemlerin bedeli karşılığı yararlanılabilen sistemler hakkında işlenmesi halinde verilecek ceza yarı oranında indirilir denilmiştir. Son olarak üçüncü fıkrada ise bu eylem nedeniyle sistemin içerdiği verilerin yok olması ya da değişmesi durumunda altı aydan iki yıla kadar hapis cezası öngörülmüştür (5237 sayılı TCK, Md. 243).

TCK'nın 244. Maddesi ise sistemi engelleme, bozma verileri yok etme veya değiştirme suçlarını ele almıştır. Bu madde 243. Maddeye kıyasla daha detaylı bir şekilde bir bilişim sistemini engelleme suçunu işlemiştir. Türk Ceza Kanunu'nun 244. maddesinde sistemi engelleme, bozma, verileri yok etme veya değiştirme suçu düzenlenmiştir. Bu suç tipinin düzenlenmesindeki amaç ise daha önce bahsi geçen Avrupa Siber Suçlar Sözleşmesi'nin (2001) 4. Maddesinde öngörülen "verilere müdahale" ve 5. maddesinde öngörülen "sisteme müdahale" düzenlemelerine uyum sağlamaktır.

TCK'nın 245. maddesinde banka veya kredi kartlarının kötüye kullanılması suçu düzenlenmiştir. Bu maddeye göre banka ve kredi kartlarının kötüye kullanılması eylemleri bağımsız bir suç tipi olarak düzenlenmekle beraber bu yolla bankaların veya bu bankaların müşterilerinin zarara sokulmasının ve çıkar sağlanmasının engellenmesi amaçlanmıştır (BTK, 2017). Bu maddeye göre bir başkasına ait olan banka veya kredi kartını kart sahibinin ya da kartın kendisine verilmesi gereken kişinin rızası olmadan bunu kullanarak fayda sağlaması halinde üç yıldan altı yıla kadar hapis ve beş bin güne kadar adli para cezası ile cezalandırılır hükmü yer almaktadır. Sahte banka hesapları

kullanarak kredi kartı üreten, satan, devreden, satın alana veya kabul eden kişilere ise üç yıldan yedi yıla kadar hapis ve on bin güne kadar adli para cezası öngörülmüştür. Yine maddenin üçüncü fıkrasında ise sahte olan bir banka veya kredi kartının kullanılarak fayda elde edilmesi durumunda bu fiilin daha ağır bir cezayı gerektiren başka bir suç oluşturmaması durumunda ise dört yıldan sekiz yıla kadar hapis ve beş bin güne kadar adli para cezası öngörülmüştür (5237 sayılı TCK, Md. 245). TCK'nın ilgili bu maddesi Budapeşte Sözleşmesi'nin siber suçlar kısmının *"Bilgisayarla bağlantılı sahtecilik"* (Md.7) ve *"Bilgisayarla bağlantılı dolandırıcılık"* (Md.8) kısımlarına da uyum sağlamaktadır (Council of Europe Budapest Convention, 2004).

Siber uzayın güvenliğinin sağlanması adına maddi ceza hukuku bağlamında yapılan düzenlemeler ve ilgili maddeler TCK'da sadece "Bilişim Alanında Suçlar" başlığı altında düzenlenmemiştir. Her ne kadar bilişim alanında işlenen suçlara dair özel düzenlemeler olarak kabul edilmese de TCK birçok farklı konuda işlenen suçların bilişim teknolojileri kullanarak ya da aracılığıyla işlenmesi durumunu ele almıştır. Özellikle Budapeşte Sözleşmesi'nin imzalanarak yürürlüğe girmesi ve dolayısıyla bir uluslararası sözleşmeden doğan yükümlülükler bağlamında iç hukukta yani TCK'da yapılan uyum çalışmaları, geleneksel ya da gerçek dünya suçlarının bilişim teknolojileri kullanarak ya da bu teknolojiler aracılığıyla da işlenebileceği gerçeğini taahuk ederek ilgili maddelerde düzenlemelere gitmiştir. TCK'da caydırıcılık bağlamında bilişim teknolojileri kullanarak ya da bu teknolojiler aracılığıyla işlenen suçlarla ilişkilendirilen ya da ilişkilendirilebilecek maddeler "Md. 123/A Israrlı Takip, Md. 124 Haberleşmenin Engellenmesi, Md. 132 Haberleşmenin Gizliliğini İhlal, Md. 133 Kişiler Arasındaki Konuşmaların Dinlenmesi ve Kayda Alınması, Md. 134 Özel Hayatın Gizliliğini İhlal, Md. 135 Kişisel Verilerin Kaydedilmesi, Md. 136 Verileri Hukuka Aykırı Olarak Verme veya Ele Geçirme, Md. 142/2-e Nitelikli Hırsızlık, Md. 157 ve 158/1-f Dolandırıcılık ve Nitelikli Dolandırıcılık, Md. 213-218 Kamu Barışına Karşı Suçlar, Md. 226 Müstehcenlik, Md. 228 Kumar Oynanması İçin Yer ve İmkân Sağlama, Md. 299-301 Devletin Egemenlik Alametlerine ve Organlarının Saygınlığına Karşı Suçlar, Md. 326-339 Devlet Sırlarına Karşı Suçlar ve Casusluk" maddeleridir. İlgili maddeler bu çalışmanın üçüncü bölümünde "Türk Ceza Kanunu'nda Bilişim Teknolojileri Kullanarak veya Bu Teknolojiler Aracılığıyla İşlenen Suçlarla İlişkilendirilen ya da İlişkilendirilebilecek Maddeler" alt başlığı

altında detaylı bir şekilde inceleneceği için tekrara düşmemek adına bu kısımda detaylarıyla belirtilmemiştir.

4. SİBER SAVAŞ VE SİBER SAVUNMA

4.1. Siber Savaş Kavramı

2007 yılında Estonya'ya karşı gerçekleştirilen büyük çaplı siber saldırılar sonrasında siber savaş olgusuna olan ilgi ve bu konuda yapılan çalışmalar gerek akademik araştırmalar düzeyinde gerekse de devletlerin bu konuda yaptığı çalışmalar ve aldığı önlemler boyutunda büyük oranda artmıştır. Gerçekleşen bu saldırıda faillerin tam olarak kim olduğu ve saldırıların nereden geldiği hiçbir zaman tam olarak belirlenmemiş olsa da bu saldırıların Rusya tarafından gerçekleştirildiği öne sürülmüştür (Boulos, 2017: 231). Üç hafta boyunca süren saldırılar, cumhurbaşkanlığı, meclis, bakanlıklar, siyasi partiler, ülkenin büyük gazeteleri, bankalar ve bakanlıklar arasında iletişimi sağlayan sistemleri kontrol eden şirketlerin web siteleri ve sistemlerini kullanılamaz hale getirmiş ve tam anlamıyla ülkede dijital bir krize neden olmuştur (The Guardian, 2007). Estonya'ya karşı gerçekleştirilen oldukça büyük çaplı bu saldırı, ülkede birçok hizmetin aksamasına ve kurumlar arasında haberleşmenin neredeyse tamamen durmasına neden olmuştur. Bu saldırılardan hemen bir sene sonra yine Rusya tarafından Gürcistan'a gerçekleştirilen siber saldırılar Estonya'dakine benzer etkiler doğurmuştur (Healy ve Jordan, 2014: 2). 2010 yılında ise ABD tarafından İsrail'in de yardım ettiği öne sürülen ve İran'ın İsfahan kenti yakınlarında bulunan Natanz nükleer tesisine karşı gerçekleştirilen siber saldırının tesisin uranyum zenginleştirme faaliyetlerini durdurduğu ve hatta reaktörlerin kontrolden çıkarak tehlikeli bir şekilde çalışmasına neden olduğu ileri sürülmüştür. Saldırı Stuxnet isimli bir virüs ile gerçekleştirilmiş ve literatüre "Stuxnet Saldırısı" olarak geçmiştir (Singer ve Friedman, 2014: 116).

Bahsi geçen saldırılara benzer türde birçok siber saldırı dünyanın farklı coğrafyalarında ve farklı boyutlarda gerçekleşmeye devam etmektedir. 2007 yılında Estonya'da gerçekleşen siber saldırılardan günümüze benzer boyutlarda yüzlerce siber saldırı gerçekleşmiştir. Bu saldırılar sadece ülkelerin dijital sistemlerini hedef almakla kalmamış aynı zamanda Birleşmiş Milletler (BM), Avrupa Birliği (AB) ve NATO gibi

uluslararası ve uluslar üstü kuruluşları da hedef alan saldırılar şeklinde gerçekleşmiştir (CFR, 2023). Gerçekleşen bu tarz kolektif saldırılarla birlikte önemini artıran siber savaş kavramı, ülkelerin savaşa girme ve yürütme şekillerini etkileyerek savaş alanında potansiyel olarak daha geniş kapsamlı sonuçlara maruz kalmalarını sağlayabileceği gerçeğini ortaya çıkartması bağlamında giderek ulusal güvenliğe yönelik en önemli tehditlerden birisi haline gelmeye başlamıştır. 21. yüzyılda siber uzayın harbin beşinci boyutu haline gelmesiyle ve dijital savaş alanlarının daha da yaygınlaşmasıyla siber saldırılar daha güçlü, daha karmaşık ve sürekli genişleyen bir dijital ortamda konuşlandırılabilir hale gelmeye başlamıştır. Teknoloji geliştikçe siber saldırganlar siber uzayda gerçekleştirecekleri saldırıları daha hassas bir şekilde gerçekleştirme, saldırıları öngörme ve önleme yeteneklerini geliştirmeye devam etmektedirler. Bu bağlamda özellikle siber savaş operasyonları değerlendirildiğinde kötü amaçlı bir yazılımın bilgisayar sistemlerine zarar vermek veya kesintiye uğratmak amacıyla kasıtlı olarak kullanılması nedeniyle diğer siber tabanlı faaliyet biçimlerinden farklı olduğu söylenebilir (Green, 2015).

Siber güç artık modern savaşın temel bir bileşeni olarak karşımıza çıkmaktadır. Günümüzde gerçekleşen savaşlarda ve gelecekteki savaşlarda başarı, siber gücü kara, hava, deniz ve uzay alanlarındaki geleneksel güçle birleştirilmesiyle mümkün olacaktır. Siber gücü daha iyi kullanmak ve konvansiyonel güçle birleşimini sağlamak için öncelikle siber güç ile konvansiyonel anlamda devletlerin sahip olması gereken zorunlu güç arasındaki benzerlikleri ve farklılıkları, siber gücün kendine mahsus özelliklerini ve şu anda neler yapıp yapamayacağını anlamak oldukça önemlidir.

Siber savaş hem saldırı hem de savunma tedbirlerini içermektedir ve bu tedbirler devletler ve devlet dışı aktörler tarafından sivil altyapılar ve askeri ağları hedef almaktadırlar. Daha önce de bahsi geçen kritik altyapılara karşı yapılan saldırılar ya da askeri ağlara düzenlenecek saldırılar siber savaş kapsamında değerlendirilebilecek türden saldırılardır. Örneğin karadan karaya ya da havadan karaya atılan akıllı füzeleri kontrol eden sistemlere ya da insansız hava araçlarını kontrol eden sistemlere yapılacak bir siber saldırı ile bu sistemlerin kontrolünün ele geçirilmesi mümkündür. Ayrıca bir ülkenin savaş stratejilerini ele geçirmek için yapılacak bir siber saldırı ulusal güvenliği tehdit edecek oldukça önemli sonuçlar doğurabilir. Ek olarak siber savaş kavramı sadece bilişim sistemlerine yapılacak siber

saldırılar kapsamında değerlendirilmemelidir. Siber uzay, konvansiyonel anlamda değerlendirilebilecek savaşlarda kara, hava ve deniz muharebe alanlarında devam eden savaşın bir parçası olarak propaganda yapma, kamuoyu oluşturma ya da iki ülke arasında devam eden çatışmaları besleyecek faaliyetler gerçekleştirme anlamında da önemlidir (Gonzales, 2015: 63).

Siber savaş kavramının sosyal bilimlerde diğer birçok kavramda olduğu gibi genel kabul görmüş bir tanımı olmadığı için bu kavram dijital siber dünyada gerçekleşen olay ve eylemleri anlatmak için oldukça serbest bir şekilde kullanılmaktadır. Siber savaş kavramı 2008 ve 2010 yılları arasında, özellikle 2007 yılında Estonya'ya karşı gerçekleştirilen siber saldırılar sonrasında, oldukça popüler hale gelmiştir. Daha önce internet kullanımının doksanlı yıllarda artmaya başlamasıyla ortaya çıkan "bilgi savaşı" kavramı, yerini kısmen de olsa siber savaş kavramına bırakmaya başlamıştır. Siber savaş, sanal dünyada yürütülen savaş olarak algılanmasının yanında konvansiyonel anlamda güç kullanımını içeren geleneksel savaş kavramının bir yansıması olarak da değerlendirilmektedir. Birçok araştırmacıya göre siber savaş kavramının tanımı, siber operasyonların biçimlerinden ziyade, savaşın amaçlarını ve motivasyonun ne olduğunu içermelidir (Lehto, 2018: 3). Bu bağlamda özellikle ülkelerin siber güç kapasitelerini artırmasıyla birlikte ortaya çıkan siber çatışmaların siber savaş kavramı çatısı altında anlaşılması gerekmektedir.

Siber çatışmalar geleneksel anlamdaki silahlı çatışmalardan farklı olarak kendine özgü bazı karakteristik özelliklere sahiptir. Siber çatışmalarda konvansiyonel güçler olan tanklar, gemiler, savaş uçakları ve füzeler gibi geleneksel silahlar yerine yazılım ve donanım kapasitelerinden oluşan bilgi ve iletişim teknolojileri yani siber güç olarak tanımlanabilecek kapasiteler kullanılmaktadır (Chen ve Dinerman, 2018: 23). Siber güç, siber uzayda elektronik ağlarla birbirine bağlı bilgi kaynaklarının kullanımı yoluyla istenilen sonuçları elde etme yeteneğidir (Nye, 2010). Dolayısıyla siber gücün kullanıldığı çatışmalar geleneksel çatışmalardan farklı olsa da elde edilmeye çalışılan sonuç aynı olabilir. Bir başka deyişle, siber çatışmaların amacı konvansiyonel çatışmalarda olduğu gibi bir ülkenin ulusal çıkarlarını korumak ya da elde etmek amacıyla karşı tarafı zorlamaya yönelik her türlü eylemi kullanmaktır (Van Houten, 2010). Bu bağlamda siber güç kapasitesi bilgisayar ve bilgisayar ağlarında veya bilgisayarlarda ve ağların kendilerinde bulunan bilgileri kullanım dışı bırakma,

yok etme, manipüle etme veya ele geçirme ile ilişkilendirilmektedir (Schaap, 2009). Geleneksel anlamda fiziksel sınırların olmadığı siber uzayda konvansiyonel çatışmalardan farklı olarak karşı iki taraf aynı coğrafi alanda operasyonel kabiliyetlerini sergileyebilmektedir (Andress ve Winterfeld, 2014). Lakin siber uzayda ortaya çıkan çatışmalar geleneksel savaş alanlarından oldukça farklıdır. Bir muharebe alanı olarak siber uzay hem mantıksal hem de aynı zamanda fiziksel, çoğunlukla özel sektörün sahip olup kontrol ettiği ve kullandığı, taktik olarak hızlı fakat operasyonel olarak yavaş, saldırı kabiliyetlerinin genellikle savunmaya hâkim olduğu ve belirsizliklerle dolu bir alandır (Rattray ve Heaey, 2010). Dolayısıyla siber uzayda gerçekleşen çatışmalar geleneksel savaş alanlarında gerçekleşen çatışmalardan birçok farklı alanda farklılık gösterebilmektedir.

Tablo 1.
Geleneksel çatışmalar ve siber çatışmaların farkları

	Geleneksel çatışmalar	**Siber çatışmalar**
Amaç	Belirli bir süre için coğrafi konum hakimiyeti yoluyla siyasi, ekonomik, ideolojik, sosyal ve dini hakimiyet elde etme	Siyasi, ekonomik, ideolojik, sosyal ve dini hakimiyet kazanmaya yardımcı olmak; rekabet avantajı için bilgi edinme
Strateji	Açık operasyonlar ve/veya gizli operasyonlar kullanmak suretiyle güç göstermek; nitelik sorunu düşük	Açık operasyonlar ve/veya gizli operasyonlar kullanmak; nitelik sorunu var
Müdahillik	Askeri veya yarı askeri personel	Etkilenen ağlara bağlı bir cihazı olan herkes
Hedefler	İnsanlar ve insan hayatını doğrudan etkileyen somut her şey	Temel olarak bilgi gibi maddi olmayan öğeler veya bilgi sistemleri gibi somut öğeler; siber-fiziksel durumlarda insan hayatını dolaylı olarak etkileyebilir
Alan	Sınırlı coğrafya	Dijital bir ağa bağlı olduğu sürece fiziksel sınırlar yok
Süre	Sınırlı bir zaman	Devam eden (lakin siber saldırılar genellikle kısa bir süre içinde gerçekleşmektedir)

Tablo 1. *(Devamı)*

Hazırlık süreci	Uzun	Nispeten kısa
Maliyet	Oldukça yüksek	Nispeten daha az
Karakteristik özellikler	Daha şeffaf	Karmaşık ve anlaşılmaz
Nitelik	Kolayca tespit edilebilir	Tespit edilmesi zor
Angajman kuralları	Açık	Net değil
Etki	Her zaman yıkıcı ve açık, hissedilebilir	Daha az yıkıcı ve kimi zaman etkileri hissedilmeyen
Yıkım (zarar)	Fiziksel yıkım ve kayıp	Bilgi kaybı
Etki alanı (kişi,kurum, kuruluş vs.)	Sınırlı sayıda insan veya kuruluş	Ağlara bağlı herkes ve tüm kuruluşlar
Etki alanı (coğrafi)	Fiziksel coğrafya	Ağ bağlantıları
Caydırıcılık	Açık, güçlü ve elde edilebilir	Sınırlı ve elde edilmesi zor
Sonuç ve kazanım	Açık	Net değil
Kazanan	Tespit edilmesi kolay, açık	Net değil
Toparlanma ve iyileşme süreci	Uzun	Nispeten daha kısa

Kaynak: Chen ve Dinerman, 2018: 26

I. Dünya Savaşıyla birlikte başlayan ülkelerin silahlanma yarışı teknolojinin gelişmesine ayak uyduracak biçimde ilerlemiştir. İkinci Dünya Savaşı ve sonrasında doksanlı yılların başlarına kadar devam eden Soğuk Savaş sürecinde ise nükleer silahlanma yarışına ek olarak ülkeler konvansiyonel silahları teknolojiyle bütünleştirerek daha etkili ve kullanışlı hale getirmeye başlamışlardır. 21. yüzyılda ülkelerin silahlı kuvvetlerinin bel kemiğini oluşturan hava kuvvetleri, radarlar, uzun menzilli akıllı füzeler, insansız hava ve deniz araçları, denizaltılar ve savaş gemileri

gibi tüm teçhizatların kontrolü her ne kadar insan unsuru gerekli olsa da bilgisayar teknolojileri ile gerçekleştirilmektedir. Tüm bu unsurların kontrolünü sağlayan bilgisayar teknolojileri ise çoğunlukla bir ağa bağlı şekilde çalışarak silahlı kuvvetlerin uzun mesafelerde personel tehlikesi olmadan operasyonlarını yürütebilme kabiliyetine sahip olmasını sağlamaktadır. Dolayısıyla bu unsurların kontrolünün gerçekleştirilecek bir siber saldırıyla devre dışı bırakılması ya da kontrol altına alınması oldukça büyük bir güvenlik zafiyeti sağlayabilecek potansiyelde bir tehlike olarak değerlendirilebilir. 2011 yılında İran ABD'ye ait RQ-170 Sentinel[6] tipi 6 milyon dolar değerindeki bir insansız casus hava aracının sistemlerine girerek Kızıl Deniz'in üstünde kontrolünü ele geçirmiş ve kendi topraklarına indirmeyi başarmıştır. İnsansız hava aracının istihbarat faaliyetlerinde bulunduğu ve tüm sistemlerinin ele geçirilerek teknolojisinin kopyalandığı iddia edilmiştir (CNN International, 2014). ABD'nin ciddi prestij kaybına ve oldukça önemli bir teknolojisini kaybetmesine neden olan bu olay, siber uzayın güvenliğinin ne kadar önemli olduğunu özellikle ülkelerin silahlı kuvvetlerinin gerçekleştireceği operasyonlar bağlamında tekrar kanıtlamıştır. Dolayısıyla, aslında siber savaş kavramını geleneksel savaş kavramından ayırmak çok da mümkün değildir. Bu bağlamda ülkelerin siber güç kabiliyetlerini geliştirme faaliyetleri konvansiyonel anlamda silahlı kuvvetlerinin güçleriyle birlikte değerlendirilmelidir.

Siber savaş kavramının en tartışmalı konularından bir tanesi ise siber uzayda gerçekleşen bir saldırının ya da saldırılar bütünün *casus belli* yani savaş sebebi kapsamında değerlendirilip değerlendirilemeyeceği konusudur. Eğer gerçekleştirilen bu saldırı bir savaş sebebi olarak değerlendirilirse verilecek olan cevap milletlerarası hukukta bulunan mütekabiliyet ilkesi kapsamında mı gerçekleşecek yoksa konvansiyonel silahların da kullanıldığı daha geniş anlamda bir savaş mı olacak soruları hala tam anlamıyla cevap bulunamayan sorulardır.

Dünyanın en güçlü askeri ittifakı olan NATO, siber uzayın güvenliği konusunu ilk defa 2002 yılında ele almış ve 2016 yılında gerçekleşen Varşova Zirvesinde ise

[6] RQ-170 Sentinel ABD Hava Kuvvetleri tarafından kullanılan ve Lockheed Martin firması tarafından üretilen insansız bir istihbarat hava aracıdır. Daha fazla bilgi için bkz. https://www.af.mil/About-Us/Fact-Sheets/Display/Article/2796993/rq-170-sentinel/

siber uzay NATO'nun kara, hava ve denizden sonra dördüncü muharebe alanı olarak birlik üyesi ülkeler tarafından kabul edilmiştir (NATO/Varşova Zirvesi, 2016). Ayrıca NATO'nun kurucu anlaşmasına göre üye ülkelerden birisinin ulusal güvenliğine yapılan bir saldırı sonucu ittifak üyesi ülkelerin saldırıya uğrayan ülkenin yanında yer alacağını bildiren 5. maddenin bir siber saldırı sonucunda devreye sokulabileceği sonucuna da varmak mümkündür.

Siber savaş konusu ile alakalı olarak uluslararası hukukun uygulanabilirliği konusu özellikle 2007 yılında Estonya'ya karşı gerçekleştirilen siber saldırılar sonrasında artan bir şekilde ilgi kazanmaya başlamış ve bu noktada NATO Müşterek Siber Savunma Mükemmeliyet Merkezi (CCDCoE) 2008 yılında Estonya'nın başkentinde kurularak ittifakın siber savunma kapasitesini artırma amacıyla çalışmalarına başlamıştır (CCDCoE, 2023). Merkez kapsamında 2009 yılında başlayan ve uluslararası hukukun siber saldırılara hangi koşullar altında ve sebeplerle savaşa girme ve güç kullanma konularını ele alan *Jus ad bellum* prensibinin uygulanabilirliği noktasında uluslararası hukuk alanında uzmanlaşmış yirmi akademisyenin üç yıl boyunca yaptığı çalışmalar sonucunda *"The Talinn Manual on the International Law Applicable to Cyber Warfare"* isimli bir çalışma ortaya çıkmıştır (Boulos, 2017: 231-233). Çalışma siber uzayda güç kullanımının uluslararası hukuk bağlamında yapılan en kapsamlı değerlendirmesi ve kurallar bütünü olarak değerlendirilebilir.

Talinn Manual bir pozitif hukuk çalışması olarak mevcut uluslararası hukuk kuralları üzerine yoğunlaşarak siber uzayda ortaya çıkabilecek çatışmalarda ya da siber saldırılar sonucunda ortaya çıkan durumlarda siber savaş konusu üzerine bir kurallar bütünü oluşturmaktadır. Her ne kadar bağlayıcılığı olmasa da siber savaş kavramının yasal olarak düzenlenmesi adına özellikle gelecekte çıkabilecek bir siber savaş durumunu ele alması bakımından önemli bir çalışma olarak değerlendirilebilir. Çalışmayı hazırlayanlar, diğer birçok araştırmacının aksine uluslararası hukukun genel ilkelerinin siber savaşa uygulanamayacağı ve bu nedenle yeni bir antlaşma hukukuna ihtiyaç olduğu varsayımını açıkça çürütmektedir. Ayrıca çatışmalarda kuvvet kullanımını düzenleyen uluslararası hukuk kuralları ile çatışan taraflar arasında çatışmanın hangi şartlarda yürütülmesi gerektiğini düzenleyen uluslararası hukuk kuralları arasında açık bir ayrım yapmakla birlikte egemenlik, devlet sorumluluğu ve

tarafsızlık yasası gibi konular da ele alınmıştır (Schmitt ve Vihul, 2017). Talinn Manual uluslararası bağlayıcılığı olmayan bir belge olmasına ve sadece bu çalışmayı hazırlayanların görüşlerini yansıtmasına rağmen, siber savaş kavramını uluslararası hukuk perspektifinden ele almaya yönelik ilk ciddi girişim olması bakımından önemlidir.

4.2. Siber Savunma

21. yüzyıl itibari ile ülkelerin ulusal savunma politikaları içerisinde siber savunma politikaları, günümüzde yürütülen ve üzerine oldukça büyük önem verilen en önemli savunma konularından birisidir. Siber savunma politikaları hem mevcut olan hem de potansiyel olarak karşılaşılabilecek simetrik ve asimetrik tehditlere ulusal ve uluslararası zeminde aynı zamanda karşı koymayı amaçlamaktadır. Her devlet kendi ulusal güvenlik tedbirleri kapsamında olası siber tehditlere karşı bir siber savunma politikası ve stratejisi geliştirme çabası içerisindedir. Günümüzde bu çabayı sadece devletler değil aynı zamanda uluslararası örgütler, büyük şirketler ve kuruluşlar ve hatta münferit olarak bireyler de göstermektedir. İçerisinde bulunduğumuz yüzyılda siber savunma en önemli güvenlik sorunları arasında yer almaktadır. Siber güvenlik, basit bir bilgisayar, internet bağlantısı veya akıllı telefonların güvenliğinin sağlanmasından, elektrik dağıtım şebekeleri, barajlar, nükleer tesisler, sanayi üretimi, insansız hava araçlarının kontrolüne kadar birçok farklı alanda güvenliğin tesis edilmesi bağlamında hayati öneme sahiptir. Teknolojinin durdurulamaz gelişimi ve internet teknolojisinin artık hayatın vazgeçilmez bir parçası olduğu günümüzde dünya, elektronik anlamda hiç olmadığı kadar birbirine bağlı bir hale gelmiştir. Bu nedenle, mevcut tehditlere ve gelecekte ortaya çıkabilecek olası tehditlere karşı siber savunma için yeni yöntemler ve eylemler geliştirmeye yönelik artan bir ihtiyacın olduğu gerçeği devletler tarafından kabul edilmektedir.

Siber uzayın toplumlar ve devlet ekonomileri için giderek daha merkezi bir hale geliyor olması yeni fırsatların ortaya çıkmasına ek olarak devletlerin baş etmek zorunda oldukları yeni güvenlik tehditlerini de beraberinde getirmiştir. Siber tehditler, organize suç örgütleri, suçlular, yabancı hükümetler ve terörist gruplar gibi farklı aktörler tarafından siber uzayı da içerecek şekilde insan yapımı her sistemin doğasında var olan güvenlik açıklarının istismar edilmesiyle ortaya çıkmaktadırlar. Özellikle

yabancı hükümetler ve terörist örgütlerin siber uzayın açıklarını kullanarak istismar etmesi suretiyle ortaya çıkan güvenlik tehditleri ise ulusal güvenlikle yakından alakalıdır.

Siber uzayın hayatın her noktasına tezahür etmesiyle birlikte teknoloji olmadan yaşamak neredeyse imkânsız hale gelmiştir. Özellikle Covid19 pandemisi sürecinde hayatın tam anlamıyla dijitalleşmesi, birçok kurum ve kuruluşun uzaktan çalışma prensibiyle yönetilir hale gelmesi ve bunun mümkün olduğunun görülmesi siber uzayı daha fazla kullanılan bir alan haline getirmiştir. Devletler ve özel şirketler siber uzaya daha bağlı bir hale gelmişlerdir. E-devlet, internet bankacılığı, e-sağlık, uzaktan eğitim, enerji dağıtımı, hava trafik kontrol ve diğer birçok temel hizmetlere kadar uzanan hizmetlerin tamamı siber altyapıya bağlı olarak internet altyapısıyla işlemektedir. Bazı ülkelerde siber uzayın ana bileşeni olan internet, gayri safi yurtiçi hasılaya gözle görülür miktarda katkıda bulunmaktadır. 2022 yılında küresel gayri safi yurt içi hasılanın %60'ını internet teknolojilerine bağlı olarak çalışan iletişim teknolojileri oluşturmuştur (IMF, 2022).

Siber uzayda ulusal güvenliğe karşı mevcut tehditlerin oldukça farkında olan devletler, kurumlar ve uluslararası örgütler, ortaya çıkabilecek siber saldırıları önlemek, caydırmak ve bu saldırılara karşı savunma yapmak amacıyla birçok farklı tedbir almaktadır. Türkiye'de dahil olmak üzere birçok devlet silahlı kuvvetler bünyesinde siber savunma komutanlıkları oluşturmuş, birçok devlet kurumu siber güvenlik birimleri kurmuş ve tüm bunlara ek olarak siber uzayın güvenliğinin sağlanmasında gerekli olan yetişmiş insan gücü ihtiyacını karşılamak üzere siber güvenlik akademileri, üniversiteler bünyesinde lisans ve lisans üstü programlar kurulmaya başlanmıştır. Devletler bunları yaparken sadece siber uzayda güvenliğin sağlanmasını amaçlamamaktadırlar. Siber uzayın bir bileşeni olan internet teknolojisinin ülkelerin ekonomilerindeki payı düşünüldüğünde tüm bu eylem ve önlemler ile ülkeler ulusal güvenliği iyileştirme, kritik altyapıların modernizasyonunun sağlanması ve güvenliğin tesis edilmesi, bilgi güvenliği ve paylaşımının sağlanması, ifade özgürlüğünün tesis edilmesi gibi konular amaçlanmaktadır (Schmitt ve Vihul, 2017: 118). NATO'nun hazırlamış olduğu ve siber uzayın güvenliğinin tesis edilmesi noktasında bir kurallar bütünü olarak

değerlendirilebilecek Talinn Manual, bahsi geçen bu konuları siber uzayın güvenliğinin sağlanmasındaki ikilemler olarak tanımlamaktadır.

Siber uzayın sağlamış olduğu ekonomik, teknolojik, politik ve sosyal avantajlar, bu alanın güvenli, savunabilir ve erişebilir olmasıyla doğru orantılıdır. Eğer bu üç faktörden herhangi birisi risk altında ise savunma noktasında tehditlerin ortaya çıkması kaçınılmazdır. Dolayısıyla siber uzayı oluşturan ana altyapının güvenliği ve bütünlüğü devletler açısından öncelikli ulusal güvenlik konuları içerisinde yer almaktadır (Hathaway ve Klimburg, 2012).

Siber uzayın ülkelerin ekonomilerinde, güvenliklerinde ve toplum içerisinde rolünün durdurulamaz artışı yeni fırsatlarla birlikte ülkelerin başa çıkmakla zorunlu oldukları yeni güvenlik tehditlerini de beraberinde getirmiştir. Siber uzayda tehdit oluşturan aktörler farklı kategoriler içerisinde anılmaktadır. Bunların en bilinenleri ise örgütlü suçlular (organize suç örgütleri), hektivistler (hacktivists), devletler ve terörist organizasyonlardır (Nikitakos ve Mavropoulos, 2014: 262). Bahsi geçen kategorilere aynı zamanda münferit olarak kişileri eklemek yanlış olmayacaktır. Günümüzde şahıslar bireysel olarak siber uzayın bir aktörü konumundadırlar. Yeterli donanıma sahip ve internet bağlantısına erişimi olan her birey potansiyel olarak siber uzayda bir tehdit unsuru sayılabilmektedir.

Organize suç örgütleri geleneksel olarak yürüttükleri suç faaliyetlerini siber uzayın getirmiş olduğu yenilik ve kolaylıklarla daha da geliştirmiş ve bu faaliyetleri dijital ortama da aktarmıştır. Kredi kartı hırsızlığı, kişisel verilerin ele geçirilmesi, kumar oynatılması ve bunun için alan sağlanması gibi birçok farklı suç dalını içerisine alacak yelpazedeki illegal aktiviteler siber uzayın karmaşık yapısı içerisinde suç örgütleri için daha az riskli ve daha az maliyetli olarak sürdürülmektedir. Bir siber güvenlik sorunu olarak değerlendirilebilecek bu faaliyetler aynı zamanda siber savunma kapsamında da değerlendirilmesi gereken türden aktivitelerdir. Ülkeler bu tip faaliyetlerin engellenmesi adına caydırıcı nitelikte yasal düzenlemeler yapmakla birlikte özellikle kolluk kuvvetleri kuruluşları çatısı altında siber suçlarla mücadele birimleri oluşturmaktadır. Türkiye'de İçişleri Bakanlığı'na bağlı olarak Emniyet Genel

Müdürlüğü ve Jandarma Genel Komutanlığı çatısı altında kurulan Siber Suçlarla Mücadele Daire Başkanlıkları[7] bunun örnekleri olarak değerlendirilebilir.

Siber savunma noktasında devletlerin önlem aldığı ve siber uzayın güvenliğini tehdit eden önemli aktörlerden birisi olan hektivist gruplar son dönemde oldukça aktif bir şekilde faaliyet göstermektedirler. Hektivizim İngilizce *"hacking"* yani bilgisayar korsanlığı kelimesi ile aktivizim kelimelerinin bir araya gelmesiyle ortaya çıkmış bir kavramdır. Hektivizim siyasi, sosyal ya da dini bir motivasyon ile bilgisayar teknolojisinin illegal olarak kullanılması aracılığıyla bilgisayar ya da internet ağlarına yetkisiz erişim sağlayarak bilgi ve belgeleri ele geçirme, yok etme ya da afişe etme eylemlerini içermektedir. Birçok farklı siber saldırı yöntemi ile eylemlerini gerçekleştiren hektivist gruplar, özellikle devlet kurumlarına ait internet sitelerini ve bilgisayar ağlarını hedef almaktadırlar. İsimleri dünyaca tanınan birçok hektivist grup bugüne kadar gerçekleştirmiş oldukları eylemlerle kimi zaman ülkelerin ulusal güvenliğini tehlikeye düşürecek bilgileri afişe etmiş, kimi zamanda devlet kurumlarının internet sitelerini ve sistemlerini kısa süreliğine de olsa kullanılmaz hale getirmeyi başarmışlardır. WikilLeaks, Anonymous, Cult of the Dead Cow gibi isimler siber uzayın en bilinen hektivist grupları içerisindedirler (Norton, 2021).

Günümüzde hiçbir devlet, kurum, kuruluş ya da bireyler siber saldırılardan tamamen korunaklı ya da bağışık değildir. Bir ağa bağlı olan her teknolojik aygıt dışarıdan gelebilecek bir siber saldırıya açıktır. İyi planlanmış ve desteklenmiş bir siber saldırı kamu hizmetlerini kesintiye uğratabilir, temel mal ve hizmetlerin üretimine ve dağıtımına engel olarak ekonomiyi olumsuz etkileyebilir ya da ulusal güvenliği tehdit edecek bilgilerin afişe edilmesiyle önemli güvenlik açıkları oluşturabilir niteliktedir. Dolayısıyla devletlerin siber uzayda karşılaşacakları bir saldırıya karşı koyabileceği savunma kapasitesi oldukça önemlidir.

Siber savunma terimi, siber saldırıların bir bilgisayar sistemine veya cihaza bulaşmasını önleme yeteneğini ifade etmektedir. Bu önleme yeteneği ise saldırganların gerçekleştireceği eylemleri önceden tahmin etmek ve ağlara yasa dışı girişleri

[7] Daha fazla bilgi için bkz. T.C. İçişleri Bakanlığı, Emniyet Genel Müdürlüğü, Siber Suçlarla Mücadele Daire Başkanlığı, https://www.egm.gov.tr/siber
T.C. İçişleri Bakanlığı, Jandarma Genel Komutanlığı, Siber Suçlarla Mücadele Daire Başkanlığı, https://www.jandarma.gov.tr/siber

engellemek için aktif adımlar atmayı içermektedir. Tüm siber savunma stratejilerinin ve taktiklerinin ortak amacı siber tehditleri önlemek, bozmak ve karşılık vermektir. Siber uzayda savunma yeterliliğine sahip olmak farklı bileşenlerin bir araya gelmesiyle mümkün olabilir. Bu bağlamda kurumlar siber saldırıları önlemeye yönelik antivirüs yazılımları kullanıyor olsa da kullanılan sistemlerin yazılımsal olarak bir saldırıya izin verecek açıklarının bulunmaması da oldukça önemlidir. Ayrıca potansiyel saldırıları önceden tahmin edecek, açıkları tespit edebilecek donanımda yetişmiş insan kaynağı da hayati önem taşımaktadır. Devletler siber uzayda savunma kapasitelerini artırmak için daha önce de belirtildiği üzere farklı birimler kurmakta ve insan gücü yetiştirmek adına büyük yatırımlar yapmaktadırlar (Slayton, 2017).

Siber uzayın güvenliği konusu savunma kapasitelerinin geliştirilmesi sorunsalı ve savunma-saldırı ikilemi üzerinden tartışılmaktadır. Birçok araştırmacıya göre en iyi savunmanın yeterli saldırı kapasitesine sahip olmaktan geçtiği düşüncesi üzerine geliştirilen siber savunma politikaları, konvansiyonel silahlanmada olduğu gibi siber saldırı yeteneklerinin geliştirilerek bir savunma mekanizması oluşturulmasını öngörmektedir (Mishra, 2020). Soğuk Savaş döneminde ülkelerin güvenlik politikalarını belirlemesinde önemli rol oynayan ve devletlerin diğer devletlerden gelecek potansiyel tehditlere karşı gücünü artırması ve silahlanmasıyla birlikte karşı tarafın güvenliğini tehdit edecek boyuta gelmesiyle diğer aktörün kendisini güvende hissetmeyerek silahlanmasına sebep olacağı ve güvenliğini artırmaya çalışan aktörün aslında daha az güvende olacağı üzerine kurulu güvenlik ikilemi kavramı (Herz, 1950), siber uzayın güvenliğinin sağlanması adına oluşturulan güvenlik ve savunma politikaları içinde geçerliliğini korumaktadır. Devletlerin siber uzayda savunma yeterliliği adına geliştirdikleri politikalarla birlikte tehdit algısını artıran diğer aktörlerin de siber uzayda saldırı ve savunma kapasitelerini artırması, zaten oldukça karmaşık bir yapısı olan siber uzayın daha güvensiz bir hale gelmesine neden olmaktadır denilebilir.

Son yıllarda yapılan siber savunma tatbikatları ise ülkelerin ve uluslararası örgütlerin bu konuya ne kadar önem verdiklerinin bir göstergesi olarak karşımıza çıkmaktadır. Siber savunma noktasında ülkelerin, kurumların ve uluslararası örgütlerin olası bir siber saldırı karşısında bu saldırılara karşı koyabilmek adına sahip oldukları yeterliliklerini test edebilme ve eksikliklerin görülebilmesi adına bu

tatbikatlar hayati önem taşımaktadır. Ayrıca uluslararası boyutlarda yapılan *Locked Sields* (CCDCoE, 2017), yine NATO tarafından yıllık olarak organize edilen *Cyber Coalition*, ve 2 yılda bir Avrupa Birliği üyesi ülkeler için organize edilen *Cyber Europe* (European Union Agency for Network and Information Security) tatbikatları siber savunma anlamında gerçekleştirilen önemli tatbikatlardır. Gerçekleştirilen bu tatbikatlar ülkelerin sahip oldukları siber savunma ve saldırı kapasitelerini test etme imkânı yaratmaktadır. Bu bağlamda özellikle güvenlik ikilemi kavramı çerçevesinde değerlendirildiğinde ülkelerin siber uzayda ortaya çıkabilecek karşı tehditlere karşı kendisini güvende hissetmediği ve buna bağlı olarak kapasite geliştirme anlamında eksikliklerini tamamlayarak uluslararası arenada iş birliğine gitme eğilimi gösterdiklerini söylemek mümkündür.

İKİNCİ BÖLÜM

DİJİTALLEŞME İLE BİRLİKTE ORTAYA ÇIKAN YENİ GÜVENLİK ALGISI VE SİBER GÜVENLİK: TEORİK ÇERÇEVE

Çağlar boyunca güvenlik anlayışı ve önemi, zamanın toplumsal, ekonomik ve siyasi bağlamlarına göre değişmiş ve gelişmiştir. İlk şehirlerin gelişiminden önce insanlar öncelikle kendilerini doğal afetlerden ve yırtıcı hayvanlardan korumaya odaklanmışlardır. Ancak topluluklar oluştukça ve insanlar şehirlerde birlikte yaşamaya başladıkça vurgu birbirleriyle güvenli ilişkiler sürdürmeye doğru kaymıştır. Sosyal bilimler alanında güvenlik kavramı sıklıkla tartışmalara yol açmakta ve tanımı konusunda bir fikir birliği bulunmamaktadır. Konuyla ilgili araştırmaların çoğu, güvenliğin hem bireysel hem de toplumsal düzeyde temel değerlere yönelik tehditlerden korunmayı gerektirdiği konusunda hemfikirdir. Ancak kavramın kapsamı belirlenirken farklı görüşler ortaya çıkmakta, bazı araştırmacılar ulusal, uluslararası veya bireysel perspektiflere odaklanmaktadır. Güvenlik çalışmalarının temeline ilişkin bu mutabakat eksikliği, konuya ilişkin farklı bakış açılarının ortaya çıkmasına neden olmuştur (Baylis, 2008: 70-75).

Güvenlik olgusu değişen bu süreç içerisinde teorisyenler tarafından zamanın şartlarına ve ortaya çıkan ulusal ve de uluslararası ortamın durumuna bağlı olarak farklı zeminlerde ele alınmış ve teorik olarak farklı çerçeveler çizilmiştir. I. Dünya Savaşı'nın sona ermesiyle ortaya çıkan uluslararası siyasi sistem bir yandan savaşın ortaya çıkarttığı yok edici ve yıkıcı izleri silmeye çalışırken diğer yandan ise Milletler Cemiyeti'nin (MC) oluşturulmasıyla dünyada barışın tesis edilmesi için uğraşmaya başlamıştır. Amerika Birleşik Devletleri'nin öncülüğünde liberal düşünce yapısı temelinde ortaya çıkan idealizm ve MC'nin savaş sonrası oluşturmaya çalıştığı yeni dünya sistemi II. Dünya Savaşıyla birlikte temelini yitirmiştir. Milletler Cemiyeti sisteminin oluşturmaya çalıştığı devletlerarası ilişkilerde ortaya çıkan anlaşmazlıkların barışçıl yollardan diplomasi ile çözülmesi gerektiği düşüncesi II. Dünya Savaşıyla bir bakıma anlamını kaybetmiştir. II. Dünya Savaşı sonrası ortaya çıkan yeni siyasi

düzende güç odaklı bir yaklaşım olarak ortaya çıkan realizm ise uzun bir süre etkinliğini korumuş fakat 1970'li yıllarda özellikle Ortadoğu'da meydana gelen gelişmeler sonucunda ortaya çıkan petrol krizi ve beraberinde ortaya çıkan birçok farklı etkenle birlikte devletlerin sahip olduğu sert güç temelinde geliştirilen realizm, güvenlik kavramını açıklamada yetersiz kalmaya başlamıştır. Bu bağlamda güvenlik kavramı farklı teorik çerçevelerde ele alınmaya başlanmıştır.

Siber uzay ve bu alanın güvenliği konusu ise teorik olarak birçok farklı yönden ele alınmaktadır. Özellikle realist yaklaşım temelinde neorealizm çerçevesinde değerlendirilebilen siber uzayın güvenliği konusu, MC'nin oluşturmaya çalıştığı düzen ile ortaya çıkan idealist yaklaşımlar ve aynı zamanda liberalist, neoliberalist teoriler ve de uluslararası ilişkiler alanının farklı okullarının ortaya koyduğu teorik çerçevelerle de bağlantılı olarak açıklanabilir bir yapıdır. Güvenlik çatı olgusu içerisinde görece olarak oldukça yeni olan siber güvenlik kavramının teorik olarak bir çerçeveye oturtulması konusu da hala üzerine farklı görüşlerin olduğu tartışmalı bir konu olarak kabul edilmektedir. Siber güvenlik kavramının teorik olarak açıklanabilmesi adına öncelikle güvenlik olgusunun tarihsel süreç içerisinde nasıl değiştiğini ve teorik olarak nasıl ele alındığını anlamak siber güvenliğin teorik olarak bir çerçeveye oturtulması bağlamında doğru olacaktır.

1. TARİHSEL SÜREÇ İÇERİSİNDE GÜVENLİĞİN DEĞİŞEN ÇEHRESİ VE FARKLI GÜVENLİK ÇALIŞMALARI YAKLAŞIMLARI

1.1. Güvenlik Olgusu: Tanımı ve tarihsel süreç içerisinde değişimi

İnsanlık tarihi kadar eski olan güvenlik olgusu, insanlığın varoluşuyla ilgili bir kavram olmakla birlikte ilk insandan günümüze yaşanan tüm değişimlere bağlı olarak farklı anlamlar içeren bir olgu olarak varlığını sürdürmeye devam etmektedir. İnsanların bireysel olarak yaşadığı ve avcı-toplayıcı özellikte hayatlarını sürdürdükleri dönemde güvenlik olgusu yırtıcı hayvanlara ve doğaya karşı verilen mücadele çerçevesinde algılanırken, insanoğlunun yerleşik hayata geçerek bir arada yaşama evresine geçmesiyle bambaşka bir boyuta evrilmiştir. Güvenlik olgusu sosyal bilimlerin konusunu oluşturan birçok farklı kavramda olduğu gibi üzerine fikir birliği

sağlanmış herhangi bir tanımı olmayan tartışmalı bir kavramdır. Genel olarak ve çoğunlukla askeri anlamda ele alınan güvenlik olgusu, savunma kavramıyla birlikte tanımlanmaya çalışılmaktadır. Sadece askeri anlamda savunma ya da ulusal sınırların güvenliğinin sağlanması noktasında ele alınarak tanımlanması mümkün olmayan güvenlik olgusunun birçok farklı yönü vardır. Özellikle güç kavramıyla yakından ilişkili olarak açıklanmaya çalışılan güvenlik kavramının zaman içerisinde farklı teorik yaklaşımlar ve değişen uluslararası sistemle birlikte farklı temellerde de ele alınmaya başlanmıştır (Buzan, 1984: 111). Dolayısıyla bu olgunun anlaşılabilmesi adına hem bireysel hem de toplumsal anlamda sınırları aşan bir yaklaşım güvenlik olgusunun anlaşılmasında ve açıklanmasında oldukça önemli bir yerde durmaktadır.

İnsan toplulukları arasındaki ilişkiler tarih boyunca farklı boyutlara dönüşmüştür. İlk ulusların oluşumuyla birlikte devletlerarası çatışmalara dönüşen çeşitli mücadelelerle karşı karşıya kalan farklı insan toplulukları farklı güvenlik kaygıları geliştirmiş ve çeşitlendirmiştir. Tarihsel süreç içerisinde ulus-devletler ortaya çıktıkça güvenlik hem ulusal hem de uluslararası öneme sahip bir meseleye dönüşmüştür. Dönemin siyasi ve ekonomik koşulları ve bunların sonuçları, güvenliğin farklı şekillerde yorumlanmasına yol açmıştır.

Güvenlik olgusu zaman içerisinde birçok farklı araştırmacı tarafından farklı şekillerde tanımlanmıştır. Baldwin'e (1997: 5-9) göre güvenlik kavramının tanımlanması konusu oldukça az sayıda araştırmacının çalıştığı bir araştırma konusu haline gelmiş küçük bir endüstridir. Yapılan bu araştırmalar güvenlik kavramının kendisinden çok ulus-devletlerin güvenlik politikalarına odaklanmış ve dışarıdan gelecek askeri tehditlere ek olarak insan hakları, ekonomi, çevre, uyuşturucu ticareti, salgın hastalıklar, suç ya da toplumsal adalet gibi kavramlara öncelik vermiştir. Yapılan bu çalışmalar normatif ve deneysel tartışmalar temelinde ele alınarak hangi değerlerin korunması gerektiği ya da bu değerlere karşı ortaya çıkabilecek tehditler üzerinde yoğunlaşmaktadır. Soğuk Savaş dönemi sonrasında güvenliğin yeniden tanımlanması çalışmaları daha karmaşık ve zor bir hale gelmiştir. Güvenlik, özellikle II. Dünya Savaşı ile toplumsal özgürlüklerin kısıtlanmasının, savaşa girmenin ya da kaynakların yer değiştirilmesinin meşru bir gerekçesi olarak gösterildiği gibi, adalet, özgürlük, eşitlik, temsil ve güç temelinde yeterince ilgi gösterilmemiş bir kavramdır (Baldwin, 1997: 5-9).

Güvenlik, tarihsel olarak insanların korunması, güvende tutulması ve tehlikelere karşı savunulmasıyla ilgili olmuştur. İnsanlar, tarih boyunca güvenliği sağlamak için farklı yollar bulmuş ve bu kavramın gelişiminde önemli rol oynamışlardır. İlk insanların güvenlik ihtiyacı, doğal olarak yaşadıkları ortama göre değişiklik göstermiştir. İnsanlar, vahşi hayvanlardan, diğer insan gruplarından ve doğal afetlerden korunmak için barınaklar ve savunma mekanizmaları oluşturmuşlardır. İlk yerleşim yerleri ve kaleler, güvenlik ihtiyacını karşılamak için inşa edilmiştir. İnsanlık tarihindeki en eski yazılı kanunlar, güvenliği sağlamak için oluşturulmuştur. Hammurabi Kanunları gibi eski kanunlar, suçlu olan kişilerin cezalandırılmasını ve bu şekilde güvenliğin sağlanmasını hedeflemiştir (Kim, 2015).

Orta Çağ'da, güvenlik kavramı daha çok savaş ve çatışma dönemleriyle ilişkilendirilmiştir. Kırsal bölgelerde köyler ve kasabalar, yerel hükümetler tarafından korunmuş ve saldırılara karşı savunulmuştur. Şehirlerde ise, surlar, hendekler, kaleler ve diğer savunma yapıları inşa edilmiştir (Buzan, 1991). Modern zamanlarda, güvenlik kavramı daha da gelişmiştir. Özellikle sanayi devrimi sonrası teknolojinin ilerlemesi, güvenlik teknolojilerinin gelişmesine yol açmıştır. İlk kez 1853 yılında Amerika Birleşik Devletleri'nde kurulan özel güvenlik şirketleri, binaların ve diğer varlıkların korunması için görevlendirilmiştir (Scholtz, 2017).

Güvenlik kavramı, aynı zamanda uluslararası ilişkilerde ve savaş durumlarında da önemli bir rol oynamıştır. İlk defa 1648 yılında Westphalia Antlaşması'yla uluslararası ilişkilerde devletlerin egemenlik haklarına saygı duyulması ve diğer ülkelerin iç işlerine karışmaması prensibi kabul edilmiştir (Buzan, 1984: 21-23). Bugün güvenlik kavramı daha çok terörizm, siber saldırılar, doğal afetler, suçlular ve diğer tehditlerle ilgili olarak kullanılmaktadır. Özellikle siber güvenlik teknolojileri ve veri koruma yöntemleri gibi yeni gelişmeler, güvenlik kavramının daha da gelişmesine ve önem kazanmasına yol açmıştır

Tarih boyunca insanoğlunun varoluş mücadelesinde güvenlik olgusu oldukça önemli bir yer teşkil etmiştir. Güvenlik insan için yeme, içme, barınma gibi temel ihtiyaçlardan birisini teşkil eder. Bu bağlamda insanın güvenlik ihtiyacı hayatın bir parçası olarak elzem bir gerekliliktir. Fiziksel anlamda güvenlik ihtiyacına ek olarak insanoğlu duygusal anlamda da güvenlik arayışı içerisindedir. Psikoloji alanında

yapılan çalışmalar insanoğlunun birbirleriyle olan ilişkilerinde duygusal olarak güvende hissetmediği durumlarda genellikle bir çatışmanın içerisinde olduğunu kanıtlamıştır (Johnson, 2022: 23).

Güvenlik olgusu farklı teorik yaklaşımlar çerçevesinde oldukça farklı şekillerde ele alınmıştır. Dolayısıyla oldukça farklı tanımlamalara ve algıya sahip olan kavram, herkes ve her şey için farklı bir anlam ifade edebilen ve sosyal bilimler alanında birçok farklı kavramda olduğu gibi oldukça sübjektif bir kavram olarak tartışmalı bir kavramdır. Özellikle siyaset bilimi ve uluslararası ilişkiler disiplinlerinde farklı düzeylerde ele alınmaktadır. Devletlerin güvenliği, sınırların güvenliği, ekonominin güvenliği, bilginin güvenliği, çevre güvenliği, enerjinin güvenliği, askeri güvenlik, bilginin güvenliği, bireylerin güvenliği gibi farklı temellerde ele alınan güvenlik olgusu birçok farklı tanımın ortaya çıkmasına da neden olmuştur.

Güvenlik, bireylerin, kuruluşların, sistemlerin veya varlıkların çeşitli tehdit veya zarar türlerinden korunmasını ifade eden bir kavramdır. Bu, fiziksel güvenlik, veri ve bilgi koruması, finansal istikrar ve duygusal refahı içerebilir. Güvenlik önlemleri, riskleri ve kırılganlıkları en aza indirmeyi, kaynakların gizliliğini, bütünlüğünü ve kullanılabilirliğini korumayı ve bireyler ve topluluklar için bir güvenlik ve güvence duygusu sağlamayı amaçlar. Güvenlik, bir tehlike, risk veya zararın oluşmasını önlemek veya minimize etmek amacıyla, belirli bir sistemi, yapıyı veya faaliyeti korumak için alınan tedbirlerin bütünüdür. Genel olarak güvenlik, insanların hayatlarını, sağlıklarını, mülklerini ve diğer varlıklarını korumak için alınan önlemler ve yapılan faaliyetlerdir. Bu önlemler, fiziksel, teknolojik, sosyal veya politik olabilir ve birçok farklı alanı kapsayabilir. Güvenlik kavramı, öncelikle risk analizi, risk yönetimi, güvenlik politikaları ve güvenlik teknolojileri gibi konuları içeren geniş bir disiplindir. 20. yüzyılın ilk yarısında gerçekleşen ve insanlık tarihinin en yıkıcı sonuçlarına neden olan iki dünya harbi sonrasında güvenlik kavramı ulusal boyuttan uluslararası boyutta incelenmeye başlamıştır. Bu bağlamda özellikle uluslararası güvenlik çalışmaları 1950'li yıllar sonrasında hız kazanmış ve Soğuk Savaş dönemi boyunca birçok farklı temelde ele alınmıştır. İkinci Dünya Savaşı sonrasında devletlerin iç ve dış tehditlere karşı nasıl korunacağı ve güvenliğin nasıl sağlanacağı konusu üzerindeki çalışmalar önem kazanmıştır. Güvenlik çalışmaları ana çatısı

altında uluslararası güvenlik konusu hala tam olarak tanımı yapılabilen ve üzerine genel olarak kabul görmüş bir görüş birliği olmayan bir konudur (Buzan, 1991).

Güvenlik olgusu ilk olarak insanların hayatlarını sürdürdüğü alanda bir temel ihtiyaç olarak yaşanılan alanın sınırları çerçevesinde ele alınmış, oluşabilecek potansiyel bir tehlikeye karşı önlem alma ve gerektiğinde savunma yapma bağlamında algılanmıştır. Dolayısıyla toplulukların yaşadığı coğrafyanın özelliklerine bağlı olarak yaşanılan alanın güvenliği, toplumun güvenliği, devletin güvenliği ve tüm bunlara bağlı olarak bireylerin güvenliği konularını içeren bağımlı faktörlerin bütünü olarak değerlendirilmiştir (Warner, 2014: 22). Güvenlik, insanların hayatlarında genel olarak kaygı, üzüntü ve risk faktörlerinin olmadığı bir durum olarak tanımlanabilir (Wolfers, 1952: 485). Bir başka tanıma göre ise güvenlik, genel çerçeve ve boyutlara tekabül eden, bireylerin konulara, toplumsal adetlere ve değişen tarihsel şartlara uygun olarak uyarlanan temel bir kavram olarak tanımlanmaktadır. (Brauch, 2008: 4). Bu bağlamda güvenlik, kaygı ve endişenin olmadığı, riskin minimize edildiği bir durumu ifade eder. Bireylerin güvende hissetmesi, güvenlik kavramının merkezinde yer alır ve bu kavram, toplumsal adetlere ve değişen tarihsel şartlara göre uyarlanır.

Güvenlik kavramı, toplumsal bir değer olarak ele alındığında, tehlike, risk, kargaşa ve korku olmadığı; koruma, güvenilirlik, risk yokluğu ve güven hissinin hâkim olduğu bir ortamı tanımlamaktadır. İnsanların her türlü tehditten uzak ve korkusuz bir şekilde yaşayabilecekleri, kendilerini güvende hissedebilecekleri bir toplumsal düzen, insanların ihtiyaçları doğrultusunda sürekli olarak işlemektedir (Brauch, 2008). Güvenlik, nesnel ve öznel olmak üzere iki boyutta ele alınabilir. Nesnel boyutta güvenlik, kazanılmış değerlerin tehdit altında olmadığı, riskten uzak olduğu anlamına gelirken, öznel boyutta bu değerlere saldırı ihtimali olmadığı anlamına gelir. Dolayısıyla güvenlik, tehditler, endişeler ve tehlikelerden uzak olma hissi olarak tanımlanabilir (Wolfers, 1952: 489).

Devletlerarası ilişkilerin yapıtaşlarından birisini oluşturan güvenlik olgusu, tarihsel süreç boyunca zamanın ve mekânın getirdiklerine ve gerek doğal olaylarının seyrine gerekse de insan ırkının birbirleriyle olan ilişkilerinde meydana gelen olayların muhteviyatına göre farklı şekillerde algılanmıştır. Bu bağlamda güvenlik olgusu, Birinci ve İkinci Dünya Savaşlarından sonra karşılıklı askeri tehditlere karşı ulusal

savunma olarak görülmüştür. Soğuk Savaş döneminde ise stratejik dengeler, uluslararası ilişkiler ve nükleer caydırıcılık ile tanımlanmıştır. 2001'deki 11 Eylül saldırılarının ardından güvenlik, terörle mücadele çabalarıyla eş anlamlı hale gelmiştir (Booth, 2007: 95-97). Teknolojinin ulusal ve uluslararası güvenliğin sağlanmasındaki kritik rolü, yirminci yüzyılda yaşanan iki Dünya Savaşı ve Amerika Birleşik Devletleri ile Sovyetler Birliği arasındaki uzun süreli Soğuk Savaş sırasında daha iyi anlaşılmıştır. Bu dönemler teknolojik hakimiyetin geleneksel insan gücünden daha değerli olduğunu göstermiştir. Bu bağlamda teknolojinin gelişmesi güvenlik kavramı algısıyla oldukça yakından bağlantılı bir şekilde ilerlemiştir. İlk çağlarda insanların güvenliklerini sağlamak adına kullandıkları araçlar, güvenlik olgusunun zamanla nitelik ve nicelik olarak şekil değiştirmesiyle ortaya çıkan farklı tehditlere karşı teknolojinin getirdikleriyle birlikte sürekli güncellenmiştir.

Güvenlik çalışmaları tarihsel süreç içerisinde hangi temelde ele alınması gerektiği noktasında çağın getirdikleri ve gerekliliklerine bağlı olarak farklı bakış açılarından ele alınmıştır. Özellikle II. Dünya Savaşından sonra ortaya çıkan dünya düzeninde güvenlik algısı, ulusal güvenlikten uluslararası güvenliğe doğru evrilmiştir. Sovyetler Birliğinin dağılmasından sonra 2000'li yılların başlarına kadar iki kutupluluğun ortadan kalktığı ve dönemin ABD başkanı Bush'un deyimiyle "Yeni Dünya Düzeni" (New World Order) kavramı kapsamında güvenlik algısı uluslararası güvenliğin askeri güvenlik temeline ek olarak insan hakları, bilginin güvenliği, özgürlük ve bireysel güvenlik gibi konuların da eklenmesine neden olmuştur. Özellikle uluslararası güvenlik kavramı temelinde yapılan çalışmalarda neyin temel alınacağı, güvenliğin hangi temelde incelenmesi gerektiği noktasında ortaya çıkan tartışmalar, güvenlik çalışmalarına farklı bir boyut kazandırmıştır. Güvenlik olgusunu kavramsal analizini ampirik çalışmalarla destekleyerek açıklamaya çalışan Buzan'a göre devlet seviyesinde ve uluslararası sistem seviyesinde ele alınan güvenlik kavramı birey seviyesinde güvenliği de içerisinde barındırmaktadır ve birey seviyesinde güvenlik olgusu diğer seviyelere bağlıdır. Ayrıca güvenlik hiçbir zaman tek bir seviyede ele alınamaz ve güvenlik çalışmalarında başvurulan referans nesne durumun gerekliliğine göre analiz seviyesiyle bağlantılı bir şekilde olmak durumundadır (Buzan, 1984: 25).

Uluslararası güvenlik çalışmaları kapsamında Buzan, uluslararası güvenlik kavramının anlaşılmasında dört temel soru olduğunu ve bu sorular bağlamında

kavramın anlaşılması gerektiğini söylemektedir. Buzan'a göre güvenlik, her zaman dahili ya da harici belirli bir referans nesnesine bağlıdır. Bu bağlamda sorulması gereken ilk soru devletin güvenlik olgusunun temel referans nesnesi olup olmadığı sorusudur. Gerek ulusal güvenlik gerekse de uluslararası güvenlik temelinde ele alınsın, ulus ya da devlet uluslararası güvenliğin temel referans nesnesidir. Uluslararası güvenlik, devletin güvenliğini insanlığın, bireylerin güvenliği ya da devletin sınırları içerisinde yaşayan azınlıkların güvenliği ile değiştirmek anlamına gelmemektedir. Ulusal güvenlik, ya da devletin güvenliği konusu, uluslararası güvenlik çalışmalarında diğer tüm referans nesnelerini kapsayan kavramlardır.

Buzan'ın sorduğu ikinci soru ise iç tehditlerin yanı sıra dış tehditlerin güvenlik çalışmalarına dahil edilip edilmeyeceğidir. Güvenlik, devlet egemenliği hakkındaki tartışmalara bağlı olduğundan devletlerin egemenlik sınırlarıyla ilgili olarak fiziki sınırlarına karşı oluşabilecek tehditlerle de alakalıdır. Sorulan üçüncü soru ise güvenliğin askeri sektör ve güç kullanımının ötesine genişletilip genişletilmeyeceğidir. Uluslararası güvenlik kavramının Soğuk Savaş döneminde askeri güvenlikle eş anlamlı hale gelmesi, değişen dünya düzeniyle birlikte güvenlik çalışmalarında diğer referans nesnelerinin ele alınıp alınmayacağı tartışmalarını ortaya çıkartmıştır. Son olarak sorulan soru ise güvenlik olgusunun tehditler ve tehlikelerden bağımsız bir şekilde ele alınıp alınamayacağı sorusudur. Ulusal güvenlik kavramının ABD ve daha genel olarak Batının kendisini tehdit altında gördüğü bir dönemde geliştirildiği göz önünde bulundurulduğunda uluslararası güvenliğin tehdit ve tehlike algılamasından bağımsız bir şekilde algılanamayacağı ise ortadadır (Buzan, 2009: 11-15; Wolfers, 1952).

Wolfers'a göre en nihayetinde güvenlik denilen olgu, güvensizliğin ortaya çıkarttığı kötülüğün olmaması durumudur. Dolayısıyla devletler bu durumu en aza indirmeye ve en düşük seviyede tutmaya eğilimli olacaklardır. Bu durum ise genellikle daha düşük seviyelerde, yani politika yapıcıların, askeri liderlerin ve karar alma sürecinde bulunan kişilerin olması gerektiğini düşündüğü seviyede gerçekleşecektir. Her durumda dış tehditlerle birlikte ulusal karakter, gelenek, tercihler ve önyargılar gibi birçok ulusal faktör bir ülkenin kendisine belirlediği güvenlik seviyesini yakalamakta etkili olacaktır (Wolfers, 1952: 488). Baldwin ise Wolfers'ın yaptığı güvenlik tanımında belirttiği kazanılmış değerlere karşı tehdidin bulunmaması

durumundaki "*tehditlerin bulunmaması*" açıklamasının belirsiz olduğu eleştirisini yapmıştır ve bu durumu elde edilmiş değerlere oluşabilecek hasar durumunun düşük olması şeklinde yeniden formüle etmiştir (Baldwin, 1997: 13).

Güvenlik terimini kullananların aklında genellikle belirli türden tehditler vardır. Örneğin ev güvenlik sistemleri genellikle potansiyel hırsızlara yöneliktir ya da ulusal güvenlik sistemleri genellikle diğer devletlere yöneliktir. Elde edilmiş değerlere yönelik tehditler pek çok kaynaktan kaynaklanabileceğinden bu boyutun açıkça belirtilmesi faydalı olacaktır. Örneğin Soğuk Savaş sırasında ulusal güvenliğe yönelik "Komünist tehdide" yönelik belirsiz söylemler, çoğu zaman bunların ideolojik tehditler mi, ekonomik tehditler mi yoksa askeri tehditler mi olduğu veya bunların hepsinin bir kombinasyonu mu olduğu konusu belirsizdir. Dolayısıyla bu durum tehdidin doğası ve büyüklüğüne ilişkin rasyonel tartışmaları engellemektedir. Bu tür akademisyenler genellikle tehdit terimini, birinin talepleri karşılanmadıkça cezalandırmak için koşullu bir taahhüt içeren eylemlere atıfta bulunmak için kullanırlar. Bununla birlikte, günlük dilde edinilmiş değerlere yönelik "tehdit" olarak sıklıkla salgın hastalıklar, seller, depremler veya kuraklıklardan söz edilir (Baldwin, 1997: 15-16).

Peki güvenlik olgusunun tarihsel süreç içerisindeki dönüşümü göz önünde bulundurulduğunda siber uzayın güvenliği konusu hangi temellerde ele alınmalıdır? Ulusal, uluslararası ya da birey seviyesinde ele alınabilecek siber uzayın güvenliği konusu, teorik olarak birçok farklı bakış açısı ile açıklanabilir. Bu bağlamda özellikle Buzan'ın güvenliğin referans nesneleri konusunda ortaya attığı sorular siber güvenlik için de geçerlidir. Bakıldığında siber uzayın güvenliği konusu kritik altyapıları ve devlet güvenliğini tehdit edebilecek bilgilerin güvenliğinin sağlanması temelinde değerlendirildiğinde bir ulusal güvenlik sorunu olarak ele alınması mümkündür. Bunun yanında fiziksel sınırları olmayan bu yeni alanın küresel boyutta ortaya çıkardığı etki göz önünde bulundurulduğunda ise bir uluslararası güvenlik konusudur. Yine aynı şekilde akıllı telefonların kullanımının ve internet teknolojisine erişimin oldukça kolaylaştığı ve yaygınlaştığı günümüzde, bireylerin siber uzaydaki etkinliği ve siber uzayın getirdiği birçok kolaylığı kullanma seviyesi temelinde düşünüldüğünde ise bireylerin güvenliği çerçevesinde de değerlendirilebilir. Özellikle kişisel verilerin korunması ve güvenliği, ifade özgürlüğü ve internette sansür bağlamında siber uzayın

güvenliği konusu birey temelli de değerlendirilmesi gereken bir konudur. Dolayısıyla siber uzayın güvenliği, güvenlik çalışmalarının bir bütün olarak ele alınmasını zorunlu hale getirmektedir. Bu bağlamda siber uzayın güvenliği konusu gerek siyaset felsefesi temelinde gerekse de uluslararası ilişkiler teorileri temelinde literatürde güvenlik çalışmalarına yön vermiş birçok farklı teorik yaklaşım çerçevesinde değerlendirilebilecek ve bu çerçevelere oturtulabilecek bir konu olması itibariyle teorik olarak farklı güvenlik yaklaşımları çerçevesinde siber uzayın güvenliği sorunsalı açıklanmaya çalışılmaktadır.

2. FARKLI GÜVENLİK YAKLAŞIMLARI ÇERÇEVESİNDE SİBER UZAYIN GÜVENLİĞİ

2.1. Siber Uzayın Güvenliğinde İdealizm ve Kolektif Güvenlik

İdealizm, devletlerin ve diğer aktörlerin barışçıl ve işbirlikçi ilişkiler kurarak dünya siyasetinde daha güvenli ve istikrarlı bir ortam yaratabileceklerine inanan bir düşünce sistemidir. Bu yaklaşım, devletlerin kendi çıkarlarını savunurken diğer devletlerin ve uluslararası toplumun çıkarlarına da saygı göstermeleri gerektiğini savunur. Uluslararası iş birliği ve diyalog temelinde şekillenmiş olan idealizm, devletlerin güvenlik konularında diğer devletler ve uluslararası kuruluşlarla iş birliği yaparak ve diyalog yoluyla sorunları çözmenin önemine vurgu yapar. İdealistler, dünya siyasetinde barış ve istikrarın korunması ve teşvik edilmesi gerektiğine inanırlar. Bu amaçla, uluslararası hukuka saygı gösterilmesi ve devletler arasındaki anlaşmazlıkların barışçıl yollarla çözülmesi gerektiğini savunurlar. İdealist güvenlik yaklaşımı, devletlerin ve uluslararası toplumun adalet ve eşitlik ilkelerine dayalı bir dünya düzeni kurmaya çalışmaları gerektiğini öne sürmektedir. Bu bağlamda idealistler, insan haklarının ve demokratik değerlerin korunması ve yayılmasının, dünya güvenliği için önemli olduğuna inanır. Bu nedenle, devletlerin ve uluslararası kuruluşların, insan hakları ve demokrasi konularında iş birliği yaparak ve bu değerleri teşvik ederek dünya güvenliğine katkıda bulunmaları gerektiğini savunurlar. İdealizm, ekonomik kalkınma ve refahın dünya güvenliğine ve istikrarına katkıda bulunduğunu ve bu bağlamda, devletlerin ve uluslararası kuruluşların, küresel ekonomik kalkınmayı

desteklemeye ve eşitsizlikleri azaltmaya çalışmaları gerektiğini öne sürmektedir (Mearsheimer, 1994; Carr, 2001; Morgenthau, 1967).

İdealizm, genellikle Wilsoncu geleneğin perspektifleri, teorileri ve yöntemleriyle özdeşleştirilmiştir. Dönemin ABD Başkanı Woodrow Wilson (1913-1921) tarafından savunulan ideallere atıfta bulunan idealist perspektifler, liberalizm ve neo-muhafazakarlık gibi insanların hedeflemesi gereken evrensel siyasi ve ekonomik idealler olduğunu kabul eder. Uluslararası politikada bu idealler, özgürlük, demokratik temsil sistemleri, serbest piyasalar ve kapitalist ticaret sistemleri olarak kabul edilir. İdealizmin belirli biçimleri, uluslararası kurumların ekonomik ve politik şeffaflığı sağladığını ve devletlerin iş birliği yapmaya yönelik eğilimlerini güçlendirdiğini iddia etmektedir. İkinci Dünya Savaşı sonrası idealizm, ulus-devletlerin iş birliği yapma yeteneğini olumsuz yönde etkileyen değişkenleri önce incelemek ve ardından zamanla ortadan kaldırmak umuduyla bilimsel pozitivizmin bazı öğretilerini de içermiştir. İdealizm, tarihinin büyük bir kısmında ulusal ideallerin göreceli ve çoğulcu olduğunu düşünen ve uluslararası politikanın güce dayalı ve aşılamaz bir düzeninden türeyen realist düşünceyle karşılaştırılmıştır. Uluslararası ilişkilerde genellikle iki tür idealist yaklaşımın olduğu varsayılmaktadır. Bunlar, liberalizm ve neo-muhafazakarlık etrafında şekillenen yaklaşımlardır. Dolayısıyla idealizm genellikle liberalist düşünceyle birlikte anılmaktadır (Badie, Berg-Schlosser ve Morlino, 2011: 1128).

Geniş anlamda idealizm, uzun ömürlü bir öğreti veya dünya işlerine yönelik bir eğilim olarak görülür ve merkezi hükümetin olmadığı, yani anarşi durumunda bulunan bağımsız politik toplulukların var olduğu tüm tarihsel dönemlerde gözlemlenebilir. İdealizm, uluslararası anarşiyi aşmayı ve daha kozmopolit ve uyumlu bir dünya düzeni yaratmayı hedefleyen iyimser bir öğreti olarak algılanmaktadır. Dar anlamda idealizm ise iki dünya savaşı arasındaki dönemle (1919-1939) yakından ilişkilidir. Özellikle uluslararası ilişkiler disiplininin teorik olarak açıklanmasının ilk aşamasına hâkim olan bir öğretidir. İnsanlığın giderek artan bağımlılığını ve birliğini vurgulamakla birlikte Milletler Cemiyeti'nin kurulmasıyla oluşturulmaya çalışılan yeni uluslararası sistemle yakından ilgilidir (Carr, 1964).

İki savaş arası dönemde idealist düşünceler bağımsız ulus-devletlerin gücünü düzenlemeye yönelik pek çok politika önerisinde bulunmuş ve neredeyse tümü,

uluslararası kuruluşlarda artan güç ve siyasi otorite sağlayarak ulus-devletlerin gücünü düzenlemeye çalışan öneriler olmuşlardır. Birbiriyle rekabet halinde bulunan ulus-devletlerin ortaya çıkarttığı çatışma ortamı, I. Dünya Savaşı felaketinin temel nedeni olarak görülmüş ve bu nedenle egemenlik ilkesi ve güç dengesi kurumu daha radikal idealistlerin görüşüne göre aynı şeyin tekrar olmaması için düzenlenmesi ve kaldırılması gereken olgular olarak idealist görüşün temel aldığı konular haline gelmiştir. Kolektif güvenlik, uluslararası anlaşmazlıkların yargı önünde çözülmesi, silahsızlanma, açık diplomasi ve hesap verilebilirlik iki savaş arası dönemde idealistlerin en çok değer verdiği politika önerileri olmuştur. Bazıları daha da ileri giderek, uluslararası bir polis gücü kurulmasını ve silah üretiminin tamamen uluslararası denetiminin gerekli olduğunu dahi savunmuştur (Long vd., 1995).

Carr, idealist düşünceyi oldukça sert bir şekilde birçok faklı yönden eleştirmiştir. Carr'ın idealistlere yönelttiği ana eleştirilerden birisi, uluslararası politikadaki gücün rolünü küçümsedikleri ve hukukun, ahlakın ve kamuoyunun rolünü hem gerçek hem de potansiyel olarak abarttıkları şeklinde olmuştur. Akıl ve tartışmanın orduları ve donanmaları değiştirebileceği fikrine özellikle sert bir şekilde karşı çıkan Carr, değişimin akıl yoluyla (en azından idealistlerin düşündüğü gibi akıl yoluyla) gerçekleşmediğini savunmuştur. Güç, her politik durumda belirleyici bir faktördür ve gücü ortadan kaldırmak politikayı ortadan kaldırmak kadar imkansızdır. Kullanılan, tehdit edilen veya sessizce bekletilen güç, uluslararası sistemin değişiminde temel bir faktör olmuştur. Bu değişim ancak gücü kullanabilenler tarafından veya güç kullanabilenlerin çıkarları doğrultusunda gerçekleştirilebilir (Carr, 2001).

Herz idealizmi daha iyi bir dünya, daha iyi siyaset ve daha iyi devlet gibi idealleri savunan ve olması gerekeni arayan ütopik idealler olarak tanımlamaktadır (Herz, 1951: 17). Realist düşüncenin öncülerinden John H. Herz idealizmi Carr'a bezer bir şekilde değerlendirerek birçok yönden eleştirmiştir. İdealistlerin ve idealist düşüncenin "ütopik" olduğunu söyleyen Herz, idealistlerin uluslararası sistemi açıklamada güç kavramını yeterince dikkate almadıklarını söylemektedir. Siyasi idealizm genellikle daha "rasyonel" bir varsayımdan hareket eder; yani, bireysel kaygılar ve genel iyilik arasında bir uyumun var olduğu veya sonunda gerçekleştirilebileceği, toplumdaki insanlar ve grupların çıkarları, hakları ve görevleri

arasında ve ayrıca gücün kolayca yönlendirilebileceği, yayılacağı, ortak iyilik için kullanılacağı ve nihayetinde siyasi ilişkilerden tamamen uzaklaştırılabileceği düşünülür. Diğer yandan idealist düşünce, bireylerin ve grupların bencil içgüdü ve tutumlarını sadece güvenlik ve çıkarlar ötesindeki düşünceler temelinde aşması gereken koşullara ve çözümlere bağlamaktadır. Bu nedenle, genellikle bireycilik, hümanizm, liberalizm, pasifizm, anarşizm, uluslararasıcılık gibi insanlar üzerinde örgütlü grupların iddia ettiği güç ve otoriteyi sınırlamak veya daha radikal olarak ortadan kaldırmak temelinde geliştirilmiş olan ideolojilerden biri olarak ortaya çıkar (Herz, 1950: 158-160).

İdealizm, I. Dünya Savaşı'nın yıkıcı etkilerini gören ülkeler tarafından ABD öncülüğünde MC'nin kurulması ile hayata geçirilmeye çalışılmış fakat II. Dünya Savaşı'nın patlak vermesiyle uygulanabilirliği ve gerçekliği tartışılan bir sistem olarak realizmin ortaya çıkmasına ön ayak olmuştur. İdealist düşünce, II. Dünya Savaşı sonrasında uluslararası sistemin dönüşümü ve Soğuk Savaş döneminde ortaya çıkan silahlanma yarışı ve nükleer caydırıcılık, Sovyetler Birliği'nin dağılmasıyla birlikte dönüşen uluslararası sistemin geldiği durum, devletler arasındaki rekabetler ve teknoloji yarışı bağlamında değerlendirildiğinde Herz'in de ifade ettiği gibi ütopik bir düşüncedir. Sınırları olmayan ve her geçen gün durdurulamayan bir şekilde genişleyip gelişen siber uzayın idealist düşünce ile tam bir açıklamasının yapılması mümkün değildir. Tehditlerin sürekli arttığı ve çeşitlendiği bu ortamda devletler sadece kendi sınırları içerisinde bile bu alanda ortaya çıkabilecek tehditlere karşı kapasite geliştirme noktasında güçlük yaşamaktadır. Ek olarak, devletlerin sınırları dışından siber uzayda aldıkları bir tehdide karşı güvenliklerini sağlamaları bu alanın uluslararası arenada düzenlenmesinin oldukça sıkıntılı olduğu göz önünde bulundurulduğunda neredeyse imkânsız hale gelmektedir.

İdealist düşünce aslında bakıldığında siber uzayda ortaya çıkabilecek güvenlik tehditlerinin önüne geçilebilmesi adına rasyonel teklifler sunabilmektedir. Lakin devletlerin bu alanda özellikle 21. yüzyıl itibari ile içerisine girdikleri güç yarışı bu durumun gerçekçi olmadığını kanıtlar niteliktedir.

Devletler ve uluslararası kuruluşlar arasında iş birliğinin ve diyaloğun teşvik edilmesini savunan idealizm, siber uzayın güvenliğinin sağlanması adına oldukça

önemli bir düşünceyi temsil etmektedir. Siber saldırılar ve siber suçların sınırların ötesine geçen küresel sorunlar olması nedeniyle etkili önleme ve müdahale stratejilerinin uygulanabilmesi için uluslararası düzeyde iş birliği ve bilgi paylaşımı gereklidir. Bu bağlamda idealizmin temel ilkelerinden olan uluslararası iş birliği ve diyalog, siber güvenliğin sağlanması adına oldukça önemlidir. NATO'nun 2016 yılında Varşova Zirvesinde siber uzayı kara, hava ve denizden sonra dördüncü operasyon alanı olarak ilan etmesiyle birlikte ittifak üyesi ülkeler arasında siber uzayda ortaya çıkabilecek tehditlere karşı kapasite geliştirme ve iş birliği oluşturma adına önemli adımlar atılmıştır. 2018 NATO Zirvesi'nde Brüksel'de yapılan toplantıda, müttefikler, NATO'nun güçlendirilmiş komuta yapısının bir parçası olarak Siber Uzay Harekât Merkezi kurma konusunda anlaşmışlardır. Ayrıca NATO ve Avrupa Birliği (AB), Şubat 2016'da siber savunma üzerine teknik düzenleme ile iş birliği yapmak konusunda anlaşmışlardır. Ortak zorluklar göz önüne alındığında, NATO ve AB, özellikle bilgi değişimi, eğitim, araştırma ve tatbikatlar alanlarında siber savunma üzerinde iş birliğini güçlendirmektedir. Yine Türkiye'nin de taraf olduğu ve 2001 yılında Budapeşte'de imzalanarak 2004 yılında yürürlüğe giren "Avrupa Siber Suçlar Sözleşmesi" ya da diğer adıyla "Sanal Ortamda İşlenen Suçlar Sözleşmesi" idealist düşüncenin savunduğu uluslararası iş birliği ve diyalog düşüncesinin siber uzay düzlemine bir yansıması olarak değerlendirilebilir.

İdealist yaklaşımın savunduğu hukukun üstünlüğü ve normlar ilkesi temelinde siber güvenlik alanında uluslararası hukuka saygı gösterilmesi ve ortak normlar ve kurallar geliştirilmesi savunulabilir. Bu, siber suçlara karşı mücadelede ve siber alanın düzenlenmesinde etkili bir yol olarak değerlendirilmektedir. Siber uzayın sınırsızlığı ve ülkelerin dışarıdan gelecek olan tehditlere açık olması bu bağlamda değerlendirildiğinde siber uzayın düzenlenmesi adına önemli bir konudur. Lakin henüz uluslararası düzeyde üzerine kabul görmüş bir siber uzay ya da siber güvenlik tanımı olmadığı gibi bu alanı düzenleyecek uluslar üstü bir yapının da varlığından söz etmek mümkün değildir.

İdealizmin temel ilkelerinden birisi olan insan haklarına ve demokratik değerlere saygı temelinde değerlendirildiğinde ise siber güvenlik önlemlerinin insan haklarına ve demokratik değerlere saygı göstererek uygulanması gerektiği sonucu ortaya çıkmaktadır. Devletlerin ve uluslararası kuruluşların, siber güvenlik politikaları

ve uygulamaları geliştirirken özgürlük, gizlilik ve ifade özgürlüğü gibi temel haklara dikkat etmeleri gerektiği savunulabilir. Artık hemen herkesin kullandığı akıllı telefonlar ve internet teknolojisi ile insanların siber uzaydaki özgürlük alanları, kişisel verilerinin güvenliği ve ifade özgürlüğü gibi kavramlar siber uzayda tehdit altında olan değerlerdir. İdealist güvenlik yaklaşımı çerçevesinde bakıldığında siber güvenlik alanında sağlanacak iş birliği ve hukuki düzenlemeler bireysel hak ve özgürlüklerin korunması anlamında katkı sağlayacaktır.

Siber güvenlik konusunda tüm devletlerin kapasitelerinin geliştirilmesinin önemi oldukça önemlidir. Gelişmiş ülkelerin, siber güvenlik konularında daha az gelişmiş ülkelere teknik yardım ve eğitim sağlaması küresel siber güvenlik düzeyini yükseltmeye ve güvensizliklerin azaltılmasına yardımcı olabilir. İdealist güvenlik yaklaşımı temelinde siber güvenlik konularında çok taraflı mekanizmaların ve süreçlerin önemi ortaya çıkmaktadır. Bu, devletlerin siber güvenlik ile ilgili endişelerini ve çözüm önerilerini paylaşabilecekleri ve ortak politikalar ve düzenlemeler oluşturabilecekleri uluslararası platformlar ve konferanslar şeklinde gerçekleştirilebilir. Siber güvenlik politikalarının ve stratejilerinin sürdürülebilir ve uzun vadeli hedeflere dayanması gerekliliği, siber güvenlik tehditlerine ve zorluklarına karşı etkili bir mücadele için devletlerin ve uluslararası kuruluşların sürekli iş birliği ve koordinasyon içinde olması gerektiği anlamına gelir.

İdealist güvenlik yaklaşımını benimseyen devletler ve uluslararası kuruluşlar, siber güvenlik olgusunu daha işbirlikçi, kapsayıcı ve insan haklarına duyarlı bir şekilde ele alarak, siber alanın düzenlenmesinde ve siber tehditlerle mücadelede daha etkili sonuçlar elde edebilir. Bu yaklaşım, küresel siber güvenlik düzeyinin yükseltilmesine ve siber alanda güvensizlik ve gerilimin azaltılmasına katkıda bulunabilir. Özetle, idealist güvenlik yaklaşımı bağlamında siber güvenlik olgusu değerlendirildiğinde uluslararası iş birliği, barış, hukukun üstünlüğü, insan hakları ve ekonomik kalkınma gibi değerlere vurgu yaparak, devletler ve uluslararası kuruluşlar arasındaki iş birliği ve ortak çözüm arayışı öne çıkmaktadır.

2.2. Liberalizm, Neo-Liberalizm ve Karşılıklı Bağımlılık Yaklaşımları Çerçevesinde Güvenlik ve Siber Uzay

Liberalizm, 17. ve 18. yüzyıllarda Aydınlanma Çağı olarak tanımlanan dönemde Batı'da ortaya çıkmış bir düşünce akımıdır. Bu dönemde, insan haklarına, bireysel özgürlüğe, anayasanın üstünlüğüne, kuvvetler ayrılığına ve rasyonel düşünceye yapılan vurgu liberalizmin temellerini oluşturmuştur. Liberal düşünce, bireysel hakları ve özgürlükleri koruma ve devletin gücünü sınırlama ihtiyacını vurgulayan bir dizi felsefi ve politik teoriye dayanmaktadır. Düşünceleriyle 17. yüzyılın sonları ve 18. yüzyılın başlarında felsefi düşünceye önemli katkıları olan John Locke'un felsefi ve politik çalışmaları liberalizmin temelini oluşturmuştur. Locke, her bireyin yaşama, özgürlüğe ve mülkiyet hakkına sahip olduğunu dile getirmiş ve bu hakların devlet tarafından korunması gerektiğini savunmuştur. Bu düşünceler, temelde devletin rolünün bireysel hakları koruma ve özgür bireylerin serbestçe faaliyet göstermesine izin veren liberal teorinin ana hatlarını oluşturmuştur (Shapiro, 2003).

Locke'un ortaya düşünceler daha sonrasında J.J. Rousseau, Adam Smith, Immanuel Kant ve John Stuart Mill gibi düşünürlerin siyasi ve iktisadi yaklaşımlarına temel oluşturmuştur. Devletin, toplumun daha geniş refahını ve sosyal adaleti teşvik etmek için daha aktif bir rol oynaması gerektiğini savunan sosyal liberalizm ve daha sonrasında devletin ekonomiye müdahalesini sınırlamayı ve serbest piyasa ekonomisini temel alan neo-liberalizm, bu düşünürlerin ortaya attığı farklı yaklaşımlarla temel bulmuştur. Bu düşüncelerin birleşimi, modern liberalizmin temelini oluşturmuştur ve bugün hala çok çeşitli politik ve ekonomik teorilere ve politikalara etki etmektedir.

Locke, insanların doğuştan gelen yaşam, özgürlük ve mülkiyet haklarının varlığını savunmuş ve hükümetlerin birincil görevinin bu temel hakları korumak olduğunu belirtmiştir. Locke ayrıca, hükümetlerin yasal olarak sadece halkın rızasıyla yönetebileceği görüşünü savunmuştur, bu da demokratik hükümetlerin temelini oluşturmakla birlikte yönetimin meşruiyetinin de temelidir. Hobbes'un aksine doğa durumunun herkesin birbiriyle savaş içerisinde olduğu durum olmadığını, bunun temelde özgürlük durumu olduğunu savunmuştur (Shapiro, 2003: 39).

Modern anlamda siyasi ve sosyal düşüncenin temellerini atan Rousseau, özgürlüğün ve eşitliğin önemini vurgulayan Toplum Sözleşmesi eserinde insanların özgür olarak doğduğunu ve sonradan köleleştirildiğini savunmuştur. Rousseau, Locke'un düşüncelerine benzer olarak insanların temelde barışçıl olduklarını ve toplumun bir parçası olmaya başladıklarında bu toplumun diğer üyeleriyle rekabet içerisine girmeye başladıklarını ve en sonunda da çatışma durumun ortaya çıktığını savunmuştur. Devleti özgürlük ve eşitlik temelinde bir toplumsal sözleşme üzerine kurulmuş siyasi bir yapılanma olarak tanımlayan Rousseau, bireylerin bu örgütlenmeye doğuştan gelen haklarla birlikte kendi kaderlerini tayin etme yetileriyle katıldıklarını savunmuştur (Morris, 1999). Dünya toplumu düşüncesinin kurucusu ve liberalizm düşüncesinin gelişmesinde önemli katkıları bulunan Kant, uluslararası ilişkiler ve etik üzerine düşünceleri ile öne çıkmıştır. Locke ve Rousseau'nun düşüncelerine paralel bir şekilde Kant'a göre, demokratik hükümetler daha barışçıldır ve demokrasinin yayılması dünya barışını teşvik edecektir. Ayrıca, insanların birbirlerine karşı etik yükümlülükleri olduğunu ve bu yükümlülüklerin hükümetler ve uluslararası ilişkiler tarafından da gözetilmesi gerektiğini savunan Kant'a göre savaşlar devletler arasındaki sorunların barışçıl yollarla çözümlendiği ve uluslararası kuruluşlarla oluşturulacak devletler üstü bir hukuk sisteminin savaşların önüne geçebileceğini savunmuştur (Kant, 1798).

Bu düşünürlerin her biri, liberal düşüncenin farklı yönlerini vurgulamış ve bu düşüncenin gelişimine katkıda bulunmuştur. Her biri, bireysel hakların, özgürlüğün ve rasyonel düşüncenin önemini vurgulamış, hükümetin ve ekonominin işleyişi üzerine düşüncelerini belirtmişlerdir.

Liberalizm özellikle uluslararası ilişkiler bağlamında değerlendirildiğinde devletlerin tek başlarına uluslararası ilişkilerin başat aktörleri olmadığını bunun yanında uluslararası örgütlerin, çok uluslu şirketlerin ve hatta kimi zaman bireylerin de uluslararası ilişkilerin aktörleri olabileceğini ve devletlerarası politikaları etkileyebileceklerini savunmuştur. Devletler arasındaki ilişkilerin anlaşılması için devletlerin toplumla olan ilişkilerinin anlaşılması gerektiğini vurgulayan liberalizme göre devletler ve devlet dışı aktörlerin karşılıklı olarak kurdukları iktisadi ya da siyasi temelde oluşturdukları karşılıklı bağımlılık devletlerin nasıl davrandığını yakından etkilemektedir (McGlinchey, Walters ve Scheinpflug, 2017: 22-26).

Liberalizmin temel prensipleri çerçevesinde güvenlik olgusu değerlendirildiğinde, güvenliğin genellikle hem bireysel hem de uluslararası düzeyde çok boyutlu bir şekilde ele alındığı görülmektedir. Liberalizm, bireysel hakların ve özgürlüklerin önemini vurgular. Bu bağlamda, güvenlik sadece devletlerin değil, aynı zamanda bireylerin de güvende olmasını kapsamaktadır. Bu nedenle, liberal güvenlik anlayışı, bireylerin yaşam, özgürlük, eşitlik, mahremiyet ve mülkiyet hakları gibi demokratik toplumlarda insan hakları kavramının temelini oluşturan hakların korunmasını içerir. Liberalizm güvenliği demokrasilerin birbirleriyle savaşmayacağı fikrini savunan demokratik barış teorisi temelinde ele alır. Bu teoriye göre, demokratik hükümetlerin çoğalması, uluslararası düzeyde barışı ve güvenliği artırabilir. Liberalizm, ekonomik bağımlılığın ve küreselleşmenin barışı teşvik ettiğini savunur. Liberalizme göre, ülkeler arasındaki ekonomik bağlar savaşın maliyetini artırır ve bu durum savaş çıkma olasılığını düşürür. Bu, ülkeler arasında bir tür negatif güvenlik bağımlılığı oluşturur (McGlinchey, Walters ve Scheinpflug, 2017: 27).

Liberalizm, uluslararası kurumların ve normların devletler arasındaki ilişkileri düzenleyerek ve barışı teşvik ederek uluslararası güvenliği artırabileceğini savunur. Bu kurumlar, devletler arasında iş birliğini teşvik eder ve çatışma durumunda arabuluculuk yapabilir. Ayrıca liberalizm, devletlerin eylemlerinin şeffaf olması gerektiğini vurgular. Bu, devletlerin birbirlerinin niyetlerini daha iyi anlamalarını ve yanıtlarını buna göre belirlemelerini sağlamakla birlikte güvenliği de artırabilir. Bu nedenle, liberal güvenlik anlayışı, bireysel hakların korunmasından, demokratik barış teorisine, ekonomik bağımlılığa, uluslararası kurumların önemine ve devletler arasındaki ilişkilerde şeffaflığa kadar geniş bir yelpazeyi kapsamaktadır (Henry, 2011).

Liberalizmin bireysel hakları ve özgürlükleri vurgulayan temel ilkeleri, siber güvenliğin sağlanmasında da önemlidir. Bireylerin kişisel bilgileri, ifade özgürlüğü ve bilgiye erişim hakları, birçok siber güvenlik politikasının merkezinde yer alır. Ayrıca, bireylerin siber saldırılara karşı korunması ve kişisel verilerinin gizliliği, liberal bir siber güvenlik politikasının önemli bir parçasını oluşturmaktadır. Siber uzayın güvenliği, daha önce de bahsedildiği üzere hem devlet hem de birey seviyesinde ele alınması gereken bir konu haline dönüşmüştür. İnternet teknolojisinin her alanda kullanılmaya başlanmasıyla birlikte bu alanda ortaya çıkan güvenlik tehditleri birey

seviyesinde oldukça yoğun bir şekilde ortaya çıkmaktadır. Kişilerin banka ve e-posta hesaplarına, sağlık kayıtlarına ya da dijital ortamda saklanan her türlü özel bilgilerine karşı gerçekleşen siber saldırılar liberalizmin ortaya koyduğu bireysel hak ve özgürlüklerin korunması prensibini ön plana çıkartmaktadır.

Fiziki sınırları olmayan siber uzayın güvenliği sorunsalının uluslararası bir sorun olduğu tartışılmaz bir gerçektir. Liberalizmin demokratik barış teorisi ve uluslararası iş birliği prensipleri bu noktada oldukça büyük önem taşımaktadır. Demokratik ülkelerin siber saldırılara karşı birlikte çalışması ve siber güvenlik normları ve standartları oluşturması liberal düşüncen kapsamında önemli bir yerde durmaktadır. Ayrıca, uluslararası kuruluşların siber güvenlik konularında iş birliği yapması ve bilgi paylaşması liberalizm temelinde değerlendirildiğinde teşvik edilen bir konu olarak değerlendirilebilir. Siber güvenlik alanında gerek uluslararası kuruluşların gerekse de devletlerin kendi aralarında yaptığı uluslararası iş birliği anlaşmaları bu durumun mevcut uluslararası sisteme bir yansıması şeklinde değerlendirilebilir. Avrupa Siber Suçlar Sözleşmesi, NATO'nun ittifak üyesi ülkeler arasında oluşturduğu siber güvenlik kapasitesinin geliştirilmesi noktasında yapmış olduğu çalışmalar ve siber güvenlik tatbikatları bu anlamda siber uzayın küresel olarak güvenliğinin sağlanması adına önem taşımaktadır.

Siber güvenlik aynı zamanda ekonomik bir meseledir. Ekonomik bağımlılık ve küreselleşme, siber güvenliğin önemini artırmaktadır. Bankacılık sistemlerine yapılacak bir siber saldırı devletler ve şirketler arasındaki para akışını etkileyebileceği gibi daha önce de üzerinde durulduğu üzere artık birçok sanayi üretim tesisinin kontrolünü sağlayan SCADA sistemlerine yapılacak saldırılar bir anda kritik öneme sahip ürünlerin üretiminde aksamalara neden olabilir. Ayrıca liberalizmin ekonomik prensiplerinin siber güvenlikte ekonomik istikrarın ve bilgi teknolojilerinin serbest hareketinin önemini vurguladığı söylenebilir. Tüm dünyanın kullandığı bilgisayar teknolojisinin belkemiğini oluşturan iletişim sistemleri Microsoft ve Apple'ın geliştirdiği işletim sistemleriyle kontrol edilmektedir (Statiste, 2023). Bu bağlamda sadece çok uluslu şirketler ve uluslararası organizasyonların iş birliği yetersizdir. Şirketler, bankalar ve devlet kurumlarının kullandığı bilgisayarların çok büyük çoğunluğunun bu iki büyük firma tarından üretildiği ve işletim sistemi olarak yine bu firmaların geliştirdiği sistemlerin kullanıldığı düşünüldüğünde, devletler ve özel

sektörün de siber uzayın güvenliğinin sağlanması noktasında iş birliği içerisinde olması bir gereklilik olarak görülmektedir. Liberalizm temelinde değerlendirildiğinde ayrıca devletlerin siber güvenlik politikalarının ve uygulamalarının şeffaf olması gereklidir. Bu, devletlerin birbirlerinin siber kapasitelerini ve niyetlerini daha iyi anlamalarını sağlayarak karşılıklı güveni ve iş birliğini teşvik edecektir. Liberalizmin öne sürdüğü uluslararası iş birliği ve diyalog düşüncesinin bu noktada devletler arasında ortaya çıkabilecek siber çatışmaları engelleyebileceği öngörülebilir.

2.3. Realizm ve Neo-realizm Temelinde Güvenlik Algısı ve Siber Uzayın Güvenliği

Realizm, çağdaş güvenlik çalışmalarını anlayabilmek için oldukça önemlidir. Toplumlar arasındaki şiddet ve güvenlik hakkında geliştirilen en etkili teorilerin birçoğu bu entelektüel geleneğin içine dahildir. Ayrıca birçok ülkede realizm, dış politika üzerine yapılan başlıca tartışmalarda araştırmacıların ve bu konu üzerine çalışan kişilerin başvurduğu önemli bir öğreti olarak karşımıza çıkmaktadır. Yükselen bir Çin ve yeniden güçlenen bir Rusya, Batı-egemen uluslararası sistemin istikrarı konusundaki rahatlığı sarstığı için realizmin güç kaymaları ve güç politikalarına odaklanması oldukça önemlidir (Wohlforth, 2020: 11).

Realizm, özellikle uluslararası ilişkilerin rekabetçi ve çatışmacı yanını vurgulayan bir düşünce ekolü olarak literatürde yerini almaktadır. Realizmin köklerinin, insanlığın en erken tarihsel yazılarında, özellikle MÖ 431 ve 404 yılları arasında yaşanan Peloponez Savaşlarının tarihçesini anlatan Thucydides'in çalışmalarından geldiği sıklıkla belirtilir. Elbette iki bin yıl önce Thucydides'in bir realist olduğunu söylemek mümkün değildir. Ancak, çağdaş bir bakış açısıyla geriye bakıldığında, teorisyenler, antik dünyanın ve modern dünyanın düşünce kalıpları ve davranışları arasında birçok benzerlik tespit etmişlerdir. Daha sonra tüm insanlık tarihini kapsayan zamansız bir teori fikrini desteklemek için onun ve diğerlerinin fikirleri çerçevesinde bugün modern anlamda kullanılan realizm fikrini ortaya çıkartmışlardır.

Devletlerin uluslararası ilişkilerin ana aktörü olduğu temel varsayımı üzerine gelişen realist düşünce, diğer kurumlar, bireyler ve organizasyonlarında uluslararası ilişkilerin birer aktörü olabileceğini fakat güçlerinin sınırlı olduğunu savunmaktadır.

Devletleri üniter yapılar olarak kabul eden realist düşüncenin temelinde ulusal çıkar kavramı politika yapıcılar için rasyonel karar almada ön planda tutulan bir faktördür. Realizm sıklıkla tarihten örnekler üzerinden ilerlediği için insanın doğasında bulunan ve tekrarlayan davranış kalıplarına rehin olduğu fikrine önemli bir vurgu yapmaktadır. Bu varsayımın merkezinde insanların bencil olduğu ve güce sahip olma isteği görüşü yer alır. Herz (1951), Hobbes'un düşüncelerine paralel olarak, insanoğlunun hayattaki mücadelesinin altında yatan temel nedenin güvenlik edinme çabası olduğunu ve bunu içerisinde bulunduğu durumun şartlarına göre doğuştan gelen bazı içgüdüsel davranışlarla gerçekleştirmeye çalıştığını söylemektedir. İnsanoğlunun hayatta kalabilme mücadelesinde farklı motivasyonların yer aldığını, bunun kimi zaman etrafındaki düşmanlara karşı güvenliğini sağlamak, kimi zaman ekonomik olarak güvende hissetmek ve kimi zamanda sadece prestij sahibi olmak adına yaptığını ve tüm bunların gerçekleşmesi için ise gücün gerekli olduğunu vurgulamaktadır (Herz, 1951: 2-5).

Herz'in realist teori kapsamında literatüre yaptığı en büyük katkı ise "güvenlik ikilemi" olarak adlandırılan ve devletlerin güvenlik bağlamında silahlanma yoluna gitmeleriyle birlikte ortaya çıkardıkları güvensizlik ortamını ifade eden kavramdır. Özellikle siber uzayda devletlerin ofansif olarak aldığı güvenlik tehditlerinin yanında uluslararası örgütler ve hatta bireylerin bu anlamda kapasite geliştirme yoluna gitmeleri güvenlik ikilemi kavramı bağlamında oldukça önemlidir.

Snyder'a göre (1984) uluslararası sistemde aktörlerin diğerlerinin niyetleri hakkındaki kesin olmayan belirsizliği göz önüne alındığında, bir aktör tarafından alınan güvenlik önlemleri diğerleri tarafından tehdit olarak algılanır ve diğerleri kendilerini korumak için bu önlemlere karşı yeni adımlar atarlar. Bu adımlar, ilk aktör tarafından diğerlerinin tehlikeli olduğu başlangıçtaki hipotezinin doğrulanması olarak yorumlanır ve böylece bu durum gerçek olmayan korkular ve gereksiz savunmaların bir döngüsünde devam eder (Snyder, 1984). Bu durum güvenlik ikilemi teorisinde ortaya atılan güvensiz ortamın nasıl doğduğuna işaret etmektedir.

Bir devlet kendini savunma amaçlı silahlanırken diğerlerini istemeden güvenliğini azaltabilir ve bunun sonucunda diğer devletlerin karşılık olarak silahlanmalarını teşvik edebilir. Kendini savunma amacıyla bir devlet silahlanırken,

istemeden başka bir sonuç ortaya çıkabilir ve bu da aslında kendi güvenliğini azaltabilir. Bu istenmeyen etkilerden biri, diğer devletlerde yarattığı güvensizliktir ve bu da diğer devletlerin silahlanarak kendilerini koruma ihtiyacı duymalarına neden olabilir. Güvenlik ikilemi, bir devletin kendi güvenliğini artırmak için yaptığı çabaların diğer devletler tarafından bir tehdit olarak algılanması durumunda ortaya çıkar. Sonuç olarak, diğer devletler bu algılanan tehdide karşı kendilerini korumak için kendi askeri kabiliyetlerini artırmak zorunda hissedebilirler. Bu durum da silahlanma yarışlarına ve devletler arasındaki gerginliklerin artmasına yol açabilir (Jervis, 1978: 168). Güvenlik ikilemi, komşu iki devletin klasik senaryosu gibi durumlarda ortaya çıkar. Bir devlet kendini savunma amacıyla askeri kabiliyetlerini artırdığında, diğer devlet bunu potansiyel bir tehdit olarak algılayabilir ve kendi askeri kabiliyetlerini artırarak yanıt verebilir. Bu karşılıklı eylem-reaksiyon dinamiği gerilimleri tırmandırabilir ve tüm taraflar için daha az güvenli bir ortam yaratabilir. Güvenlik ikilemi, sadece askeri araçlarla güvenliği sağlamanın doğal zorluklarını vurgular. Bu durum, savunma amaçlı eylemlerin bile istemeden gerilimleri artırarak daha az güvenli bir uluslararası sistem ortaya çıkartabileceğini göstermektedir (Glaser, 1997: 174-177).

Realistler, insanoğlunun bencilliğinin, güç hırsının ve başkalarına güvenme yeteneğinin eksikliğinin tahmin edilebilir sonuçlara yol açtığına inanmaktadır. Belki de bu yüzden savaş denilen olgu tarih boyunca bu kadar yaygın olmuştur. Bireyler devletlere organize olduğundan insan doğası devlet davranışını etkilemektedir (Herz, 1951: 19). Bu konuda, Niccolò Machiavelli temel insan özelliklerinin devletin güvenliğini nasıl etkilediğine odaklanmıştır. Machiavelli, bir liderin öncelikli endişesinin ulusal güvenliği teşvik ve inşa etmek olduğunu vurgulamıştır. Bu görevi başarıyla yerine getirebilmek için liderin uyanık olması ve hem iç hem de dış tehditlerle etkili bir şekilde başa çıkması gerektiğini söyleyen Machiavelli, bir liderin hem bir aslan hem de bir tilki olması gerektiğini söylemiştir. Güç (aslan) ve aldatma (tilki), dış politikanın yürütülmesi için kritik araçlardır. Machiavelli'nin görüşünde liderler ortalama vatandaşı yönlendiren geleneksel dini ahlaka değil sorumluluk etiğine uymalıdırlar. Yani mümkün olduğunda iyi, gerektiğinde ise devletin hayatta kalmasını sağlamak için şiddeti kullanmaya da istekli olmalıdırlar (Machiavelli, 2021: 95).

Realizm birçok düşünür tarafından farklı dönemlerde ele alınmış ve tanımlanmaya çalışılmıştır. Yapılan bu çalışmalar temelde Nicolo Machiavelli ve Thomas Hobbes'un toplum ve siyaset üzerine ortaya koydukları düşünceler temelinde ortaya çıkmıştır. Bugünün realist düşüncesinin kurumsallaşmasında ortaya çıkan düşünürler ise yapmış oldukları çalışmaları Machiavelli ve Hobbes'un toplum ve siyaset üzerine geliştirdikleri düşünceler üzerinden oluşturmuşlardır.

Waltz (1979) realist düşünceyi devletlerin çıkarı temelinde değerlendirmiştir. Waltz'a göre devletin çıkarı, hareketin kaynağını sağlar ve politikanın gereklilikleri, devletler arasındaki düzensiz rekabetten doğmaktadır. Bu gerekliliklere dayalı hesaplama ise bir devletin çıkarlarına en iyi hizmet edecek politikaları ortaya çıkarabilir. Başarı politikanın en nihai testidir ve başarı, devletin korunması ve güçlendirilmesi olarak tanımlanır. (Waltz, 1979: 117). Morgehenthau (1960) ise realizmi insan doğasında var olan güç edinme gereksinimi üzerine temellendirmiştir. Morghentau'ya göre politika, insan doğasının kökeninde olan objektif yasalar tarafından yönetilmektedir. Realizm düşüncesinin uluslararası siyaset sistemi içerisinde yolunu bulmasında baz aldığı temel konu güç açısından tanımlanan çıkar kavramıdır. Güç ve çıkar içerik açısından değişkendir ve evrensel ahlaki prensipler devletlerin eylemlerine uygulanamaz. Politik realizm, belirli bir ulusun ahlaki arzularını evreni yöneten ahlaki yasalarla özdeşleştirmeyi reddeder (Morgenthau, 1967: 4-10).

Mearsheimer (1994) devletleri rasyonel varlıklar olarak kabul eder ve anarşik uluslararası sistem içerisinde devletler doğal olarak bazı saldırgan askeri yeteneklere sahiptir. Bu durum devletlere birbirlerine zarar verme ve hatta yok etme gücü vermektedir. Hiçbir devlet başka bir devletin saldırgan askeri yeteneklerini kendisine karşı kullanmayacağından emin olamaz. Yani devletler her zaman potansiyel bir saldırıya karşı bir beklenti içerisindedirler ve hazır olmalılardır. Devletleri harekete geçiren en temel motivasyon ise hayatta kalmaktır (Mearsheimer, 1994: 9-10). Realizmin önemli temsilcilerinden bir diğer isim olan Gilpin'e göre ise sosyal ve siyasi ilişkilerin temel birimleri birbirleri arasında çatışma içerisinde bulunan gruplardır. Devletlerin başlıca motivasyonu ulusal çıkarlarıdır ve güç ilişkileri uluslararası ilişkilerin temel bir özelliğidir (Gilpin, 1996: 7-8). Carr (1964), tarih neden-sonuç ilişkilerinin bir dizisidir ve seyrinin entelektüel çabalarla anlaşılabileceğini ancak

hayal gücü tarafından yönlendirilemeyeceğini söylemiştir. Carr'a göre teori pratik yaratmaz ancak pratik teoriyi yaratır ve politika etik işlevi değildir, fakat etik politikanın işlevini belirler (Carr, 1964: 63-64). Realizmin en önemli temsilcilerinden birisi olan Carr, bu düşünceleriyle idealizmin eleştirisini yapmış ve aslında uluslararası sitemde ne olması gerektiği ile ilgili değil de ne olduğuyla, yani pratikte var olanla uğraşılması gerektiğini söylemiştir.

Gilpin (1996) realizmin temelinin Aristoteles'in insanın bir siyasi hayvan olduğu gözlemine dayandırmaktadır. İnsanlar, bağlılık gösterdikleri ve ölmeye bile razı oldukları sosyal grupların üyeleri olarak varoluş nedenlerini bulurlar ve liberal teoride var olduğu varsayılan yalnız bireyler değillerdir. Sosyal ve siyasi etkileşimlerin temel birimi, grubun kendisi veya *"çatışma grubu"* olarak adlandırılan şeydir. Ancak, çatışma gruplarının doğası ekonomik, teknolojik ve diğer gelişmelerle birlikte sürekli değişmiştir. Örneğin, Aristoteles'in Yunanistan'ında temel birim polis veya şehir devletiydi. Ancak modern dünyada başlıca çatışma grupları ulus devletler olarak karşımıza çıkmaktadır. Modern devlet askeri gücü düzenleme, ekonomik işleri yönetme ve güvenlik sağlama konusunda daha etkili olduğu için önceki türdeki siyasi varlıkları, örneğin kabileleri ve imparatorlukları yerinden etmiştir. Bu nedenlerle bireyler, bağlılıklarını diğer siyasi varlıklardan devlete devretmişlerdir. Devlet ve birey arasındaki bu ilişki ise bir çıkar-fayda ilişkisi şeklinde devam etmektedir (Giplin, 1996: 7).

Realizm siyasi düzen ile güvenlik arasındaki ilişkiyi aydınlatmak için tüm bu varsayımlardan yola çıkmaktadır. Eğer bireyler arasındaki etkileşimler gerçekten bir grup üyesi gibi düşünme ve hareket etme eğilimi (*groupism*)[8], bencillik ve güç-merkezcilikle karakterize ediliyorsa, o zaman politika bir düzeni uygulayacak bir merkezi otorite olmadıkça çatışmalı olma eğilimindedir. Anlaşmaları uygulayacak bir otorite olmadığında, yani anarşi durumunda, herhangi bir aktör istediğini elde etmek için güce başvurabilir. Bir aktör bugün hiç kimsenin silaha sarılmayacağından oldukça

[8] Wohlforth (2016) "*Realism and Security Studies*" isimli makalesinde realizminin üç temel varsayımından birisi olarak tanımladığı "*groupism*" kavramının tam olarak bir Türkçe karşılığı olmasa da Merriam-Webster sözlüğünde "*bir grup üyesi gibi düşünme ve hareket etme eğilimi: bireysellik ve kültürel çeşitlilik aleyhine bir grup kültürünün normlarına uyum sağlama eğilimi*" şeklinde tanımlanmıştır. Detaylı bilgi için bkz. https://www.merriam-webster.com/dictionary/groupism

emin olsa bile, yarın birisinin bunu yapabilme olasılığı her zaman vardır. Bu nedenle herkes bu olasılığa karşı hazırlıklı olma eğilimindedir. Eğer aktörler bir anlaşmayı uygulamak için üst düzey bir otoriteye güvenebilseydi kolayca çözülebilecek anlaşmazlıklar savaşa varmadan çözülebilme ihtimaline sahip olabilirdi. Bu nedenle realizmin temel argümanı anarşinin güvenliği sorunlu ve potansiyel olarak çatışmalı bir hale getirdiği ve savaşın temel nedenlerinden biri olduğudur (Wohlforth, 2020).

2.3.1. Neo-Realizm ve Güvenlik

Realizm, açık bir dizi varsayım ve öneriyle tanımlanan bir teori değildir. Realizm, kendilerini belirli bir analiz tarzı veya geleneğin içine yerleştiren ve bu şekilde sınırlayan bir dizi analistin çalışmalarıyla özellikle I. Dünya Savaşı'ndan günümüze şekillenerek ortaya çıkmış bir öğretidir. Donnelly realizmi birçok farklı araştırmacının da belirttiği üzere genel bir yönelim, felsefi bir eğilim, teoriyi şekillendiren normatif vurgular ya da bir düşünce tarzı şeklinde tanımlanmaktadır (Donnelly, 2000: 6). Yapılan çalışmalar birçok farklı tarz veya geleneğin içerisinden çıkarak realizm öğretisini zaman içerisinde uluslararası sistemin içerisinde bulunduğu zaman ve duruma bağlı olarak eleştirmiş ve bugün üzerine çalışılan farklı realist teorilerin ortaya çıkmasını sağlamışlardır.

Realizme yönelik bilimsel eleştirilerin 1960'lar ve 1970'lerde artması ve siyasetin bilimsel bir yaklaşımla incelenmesine olan ilginin özellikle ABD'de popüler hale gelmesi, realist düşüncede farklı yaklaşımların ortaya çıkmasına neden olmuş ve realist düşünce çatısı altında farklı teoriler üretilmeye başlanmıştır. Bu bağlamda Kenneth Waltz, bazı temel realist fikirleri tümden gelim yöntemiyle yukarıdan aşağıya bir teorik çerçeveye dönüştürerek realist düşünceyi canlandırmaya çalışmıştır. Bu yaklaşım, başlangıçta "yapısal gerçekçilik" olarak bilinse de günümüzde genellikle neo-realizm olarak adlandırılmaktadır (Wohlforth, 2020).

Kenneth Waltz'un 1979 tarihli "Theory of International Politics" kitabı uluslararası ilişkiler alanında yapılan akademik çalışmalarda uzun bir süre boyunca en etkili teorik çalışmalardan birisi olmuş ve çağdaş neo-realizmin ana metni haline gelmiştir. Devletlerin ve diğer uluslararası aktörlerin özellikleri ve etkileşimleri açısından büyük farklılıklar olmasına rağmen Waltz (1979), tarih boyunca uluslararası hayatın işleyişinde dikkat çekici bir benzerlik olduğuna dikkat çekmiştir ve bu

benzerliklerin uluslararası sistemde var olan kalıcı anarşinin yapısından kaynaklandığını söylemiştir. Waltz'a göre siyasi yapılar öncelikle düzenleme prensipleri tarafından tanımlanır ve ayırt edilir. Siyasi aktörlerin otorite ve itaat ilişkileri hiyerarşik olarak düzenlenmiş veya düzenlenmemiş bir şekilde gerçekleşebilir. Uluslararası sistemin anarşik düzeni içerisinde düzen bir üst otorite tarafından dayatılmaz ve bu düzen eşit statüdeki siyasi aktörlerin etkileşiminden ortaya çıkar. Anarşinin olduğu düzenlerde ise Waltz'a göre her devlet ayrı, özerk ve resmi olarak eşit bir siyasi birimdir ve çıkarlarını gerçekleştirmek için nihayetinde kendi kaynaklarına güvenmek zorundadır. Anarşinin bulunduğu ortamlarda "*her bir birimin teşvik edici nedeni kendisini kendi ihtiyaçlarını karşılayabilecek bir konuma koymaktır çünkü başka birine güvenmek mümkün değildir*" (Waltz, 1979: 107). Bu nedenle, tüm önemli işlevler her bir devlet tarafından gerçekleştirilmelidir. Uluslararası siyasette politik iş bölümü çok azdır ve devletler arasında görevlerin keskin bir farklılaşması yoktur (Waltz, 1979: 93-97).

Realizmde devletlerin güç ve ulusal çıkar üzerine kurulmuş olan ana amaçlarının neo-realizmde bu olgulardan kayarak güvenliğe odaklandığı görülür. Waltz'ın da belirttiği üzere devletlerin ana amaçları hayatta kalmaktır (Waltz, 1979: 98) ve bu noktada bunu sağlayabilmek için devletler bir üst otoritenin bulunmadığı anarşik uluslararası siyasal ortamda her zaman hazırlıklı olmalıdırlar ve bu bağlamda gerekli olan hazırlıkları her zaman en üst seviyede tutmalıdırlar (Mearsheimer, 2013: 77-80). Bu noktada neo-realizmin sorguladığı asıl önemli olan konu ise klasik realizmde devletlerin güç edinme amacının devletlerin hayatta kalabilme arzusu temelinde güvenliklerini en üst seviyede tutmak noktasında bunu sağlayacakları konusudur. Klasik realizmde özellikle Morgenthau'nun insanların doğasında bulunan güç edinme arzusunun devletlerin de doğasında bulunduğu fikri (Morgenthau, 1967) neo-realizmde farklı bir şekilde algılanmıştır. Neo-realizmde insanoğlunun doğasında bulunan güç edinme arzusu ile devletlere atfedilen aynı arzu arasındaki ilişkinin düşük bir seviyede olduğu vurgulanmıştır ve bir üst otoritenin bulunmadığı uluslararası siyasi sistem içerisinde devletlerin kendi güvenliklerini sağlamak amacıyla güç edinme isteği içerisinde olmakla birlikte hayatta kalabilmek için tek seçenekleri de budur (Mearsheimer, 2013: 77-80).

Neo-realist teoriler, devletler arasındaki kültürel farklılıkları ve siyasal sitemlerindeki farklılıkları göz ardı etmektedir çünkü uluslararası sistem tüm büyük güçler için aynı temel olanakları yaratmaktadır. Bir devletin demokratik mi yoksa otokratik mi olduğu, diğer devletlere karşı nasıl davrandığı konusunda nispeten daha az öneme sahiptir. Bir devlette dış politikayı yürüten kişinin kim olduğu da neo-realizmde pek önemli değildir. Neo-realizmde daha önce de belirtildiği üzere devletlerin benzer oldukları varsayılır. Tek farklılık bazı devletlerin diğerlerinden daha güçlü veya daha zayıf olmasıdır. Neo-realizmin odaklandığı nokta olan devletlerin hayatta kalmak için edinmeye çalıştıkları gücün niteliğidir. Kenneth Waltz gibi defansif realistler (1979), dünya gücünün payını maksimize etmeye çalışmanın akıllıca olmadığını savunur. Çünkü çok fazla güç elde etmeye çalışan devletler sistem tarafından cezalandırılacaktır. Hegemonya arayışının özellikle aptalca olduğunu iddia ederler. John Mearsheimer gibi ofansif realistler ise tam tersini savunurlar. Mümkün olduğunca çok güç elde etmenin ve durum uygun olduğunda hegemonya arayışında bulunmanın stratejik açıdan mantıklı olduğunu savunurlar. Bu argüman, fethetme veya hükmetme eyleminin kendiliğinden iyi olduğunu değil, aşırı güce sahip olmanın hayatta kalmanın en iyi yolu olduğudur. Klasik realistlere göre güç, devletler için bir amaçtır. Neo-realistlere göre ise güç, bir amaç için bir araçtır ve nihai amaç hayatta kalmaktır. Güç, bir devletin kontrol ettiği maddi yeteneklere dayanır. Güç dengesi, öncelikle bir devletin sahip olduğu silahlı kuvvetler ve nükleer silahlar gibi devletlerin sahip olduğu somut askeri varlıkların bir fonksiyonudur. Bununla birlikte devletlerin ikinci bir tür gücü vardır ve bu askeri güç oluşturmak için gereken sosyo-ekonomik unsurları ifade eder. Büyük güçler, askeri güçlerini inşa etmek ve savaşmak için para, teknoloji ve personele ihtiyaç duyarlar ve bir devletin ikincil gücü, rakip devletlerle rekabet ederken kullanabileceği ana potansiyeli ifade eder. Bu tartışmadan açıkça anlaşılmalıdır ki, devletlerin güç kazanabilecekleri tek yol savaş değildir (Mearsheimer, 2013: 80).

2.3.2. Güvenlikleştirme Kavramı

Realizm ve neo-realizm çalışmalarının 1980'li yılların ortalarından sonra özellikle Sovyetlerin dağılma sürecine girmesi ve Soğuk Savaş döneminin sona doğru yaklaştığının görüldüğü dönemde Buzan önderliğinde realist düşüncenin önemli isimlerinin Kopenhag Üniversitesi'nde yaptıkları güvenlik çalışmaları sonucunda

ortaya çıkan "güvenlikleştirme" (securitization) kavramı, devletlerin ulusal güvenlik konularını nasıl ele aldığını ve tehdit oluşturduğu düşünülen konuların nasıl bir ulusal güvenlik meselesi haline geldiğine dair farklı yaklaşımların ortaya çıkmasını sağlamıştır.

Güvenlikleştirme, bir konunun veya bir meselenin güvenlik alanına dahil edilmesi veya güvenlik açısından önemli bir konu olarak kabul edilmesidir. Güvenlikleştirme süreci belirli bir tehdidin veya riskin tanımlanması, anlamlandırılması ve güvenlik gündemine dahil edilmesini içerir. Güvenlikleştirme, bir konunun sadece güvenlik boyutunu vurgulamakla kalmaz aynı zamanda o konunun diğer alanlardaki politika tartışmalarından veya çözüm arayışlarından ayrılmasına da yol açabilir. Bu süreç, belirli bir tehdidin veya riskin güvenlik politikaları ve güvenlik önlemleriyle ele alınması gereken bir mesele olarak algılanmasını sağlar. Güvenlikleştirme süreci genellikle bir dizi aktör tarafından gerçekleştirilir. Devletler, uluslararası örgütler, medya, sivil toplum kuruluşları veya diğer ilgili paydaşlar belirli bir konuyu güvenlik gündemine taşımak için çaba gösterebilirler. Bu çabalar, kamuoyu oluşturma, politika yapım süreçlerine müdahale etme veya güvenlik politikalarının şekillenmesine katkıda bulunma yoluyla gerçekleşebilir. Güvenlikleştirme objektif bir gerçekliği yansıtmak yerine, konuların ve sorunların belirli bir güvenlik çerçevesine yerleştirilmesiyle ilişkilidir. Bu durum güvenlik meselelerinin tanımlanması, önceliklendirilmesi ve çözümlenmesi sürecinde siyasi ve toplumsal tercihlerin etkisini yansıtır (Buzan ve Wæver, 2009: 255-58).

Ancak güvenlikleştirme süreci eleştirel olarak da incelenebilir. Kavram belirli bir tehdidin abartılmasına, aşırı militarizasyona veya olağan dışı güvenlik önlemlerine yol açabileceği endişesiyle eleştirilmektedir. Ayrıca güvenlikleştirme süreci, bazı konuların diğer önemli politika tartışmalarından veya alternatif çözüm yollarından dışlanmasına neden olabilir. Genel olarak güvenlikleştirme bir konunun güvenlik gündemine dahil edilmesi ve güvenlik perspektifiyle ele alınmasını ifade eder. Bu süreç politika yapımında ve güvenlik politikalarının şekillenmesinde etkili olabilir ancak eleştirel bir değerlendirme gerektirir. Güvenlikleştirme süreci genellikle politik bir süreçtir ve belirli bir tehdidin veya sorunun güvenlik meselesi olarak tanımlanması, toplumda bir endişe yaratması ve güvenlik önlemlerinin uygulanması ile sonuçlanabilir. Bununla birlikte güvenlikleştirme eleştirel bir perspektiften de ele

alınabilir ve politikaların belirli bir tehdit veya sorunu abartarak aşırı güvenlikleştirme olarak adlandırılan durumda olmasıyla ilgili tartışmaları da içerebilir. Güvenlikleştirme, güvenlik politikalarının belirlenmesi ve uygulanmasında önemli bir rol oynar ve belirli bir sorunun veya tehdidin güvenlikleştirilmesi politika yapıcılar tarafından o konuya daha fazla dikkat ve kaynak ayrılmasına yol açabilir. Ancak bu süreçte dikkate alınması gereken eleştirel bir perspektif ve dengeli bir yaklaşım da önemlidir (Buzan, 1987).

2.3.3. Realizm ve Neo-Realizm Temelinde Siber Güvenlik ve Güvenlikleştirilen Siber Uzay

Devletlerin uluslararası sistem içerisinde hayatta kalma amacıyla kendi ulusal çıkarlarını koruma eğiliminde olduğunu ve bu çıkarların genellikle güç ve güvenlik üzerine odaklandığını öne süren realist teori, uluslararası sistemin anarşik bir yapıda olduğunu ve devletlerin güvenliğini garanti altına almak için her zaman hazırlıklı olmak zorunda olduklarına ek olarak bu konuda kendi kaynaklarına dayanmak zorunda olduklarını da belirtmektedir. Siber güvenlik olgusu realizmin öne sürdüğü temel düşünceler altında ele alındığında, bu yapı ve dinamiklerle iç içe geçtiği görülmektedir.

Realist teorinin ortaya attığı uluslararası sistemdeki anarşi, sınırları olmayan ve kontrol edilemeyen bir biçimde genişleyerek hayatın her alanına tezahür eden siber uzay için kullanılabilecek bir tanımlamadır. Geldiğimiz noktada siber uzay tam olarak bir anarşi ortamını yansıtmaktadır. Herhangi bir üst otoritenin olmadığı, kontrol edilmesi oldukça güç olan ve insan eliyle üretilmiş bu yeni alan bir kuralsızlıklar dizini şeklinde günden güne genişlemektedir. Her ne kadar ülkelerin kendi hukuk sistemlerinde siber uzayın güvenliğini sağlamak adına yaptıkları yasal düzenlemeler olsa da bu durum sınırları olmayan bu yeni alanın uluslararası anlamda güvenliğinin sağlanmasında yeterli değildir. Siber uzayda ortaya çıkan tehditler, çatışmalar ya da suçlar tek bir coğrafyayla sınırlı değildir. Zaten klasik anlamda bir siber coğrafya olarak tanımlanabilecek herhangi bir alan da yoktur. İnternete erişimin olduğu her mekân siber uzayın bir parçası olarak değerlendirilebilir. Dolayısıyla bu alanda ortaya çıkan ya da çıkması muhtemel güvenlik tehditlerini kontrol altında tutabilecek bir otoritenin yoksunluğu siber uzayı realist teorinin ortaya koyduğu ve anarşinin hâkim

olduğu uluslararası sistemin bir parçası haline getirmektedir. Bu bağlamda devletler, siber uzayda güvenliğin garanti edilememesinin, bu alanın anarşi düzeninin bir sonucu olduğunun farkında olarak siber saldırılara karşı kendilerini korumak için sürekli bir çaba içindedirler. Devletlerin bu bağlamada iç hukuk sistemlerinde yaptıkları yasal düzenlemeler, oluşturdukları siber güvenlik kurum ve kuruluşları, siber güvenliğin sağlanması noktasında yetişmiş nitelikli elemanların temin edilmesi için oluşturulan eğitim kurumları ve programlar bu çerçevede değerlendirilebilir. Günümüzde birçok ülke siber güvenlik tehditlerinin farkında olarak bu alanda güvenliğin sağlanması adına farklı girişimlerde bulunmaktadırlar. Örneğin Türkiye'nin bu alanın güvenliğini sağlamak için gerek yaptığı yasal düzenlemeler gerekse de oluşturduğu yeni birimler bu durumun bir örneğini teşkil etmektedir.

1990'lı yılların başında konunun öneminin farkına varan Türkiye, siber alan ile ilgili olarak ilk defa 6 Haziran 1991 tarihinde 3756 Sayılı Türk Ceza Kanunu'nun Bazı Maddelerinin Değiştirilmesine Dair Kanun ile siber uzayda işlenen suçlar bağlamında bir düzenlemeye gitmiştir. Bu kanunun 20. Maddesinde "Bilişim Alanında Suçlar" başlığı altında bilgileri otomatik işleme tabi tutulmuş bir sistemden programların, verilerin veya diğer unsurların hukuka aykırı olarak ele geçirilmesi veya bunların başkasına zarar vermek üzere kullanılması, nakledilmesi veya çoğaltılması yasayla ceza unsuru olarak kabul edilmiş ve bu cezanın hükümleri düzenlenmiştir (Resmî Gazete, 1991, 3756 Sayılı Kanun). Bu yasal düzenlemeye ek olarak geçtiğimiz son yirmi yıl içerisinde yasal zeminde birçok farklı düzenleme yapılmıştır. 5651 sayılı "İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun" (Resmî Gazete, 2008, 5651 Sayılı Kanun), 2008 yılında kabul edilen 5809 sayılı "Elektronik Haberleşme Kanunu" (Resmî Gazete, 2008, 5809 Sayılı Kanun) ve 6698 sayılı "Kişisel Verilerin Korunması Kanunu" (Resmî Gazete, 2016, 6698 Sayılı Kanun) gibi kanunlar yapılan bu düzenlemelerin örnekleri olarak karşımıza çıkmaktadır.

Benzer şekilde Ulusal Siber Olaylara Müdahale Merkezinin (USOM) oluşturulması ile Siber Olaylara Müdahale Ekiplerinin (SOME), siber suçlarla mücadele ve istihbarat faaliyetleri yürüten kurumlar içerisine kolluk kuvvetlerini oluşturan kurumların siber güvenlik ile ilgili oluşturdukları alt birimler, daha önce 2011 yılında kurulan "Emniyet Genel Müdürlüğü, Bilişim Suçlarıyla Mücadele Daire

Başkanlığı" ve sonrasında 2013 yılında isim değiştirerek faaliyetlerine devam eden "Siber Suçlarla Mücadele Daire Başkanlığı", "Jandarma Genel Komutanlığı Muhabere Elektronik Bilgi Sistemleri Başkanlığı ve Siber Suçlarla Mücadele Daire Başkanlığı", "Bilgi Teknolojileri ve İletişim Kurumu" ve "Türk Silahlı Kuvvetleri Siber Savunma Komutanlığı" gibi kurumlar bu bağlamda siber uzayın anarşi ortamında siber güç kazanımı ve kapasite artırımı ile güvenliğin tesis edilmesi adına atılan adımlar olarak değerlendirilebilir.

Realizmin ileri sürdüğü devletlerin kendi çıkarlarını korumak ve hayatta kalmak adına güç edinme isteği temelinde devletlerin siber güvenlik kapasitelerini artırmaya çalışmaları hem kendilerini siber tehditlere karşı koruma yeteneklerini geliştirmeye, hem de potansiyel rakiplerine karşı siber güç kullanma kapasitelerini artırmaya çalışmaları olarak değerlendirilebilir. Realizm, devletlerin gücünü kullanarak potansiyel saldırganları caydırma eğiliminde olduğunu savunur. Bu, siber güvenlik bağlamında devletlerin siber saldırılara karşı caydırıcı bir güç oluşturmayı hedeflemesini ve böylece diğer devletleri kendi siber altyapılarına saldırmaktan caydırmayı hedeflemesini içermektedir. Daha önce siber savaş konusunda belirtildiği üzere siber uzay ve bu alanda gerçekleştirilen saldırılar modern savaşın kaçınılmaz bir parçası haline gelmiştir. Devletler siber uzaydaki ulusal çıkarlarını korumak ve güçlerini artırmak için yatırım yapmakta ve teknolojilerini geliştirme çabası içerisindedirler. Dolayısıyla siber güvenliğin devletlerin ulusal çıkarlarını koruma ve güçlerini artırma çabalarının bir parçası olduğu gerçeği ve bu çabaların anarşik uluslararası siber sistemin yapısal dinamiklerinden doğduğunu söylemek mümkündür.

Realist teori, insan doğasının temelde bencil ve rekabetçi olduğunu öne sürer. İnsanların kendi çıkarları için hareket etme eğiliminde olduğunu, güç peşinde koştuğunu ve diğerlerinin üzerinde üstünlük sağlama arzusu olduğunu belirtir. Bu görüş, siber uzayda bireylerin ve devletlerin nasıl hareket ettiğini anlamada önemli bir çerçeve sağlamaktadır. Realist teorinin öne sürdüğü bencil insan doğası, bireylerin siber uzayda nasıl hareket ettiğini açıklayabilir. Örneğin, bazı bireyler finansal kazanç, siyasi hedefler, kişisel tatmin veya basitçe kaos yaratma arzusu ile hareket ederek siber

suçlara başvurabilmektedirler. Hackerların[9], dolandırıcıların ve diğer siber suçluların realist teorinin varsaydığı bencil ve güç arzusu doğrultusunda hareket ettiklerini söylemek yanlış olmayacaktır.

Devletlerin uluslararası sistem içerisindeki etkileşimleri ve politikaları üzerinde de önemli etkileri olan güç arzusu konusunda da vurgu yapan realist teori kapsamında devletlerin siber uzaydaki eylemleri genellikle kendi ulusal çıkarlarını koruma ve güçlerini artırma çabaları olarak yorumlanabilir. Devletler siber saldırılar düzenleyebilir, siber casusluk yapabilir veya siber savunma yeteneklerini güçlendirebilir. Böylece siber uzayda daha üstün bir konum elde etmeye çalışabilirler. Ayrıca realist teorinin öne sürdüğü devletlerin birbirlerine karşı güç dengesini koruma eğiliminde oldukları, genellikle siber uzayda devletlerin kendi siber yeteneklerini geliştirme ve rakiplerinin, yani diğer devletlerin, siber yeteneklerini öğrenmeye çalışmaları ve bu bağlamda yaptıkları istihbarat faaliyetleri şeklinde gerçekleşmektedir. Dolayısıyla realist teorinin insan doğasına ilişkin varsayımları, siber uzaydaki davranışları ve dinamikleri anlamak için kullanışlı bir altyapı sağlayabilir. Bireylerin ve devletlerin siber uzayda nasıl hareket ettiklerini ve neden belirli eylemlerde bulunduklarını anlamada önemli bir çerçeve sunar.

Kenneth Waltz'ın önderliğini yaparak ortaya attığı düşünceler neticesinde oluşan neo-realizm ya da diğer adıyla yapısal realizm, klasik realizme benzer bir anlayışı sürdürürken, uluslararası ilişkilerin anarşik yapısına daha fazla odaklanır ve devletlerin davranışlarını bu anarşik yapı içinde anlamaya çalışır. Neo-realistlere göre, uluslararası sisteme klasik realizmde olduğu gibi anarşi hakimdir ve bu anarşi, devletlerin eylemlerini ve davranışlarını belirler. Siber güvenlik bağlamında bu anarşik yapının bir sonucu olarak devletlerin siber tehditlere karşı sürekli olarak hazırlık yapmak ve hazırlıklı olmak zorunda olduklarını söylemek mümkündür. Neo-realizm, güç dengesi kavramını merkeze alır ve devletlerin bu dengede daha üstün bir konuma gelmek için siber yeteneklerini geliştireceğini öngörür. Dolayısıyla bu bağlamda devletlerin siber saldırılara karşı savunma yeteneklerini geliştirmek için teknoloji ve bilgiye yatırım yapacakları öngörülebilir.

[9] Tam bir Türkçe karşılığı olmayan bu kelime siber uzayda gerekli teknik ve teorik bilgiye sahip olan ve bilgisayar sistemlerine genellikle yasal olmayan yollardan sızabilme kapasitesi ve yeteneğine sahip olan kişiler için kullanılmaktadır.

Neo-realizm, devletlerin kendi güvenliklerini sağlamak için genellikle kendi güçlerine güvendiklerini ve dolayısıyla kolektif güvenlik çabalarına şüpheyle yaklaştıklarını öne sürmektedir. Waltz'ın "self-help" olarak tanımladığı bu yaklaşım, devletlerin güvenliklerini sağlamak adına kendilerinden başka kimseye güvenemeyecekleri temeline dayanmaktadır (Waltz, 1979). Siber uzayın güvenliğinin sağlanmasında kullanılan teknoloji ve alt yapılar temelinde düşünüldüğünde bu konu ayrı bir önem taşımaktadır. Siber uzayı oluşturan bileşenlerden bilgisayar ve internet teknolojisinin dünya pazarında ana üreticileri tüm dünyada kullanılan bilgisayarların ve işletim sistemlerinin büyük çoğunluğunu üretmektedirler. Dolayısıyla devletler bu bağlamda kendi teknolojilerini üreterek daha güvenli bir siber uzay oluşturma çabası içerisindedirler. Lakin burada ortaya çıkan durum ise kendi teknolojisini üreten devletlerin dünyanın büyük çoğunluğundan farklı bir teknoloji kullanıyor olmasının, onları daha güvenli yapmak yerine mevcut teknolojinin dışında kalarak daha güvensiz de yapabileceği gerçeğidir. Örneğin dünyanın en büyük bilgisayar üreticilerinden birisi olan Lenovo'nun ürünlerini kullanmak yerine devletlerin kendi ürettiği bilgisayarları kullanıyor olması daha güvenli bir tercih olabileceği gibi, Lenovo'nun geliştirdiği ve dünyanın büyük bir kısmının kullandığı teknolojiden uzak bir sistem kullanıyor olmak daha güvensiz bir siber uzay da ortaya çıkartabilir. Siber güvenlik bağlamında bu durum devletlerin siber güvenlik konusunda tek başına hareket etme ve uluslararası kuruluşlar veya diğer devletlerle iş birliği yapma konusunda şüpheci bir yaklaşımla hareket edecekleri anlamına gelmektedir. Neo-realist bakış açısından bakıldığında, bir devletin siber uzayda sahip olduğu güç kapasitesi siber güvenliğin sağlanması adına belirleyici faktördür. Bu ise siber güç kapasitesinin devletlerin politika ve strateji belirlemedeki önemini vurgular. Neo-realizm bağlamında değerlendirildiğinde siber güvenliğin uluslararası sistemin ve siber uzayın anarşik yapısı ve güç dengesi dinamikleri temelinde anlaşılması gerektiği sonucu ortaya çıkmaktadır.

Realist teoriyle birlikte ortaya çıkan güvenlikleştirme kavramı daha önce de belirtildiği üzere bir konunun veya olgunun siyasi aktörler tarafından bir güvenlik tehdidi olarak sunulduğunda o konu veya olgunun güvenlikleştirildiği anlamına gelmektedir. Bu süreç genellikle bir konunun ya da olgunun acil ve olağanüstü önlem gerektiren bir tehdit olarak algılanmasına ve sunulmasına yol açar. Siber güvenlik,

son yıllarda güvenlikleştirme kavramı çerçevesinde değerlendirilen bir alan olmuştur. Devletler siber tehditleri bir ulusal güvenlik meselesi olarak tanımlayarak bu tehditlerle mücadele için önemli kaynak ve çabalar harcamakta ve siber uzayı güvenlikleştirme çabası içerisindedirler. Devletler, siber tehditlerle mücadele etmek ve siber altyapıları korumak için çeşitli yasalar ve düzenlemeler yapmaktadırlar. Daha önce Türkiye örneğinde verilen yasal düzenlemeler ve kurumlar bazında getirilen yeniliklere ek olarak siber uzayın güvenlikleştirilmesi konusuna Amerika Birleşik Devletleri'nde Federal Bilgi Güvenliği Yönetimi Yasası (Federal Information Security Modernization Act, FISMA) (CISA, 2023) ve Avrupa Birliği'nde Genel Veri Koruma Tüzüğü (General Data Protection Regulation, GDPR) (EC, 2022) gibi düzenlemeler, siber güvenlik tehditlerinin önlenmesi ve yönetilmesi için yasal çerçeveler oluşturmuştur.

Devletler ayrıca ulusal düzeyde siber güvenlik stratejileri ve politikaları geliştirmiştir. Bu stratejiler genellikle siber tehditlere karşı savunma yeteneklerini artırmayı, siber olaylara yanıt vermeyi ve siber altyapıları korumayı amaçlar. Türkiye'de 2011 yılında 655 Sayılı Ulaştırma, Denizcilik ve Haberleşme Bakanlığının (UDHB) Teşkilat ve Görevleri Hakkında Kanun Hükmünde Kararname (KHK) ile siber güvenlik faaliyetleri ve hizmetleri ile ilgili kamu kurum ve kuruluşları arasında gerekli olan koordinasyonun sağlanması görevinin UDHB'na verilmesi (Resmî Gazete, 655 Sayılı KHK, 2011), 2012 yılında Bakanlar Kurulu kararı ile UDHB başkanlığında "Siber Güvenlik Koordinasyon Kurulu" kurularak siber güvenliğe yönelik ilkelerin, teşkilat, görev ve sorumlulukların resmi olarak belirlenmesi ve bakanlık ve kamu kurumlarının üst düzey yöneticilerinden oluşan Siber Güvenlik Kurulu oluşturulması bu bağlamda değerlendirilebilir. Siber Güvenlik Kurulu tarafından "Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı" ve daha sonrasında yayımlanan 2016-2019 Ulusal Siber Güvenlik Stratejisi ve Eylem Planı ve son olarak 2020-2023 Ulusal Siber Güvenlik Stratejisi ve Eylem Planı yine aynı çerçevede değerlendirilebilecek adımlardır.

Siber uzayın güvenlikleştirilmesinde birçok devlet siber güvenlikle ilgili sorunları ele almak için özel kurumlar ve birimler oluşturmuştur. Örneğin, Amerika Birleşik Devletleri'nde Siber Güvenlik ve Altyapı Güvenliği Ajansı (Cyber Security & Infrastructure Security Agency, CISA) ve Birleşik Krallık'ta Ulusal Siber Güvenlik

Merkezi (National Cyber Security Centre, NCSC) bu tür kurumlar arasında değerlendirilebilir. Ayrıca devletlerin siber tehditlere karşı proaktif bir yaklaşım benimseyerek siber savaş yeteneklerini geliştirme çabaları devletlerin siber saldırılara karşı caydırıcı olma ve gerektiğinde karşı saldırı düzenleme yeteneklerini artırma amacı taşımaktadır. NATO üyesi ülkelerin ittifak çatısı altında siber savunma ve saldırı kapasitelerini geliştirmeye yönelik katıldıkları siber güvenlik tatbikatları bu bağlamda değerlendirilmesi gereken bir konudur. Türkiye'nin de aktif olarak katılım sağladığı bu tatbikatların sonuncusu olan 2022 LockShields Tatbikatında 10 kişilik Türkiye takımı 9'uncu olmuştur (BİLGEM SGE, 2022).[10] Bu örnekler, devletlerin siber güvenlik tehditlerine nasıl tepki verdiğini ve siber uzayın nasıl bir güvenlik meselesi olarak algılandığını göstermektedir.

Siber uzayın güvenlikleştirilmesi, çeşitli güvenlik önlemlerinin uygulanması ve genellikle devletin dijital alan üzerinde daha fazla kontrol kurması anlamına gelmektedir. Ancak bu süreç genellikle bazı etik ve politik sorunları da beraberinde getirebilmektedir. Çünkü güvenlikleştirme genellikle daha fazla devlet kontrolü ve bazen bireysel özgürlüklerin kısıtlanması anlamına da gelebilecek bir olgudur. Devletler, siber tehditlerle mücadele etmek için genellikle dinleme ve gözleme gibi çok kapsamlı gözetim ve denetim yetenekleri kullanır. Bununla birlikte bu gözetim, bireylerin kişisel hayatının gizliliği ve mahremiyet haklarına ciddi bir tehdit oluşturabilir. Örneğin, Amerika'da Ulusal Güvenlik Ajansı'nın (National Security Agency, NSA) kitlesel gözetim programları özellikle Edward Snowden tarafından yapılan ifşaatlar sonrasında ciddi eleştirilere maruz kalmıştır (The Guardian, 2013). Dolayısıyla siber güvenlik önlemleri aynı zamanda bireysel özgürlükleri kısıtlayabilecek önlemlerdir. Buna ek olarak internet sansürü ve bilgiye erişimin engellenmesi devletlerin siber tehditlerle mücadele aracı olarak kullandığı yöntemlerden biridir. Bu durum ise ifade özgürlüğüne ve bilgiye erişim hakkına zarar verebilecek önlemler olarak değerlendirilebilir. Bu bağlamda Türkiye'de 2022 yılında çıkartılan 7418 sayılı "Basın Kanunu ve Bazı Kanunlarda Değişiklik Yapılmasına Dair Kanun" (Resmî Gazete, 7418 sayılı Kanun, 2022) halk arasında "Sosyal Medya

[10] NATO kapsamında düzenlenen siber güvenlik tatbikatları hakkında daha fazla bilgi için bkz. https://ccdcoe.org/exercises/locked-shields/

Yasası" ya da çoğunlukla "Sansür Yasası" olarak anılmış ve özellikle basın ve ifade özgürlüğünün kısıtlandığı noktasında ciddi eleştirilere maruz kalmıştır.

Devletlerin siber güvenlik önlemleri hukuki sorunlara da yol açabilir. Örneğin, devletlerin siber saldırılara karşı müdahale etme hakkı veya yeteneği, uluslararası hukuk çerçevesinde çeşitli tartışmalara neden olmaktadır. Ayrıca, devletler arasında siber suçların tanımlanması ve kovuşturulması konusunda geniş bir uyumsuzluk vardır. Bu sorunlar siber uzayın güvenlikleştirilmesi sürecinde dikkate alınması gereken önemli etik ve politik meselelerdir. Devletler siber güvenliği sağlarken bireysel özgürlükler ve hukukun üstünlüğü gibi temel değerlere de saygı göstermek zorundadır. Aksi takdirde siber güvenlik önlemleri demokratik değerler ve insan haklarına zarar verebilir. Bu nedenle siber güvenlik politikalarının oluşturulmasında dengeli bir yaklaşımın benimsenmesi önemlidir.

Realist düşüncenin ortaya çıkarttığı güvenlik ikilemi teorisi ise siber uzayda devletlerin kapasite geliştirme noktasında yaptığı çalışmaların anlaşılmasında oldukça önemli bir yer tutmaktadır. Daha önce belirtildiği üzere güvenlik ikilemi teorisine göre bir devletin güvenliğini artırmaya yönelik çabaları, diğer devletler arasında tehdit algısı yaratma potansiyeline sahiptir. Bu durum genellikle silahlanma yarışlarına, gerginliklere ve potansiyel olarak çatışmalara yol açabilir. Bu bağlamda siber uzayda güvenlik ikilemi oldukça belirgindir. Bir devlet, siber saldırı ve savunma kapasitelerini artırdıkça diğer devletler bu hareketi bir tehdit olarak algılayabilir. Siber yeteneklerin geliştirilmesi genellikle gizli bir süreç olduğu için bir devletin gerçek niyetleri ve kabiliyetleri hakkında belirsizlik genellikle yüksektir. Bu belirsizlik diğer devletlerin aşırı tepki göstermesine veya savunma amaçlı olduğu iddia edilen yetenekleri saldırgan bir amaç için kullanma korkusuna yol açabilir. Örneğin bir devletin siber savunma kapasitesini artırma çabaları diğer devletler tarafından siber saldırı kapasitesini geliştirme girişimi olarak algılanabilir. Bu durum karşılıklı güvensizliği artırabilir ve diğer devletlerin benzer şekilde siber kapasitelerini artırmalarını tetikleyebilir. Sonuçta bu durum siber uzayda bir silahlanma yarışına yol açabilir. Siber güvenlik ikileminin çözülmesi özellikle devletlerin niyetlerini ve kabiliyetlerini daha şeffaf hale getirmeye ve güven oluşturacak tedbirleri benimsemeye yönelik çabaları gerektirir. Dolayısıyla siber güvenlik konusunda uluslararası normların ve düzenlemelerin geliştirilmesi, devletler arası siber güvenlik konusunda diyalog ve iş

birliğinin teşvik edilmesi ve siber saldırıların kullanımının kısıtlanması gibi eylemler bu çerçevede değerlendirilmesi gereken konulardır.

3. SİBER TOPLUM ve YENİ BİR TOPLUM SÖZLEŞMESİ ARAYIŞI: SİBER TOPLUMSAL SÖZLEŞME MÜMKÜN MÜ?

Günümüz dünyasında teknolojinin hayatın her seviyesine sirayet ettiği ve artık deyim yerindeyse teknoloji olmadan bir hayat sürdürmenin birçok insan için neredeyse imkânsız hale geldiği yadsınamaz bir gerçekliktir. Sanayi Devrimi ile başlayan, endüstri ile devam eden ve bilişim teknolojisi ile modern dünyada en son geldiği noktaya ulaşan teknoloji, özellikle bilgisayar teknolojisi ve beraberinde getirdiği internet ile artık günlük hayatın rutin bir parçası haline gelmiştir. Daha önce de üzerinde durulan akıllı telefonlar ile hemen her bireyin sürekli yanında taşıdığı internet teknolojisi sosyal hayatın merkezine yerleşmiş, insan ilişkilerinin boyutunu gerçek dünyadan sanal dünyaya taşımış ve bunun yanında hayatı kolaylaştıran birçok yeni uygulamayı da beraberinde getirmiştir.

E-devlet uygulamaları, sanal bankacılık, internet alışveriş siteleri, mesajlaşma uygulamaları, görüntülü konuşma ve mesaj gönderme teknolojisi, harita uygulamaları gibi birçok teknolojik uygulama insanların günlük hayatta kullandığı ve hayatın vazgeçilmez bir parçası haline gelen uygulamalardır. Akıllı telefonların ilk kullanılmaya başlandığı dönemde internet teknolojisine erişimin oldukça kısıtlı olduğu ve bu cihazların çoğunlukla bir fotoğraf makinası olarak kullanıldığı dönemin ardından teknolojinin durdurulamayan gelişimiyle birlikte her biri kişisel bir cep bilgisayarına dönüşen bu cihazlar, hayatı kolaylaştıran uygulamaları insanlığa sunmasının yanında bilgiye erişim kaynağı haline de gelmiştir. Tüm bunların yanında sosyal medya platformlarının artan kullanımı insanların tanıştığı, sosyalleştiği ve anılarını paylaştığı yeni bir ortamın oluşmasını sağlamıştır. Covid19 pandemisinin zirve yaptığı dönemlerde insanların sosyalleşme, iletişim, alışveriş, eğitim ve iş hayatının merkezine oturan internet teknolojisi, en basit market alışverişinin dahi gerçekleştirilebildiği bir kolaylığa dönüşmüştür. Her türlü kişisel bilginin muhafaza edildiği, kişisel bilgi ve fotoğrafların paylaşıldığı bu yeni ortam daha önce detaylı bir şekilde bahsedilen riskleri de beraberinde getirmiştir.

Bilgisayarlar ve akıllı telefonlardan küçük ev aletlerine, üretim faaliyetleri gerçekleştiren büyük fabrikaların tesislerini yöneten sistemlerden ülkelerin silahlı kuvvetlerinin kullandığı birçok farklı savunma ve saldırı sistemine, havayolu, raylı sistemler ve karayolu ulaşım sistemlerinin kontrol mekanizmaları da dahil olmak üzere her türlü ulaşım cihazının kontrolünün sağlanmasında kullanılan sistemlerin artık bir şekilde internet teknolojisiyle uzaktan kontrol edilebilir hale gelmesi son dönemde sıklıkla kullanılan "dijital toplum" kavramını doğrular bir niteliğe dönüşmüştür. Ülkelerin kritik altyapılar olarak tanımladığı ulaşım, enerji, finans, sağlık ve savunma gibi alanlarda kullanılan SCADA sistemleri, zaman ve mekân kavramının dışında internet bağlantısının olduğu her yerden her saniye kontrol edilebilir hale dönüşmüştür. Covid19 pandemisi döneminde fiziki olarak kapanan iş yerlerinin faaliyetlerini sanal ortamda yürütmesi ve çalışanların evlerinden işlerini sürdürmesi ve öğrencilerin uzaktan eğitimle okullarına devam ederek eğitim hayatlarına devam etmesi siber uzayın bambaşka bir boyut kazanmasına yol açmış ve artık birçok alanda fiziki olarak binalara, ofislere ve hatta okullara bile ihtiyacın olmadığı düşüncesi ortaya çıkmıştır. İnsanların, devletlerin ve toplumların giderek dijitalleşmesi ise insan eliyle oluşturulmuş ve fiziki sınırları olmayan siber uzayda yeni bir toplumsal anlayışın ortaya çıkmasına neden olmuştur. Zamanın ve mekânın kısıtlamalarından sıyrılarak istenilen her yerde ve her zamanda insanoğlunun gerçek dünyada gerçekleştirdiği faaliyetlerin birçoğunu siber uzay denilen bu yeni dünyada da gerçekleştirmeyi mümkün kılan günümüz teknolojisi, toplumsal hayata önemli değişiklikler ve yenilikler getirmiştir.

3.1. Siber Uzayla Birlikte Ortaya Çıkan Yeni Düzen: Siber Toplum

Siber uzayın hayatın her alanına sirayet eden kullanımının artışı ile "dijital" veya "çevrimiçi" toplum olarak adlandırılan yeni bir tür toplum ortaya çıkmaya başlamıştır. Bu toplum, coğrafi veya ulusal sınırlar gibi fiziki sınır kısıtlamaları olmaksızın zamansal ve mekânsal olarak bağımsız bir şekilde dijital ağlar aracılığıyla sürekli birbirine bağlıdır (Housley, 2022: 16).

Siber uzayın artan kullanımı ve buna bağlı olarak iletişim teknolojilerinin geldiği nokta ile dünya genelindeki bireyler arasında anlık iletişim ve etkileşim sürekli bir şekilde devam etmektedir. Bu durum ise sürekli bağlı ve iletişim halinde olan yeni

bir toplumun ortaya çıkmasına neden olmuştur. Siber toplum olarak adlandırılabilecek olan bu yeni toplum, geleneksel anlamda bir üst otoritenin egemenliği altında yaşayan toplumlara haiz olan özelliklerden oldukça büyük farklılıklar göstermektedir. Siber uzayın ana bileşenlerinden bilgisayar ve internet teknolojisinin günümüzde geldiği nokta özellikle bilgiye erişimi ve bilgi alışverişini devrim niteliğinde değiştirmiştir. Artık her an ve her yerde bilgiye erişimi mümkün kılan internet teknolojisi, geleneksel anlamda mevcut olan kütüphanelerin yerini dijital kütüphanelerle doldurmakta ve daha önceleri spesifik bir bilgiye ulaşabilmek için harcanan süreleri arama motorları sayesinde saniyelerle ölçülebilecek kısa sürelere indirmektedir. Bu bağlamda artan erişilebilirlik, bilginin önemli bir kaynak olduğu bilgi toplumlarının yükselişini hızlandırmıştır. Elektronik kitaplar, video paylaşım siteleri ve açık kaynak eğitim platformları bu durumu oldukça mümkün kılmaktadır. İnternet, insanlar için bilginin paylaşılması ve yayılması adına benzersiz bir ortam oluşturmuştur. Aynı zamanda bilgiye erişim hızlanmış ve hiçbir zaman olmadığı kadar kolaylaşmıştır. Bilgi, artık herkes için birkaç tıklama ya da dokunuş uzakta ve dünyanın herhangi bir yerinden erişilebilir hale gelmiştir.

Bilginin yayılma hızı, internet sayesinde tahmin edilemeyecek boyutta artmıştır. Özellikle sosyal medya platformları sayesinde haber ve bilginin neredeyse anında yayılması oldukça kolay bir hale gelmiştir. İnternet, kullanıcıların bilgiyi kolayca paylaşmasını ve iş birliği yapmasını da mümkün kılmıştır. Örneğin, Wikipedia gibi platformlar kullanıcıların bilgiyi topluca oluşturmasına ve düzenlemesine izin vermektedir. Eğitimde dijital dönüşüm, çevrimiçi dersler ve uzaktan eğitim gibi bilgiye erişim yolları da aynı şekilde genişlemiştir. Bu durum öğrencilere ve öğrenmeye devam etmek isteyen kişilere daha esnek ve uygun maliyetli öğrenme olanakları sunmaktadır. İnternetin artan kullanımı devasa miktarda verinin toplanması ve analiz edilmesine de olanak sağlamaktadır. Bu büyük veri akışı yeni bilgilerin keşfedilmesine ve anlaşılmasına olanak sağlamaktadır. Ancak bu dönüşümün de zorlukları ve endişeleri vardır. Bilgiye erişim konusundaki dijital uçurum, veri güvenliği, gizlilik, yanıltıcı bilgi ve bilgi manipülasyonu gibi konular önemli endişeler arasında değerlendirilmektedir.

Artık hemen herkesin kullandığı sosyal medya platformları ise sosyal etkileşimleri dönüştürerek yeni türden ilişkilerin ve toplulukların gelişmesine olanak

sağlamıştır. Sosyal medya platformları (Facebook, Twitter, Instagram vb.), kullanıcıların dünya çapında anlık olarak bağlantı kurmalarını sağlamaktadır. Bu platformlar kişisel ve profesyonel ağlar oluşturmak, haberleri ve görüşleri paylaşmak ve etkileşimli bir dijital toplumda yer almak için bir araç sunmaktadır. Hatta bu durumun insanların kimliklerini de etkilediğini söylemek mümkündür. Çünkü çevrimiçi kişilikler, kişilerin sosyal medya platformlarında kendilerine oluşturdukları yeni profillerle gerçek dünyada var olan kişiliklerinden bambaşka bir karaktere bürünmelerine imkân sağlamış ve insan eliyle üretilmiş bu yeni alanda oluşan toplumun bir parçası olarak etkinlik sürdürmelerine izin verir hale gelmiştir. Bir başka deyişle, insanlar siber uzayda oluşturdukları yeni profilleriyle bambaşka bir kişilikte kendilerinin bir uzantısı şeklinde varoluşlarını sürdürebilmektedirler. Çevrimiçi platformlar, kullanıcıların dijital kimlikler oluşturmasına ve bunları kişiselleştirmesine olanak sağlamaktadır. Bu kimlikler, çevrimiçi etkileşimlerde ve topluluklarda temsil edilmeyi ve kişinin çevrimiçi varlığını ifade etmesini mümkün hale getirmektedir.

Siber uzayla birlikte çeşitli konulara, ilgi alanlarına ve etkinliklere odaklanan çevrimiçi topluluklar oluşmuştur. Bu topluluklar, benzer ilgi alanlarına sahip bireyler arasında sosyal bağlar oluşturmakta ve çoğu zaman dünya genelindeki kullanıcıları bir araya getirmektedir. İnternet, insanların çevrimiçi olarak birlikte çalışmasını ve birbirleriyle etkileşime girmesini de mümkün kılmıştır. Örneğin kullanıcıların bir projeye katkıda bulunduğu açık kaynak toplulukları ve insanların spesifik bir konuyu tartıştığı çevrimiçi forumlar gibi platformlar bu durumu mümkün kılmaktadır.

Siber uzayda ortaya çıkan toplum içerisindeki aktörler arasındaki etkileşimin gerçek dünyada var olan etkileşimler kadar gerçekçi olamayacağı kabul edilen bir

olgudur. Lakin sanal gerçeklik (virtual reality, VR)[11] ve artırılmış gerçeklik[12] (augmented reality, AR) teknolojileri sayesinde sosyal etkileşimlerin daha gerçekçi ve etkileşimli hale geldiği yeni bir döneme girilmiştir. Bu teknolojiler, insanların sanal dünyalarda birlikte var olmasını ve etkileşime girmesini sağlar. Ancak bu dönüşümün de zorlukları ve riskleri vardır. Gizlilik ihlalleri, dijital ayrımcılık, siber zorbalık ve kişisel bilgilerin kötüye kullanılması gibi konular önemli endişe kaynaklarıdır. Bu nedenle siber toplumun sunduğu yeni sosyal etkileşim ve ilişki biçimlerini dikkatlice yönetmek önemlidir.

Siber uzay aynı zamanda ticaretin her türlü işleyiş şeklini de değiştirmiştir. E-ticaret ve dijital para birimleri, küresel anlamda ekonomik sistemi dönüştürerek iş yapma ve ekonomik işlemler gerçekleştirme yöntemlerinde tamamen yeni yöntemleri iş dünyasına sunmuştur. Bu durum geleneksel ekonomilerin yanında faaliyet gösteren küresel bir dijital ekonominin ortaya çıkmasına da neden olmuştur. Artık ticaretin yeni merkezi siber uzayda gerçekleştirilen alışveriş eylemlerine dönüşmüştür. Tüm bunların yanında para transferi ve ödemelerin saniyeler içerisinde gerçekleşebildiği bu yeni ortam, sadece bireylerin değil, şirketlerin, bankaların ve hatta devletlerin de aralarındaki ekonomik ve ticari ilişkilerin dijitalleştiği yeni bir düzenin ortaya çıkmasını sağlamıştır.

---

[11] Sanal gerçeklik (Virtual Reality, VR), kullanıcıların tamamen dijital ve yapay bir ortamda etkileşime girmesine olanak sağlayan bir teknolojidir. VR teknolojisi, kullanıcıları gerçek dünyadan soyutlar ve onları bilgisayar tarafından oluşturulan bir dünyaya yerleştirir. Bu, genellikle bir VR kulaklığı veya gözlüğü kullanılarak yapılır. Sanal gerçeklik ortamında, kullanıcılar genellikle kendilerini tamamen farklı bir mekân veya durumda bulurlar, bir video oyununda fantastik bir dünya, bir mimari simülasyonda henüz inşa edilmemiş bir bina veya bir eğitim programında gerçek hayatta tehlikeli olabilecek bir senaryo olabilir. Sanal gerçeklik, kullanıcıya genellikle 360 derecelik ve üç boyutlu bir görüş alanı ve genellikle stereoskopik görüş sağlar, bu da derinlik algısını oluşturur ve böylece daha fazla daldırıcılık ve gerçekçilik sağlar. Sanal gerçeklik, çeşitli uygulamalar için kullanılır. Oyun sektörü, bu teknolojinin öncülerinden biri olmuştur, ancak VR artık eğitim, sağlık hizmetleri, mimarlık, sanat ve birçok başka alanda da kullanılmaktadır. Örneğin, tıbbi eğitimde, cerrahlar karmaşık prosedürleri gerçek bir hasta üzerinde uygulamadan önce sanal gerçeklik ortamında pratik yapabilirler. Sanal gerçeklik, kullanıcının deneyimlerini ve etkileşimlerini zenginleştiren bir teknoloji olmasına rağmen, fiziksel hareket sınırlamaları, maliyet ve siber hastalık gibi bazı potansiyel sorunlarla karşılaşmaktadır. Daha fazla bilgi için bkz. https://www.britannica.com/technology/virtual-reality

[12] Artırılmış gerçeklik (Augmented Reality, AR), dijital bilgileri ve görüntüleri, gerçek dünyanın üzerine ekleyen bir teknolojidir. Bu, genellikle bir akıllı telefon, tablet veya özel bir AR gözlüğü gibi bir cihaz üzerinden yapılır. Cihaz, genellikle bir kamera veya sensörler aracılığıyla gerçek dünyayı algılar ve ardından ekran üzerinde bu görüntülerin üzerine dijital bilgiler yerleştirir. Öğrencilerin karmaşık konuları daha iyi anlamalarını sağlamak için AR kullanılabilir. Örneğin, bir biyoloji öğrencisi, bir hücrenin 3D modelini görmek ve parçalarının her birini ayrı ayrı incelemek için AR'yi kullanabilir. Daha fazla bilgi için bkz. https://www.britannica.com/technology/augmented-reality

Siber uzayla birlikte ortaya çıkan dijital toplum, beraberinde aynı zamanda siyasi sonuçlar doğuracak değişimleri de getirmiştir. İnternet, çevrimiçi aktivizmden sosyal medyanın seçimler üzerindeki etkisine kadar siyasi katılımı ve söylemi dönüştürür hale gelmiştir. Sosyal medya platformlarından herhangi birisini kullanan her bireyin potansiyel olarak siyasi bir etki doğurabilecek gücünün olduğu gerçeği artık kabul edilen bir olgudur. Bu platformlarda yapılan basit bir paylaşım oldukça kısa süreler içerisinde büyük kitlelere ulaşabilmekte ve siyasi süreçlere olumlu ya da olumsuz etkilerde bulunabilmektedir. Ayrıca özellikle seçim süreçlerinde siyasilerin seçim kampanyalarının oldukça büyük bir kısmını oluşturan sosyal medya paylaşımları, siber uzayda oluşan bu yeni toplumun siyasi sonuçları arasında değerlendirilebilir. Siber toplumun siyasete olan etkisi, son yıllarda oldukça belirgin hale gelmiştir. İnternet, siyasilerin seçmenlere ulaşmasının ve mesajlarını yaymanın önemli bir aracı haline gelmiştir. Örneğin, Barack Obama'nın 2008 ve 2012 seçim kampanyaları, sosyal medyanın ve çevrimiçi organizasyonun politikada ne kadar etkili olabileceğini göstermiştir (Carter ve Yanes, 2012). Ancak bu durum aynı zamanda siber güvenlik ve veri gizliliği konularını da gündeme getirmiştir. 2016 ABD başkanlık seçimleri sırasında yaşandığı iddia edilen Rus müdahalesi (FBI, 2018) ve Cambridge Analytica[13] skandalı (The New York Times, 2018), bu konunun önemli örnekleri olarak karşımıza çıkmaktadır. İnternet ve sosyal medya, sosyal ve politik hareketlerin yayılmasında ve organize olmasında önemli bir rol oynamaktadır. Örneğin, Arap Baharı[14], Occupy Wall Street[15] ve Gezi Parkı protestoları gibi birçok hareket, sosyal medyanın insanların mobilizasyonu ve bilginin yayılmasındaki gücünü sergilemiştir. Bu örnekler, siber toplumun politikaya olan etkisinin karmaşıklığını ve genişliğini göstermektedir. Her durumda politikacıların, politika yapıcıların ve vatandaşların, bu

[13] Bir İngiliz veri firması olan Cambridge Analytica'nın 2016 ABD genel seçimlerinde milyonlarca Facebook kullanıcısına ait verileri ABD eski başkanı Donald Trump'ın seçim kampanyasında kullanılmak üzere sızdırmasının ardından ortaya çıkan Cambridge Analytica Skandalı oldukça önemli siyasi yankılar bulmuştur. Skandalın ortaya çıkmasından sonra firmaya ve yetkili çalışanlarına karşı ABD mahkemelerinde hukuki süreç başlatılmıştır.

[14] Arap Baharı sürecinde sosyal medyanın etkisi üzerine daha fazla bilgi için bkz. Wolfsfeld, Gadi, Elad Segev, and Tamir Sheafer. "Social Media and the Arab Spring: Politics Comes First." The international journal of press/politics 18.2 (2013): 115–137. https://journals-sagepub-com.mutex.gmu.edu/doi/full/10.1177/1940161212471716

[15] 2011 yılında ABD'nin NewYork kentinde yaklaşık 20.000 kişinin katıldığı ve birkaç ay boyunca süren gösterilerin yaşandığı, insanların çadırlar kurarak dünyanın finans merkezi olarak bilinen "*Wall Street*" caddesini bir bakıma işgal ettiği "*Occupy Wall Street*" gösterileri hakkında daha fazla bilgi için bkz. https://www.cbsnews.com/news/occupy-wall-street-uses-social-media-to-spread-nationwide/

etkileri anlamak ve yönetmek için yeni stratejiler ve politikalar geliştirmesi gerektiği bir gerçektir.

Siber uzay beraberinde getirdiği tüm avantajlarına rağmen, oluşturduğu dijital toplum için önemli zorlukları da ortaya çıkartmıştır. Gizlilik, veri güvenliği, dijital bölünme, yanıltıcı bilgi ve siber suçlar, bu zorlukların ve endişelerin bazılarıdır. Ayrıca bu yeni toplumu yönetmek, küresel ve sınırsız doğası nedeniyle oldukça karmaşıktır. Bu durum ise internet yönetimi, kurallar ve düzenlemelerin oluşturulmasında uluslararası iş birliği ihtiyacı hakkındaki tartışmalara yol açmaktadır.

Siber uzay tarafından ortaya çıkan bu yeni toplum hala bir dönüşüm içerisinde olmakla beraber henüz tam olarak sonuçları tamamen anlaşılamamıştır. Siber uzay insan ilişkilerini, kurumları ve sistemleri şekillendirmeye ve dönüştürmeye devam etmektedir. Siber uzayın getirdiği bu sosyal değişim ve dönüşüm sürecinde beraberinde getirdiği fırsat ve kolaylıkların yanında ortaya çıkarttığı yeni tehditler ve zorlukları dengede tutarak bu yeni alanın karmaşıklıklarını dikkatle yönetmek bireyler, hükümetler ve şirketler için önemli bir yerde durmaktadır.

3.2. Siber Toplumla Birlikte Ortaya Çıkan Yeni Düzen Arayışı: Siber Uzayda Bir Toplumsal Sözleşme Mümkün mü?

Güvenlik kavramı, siber uzayın beraberinde getirdiği siber güvenlik söylemi ile geçtiğimiz son yirmi yılda ulusal siber politikaları ve internetin kontrol edilmesi/ yönetilmesi bağlamında hem devlet hem de devlet dışı aktörleri içeren karmaşık bir güvenlik rejimine atıfta bulunan bir tartışmaya dönüşmüştür. Özellikle ABD Ulusal Güvenlik Ajansı (National Security Agency, NSA) çalışanlarından Edward Snowden'ın Ulusal Güvenlik Ajansı tarafından yürütülen küresel bağlamda hiçbir hukuki altyapı olmadan sadece ABD vatandaşlarının değil aynı zamanda birçok farklı ülkede farklı kişilerin hukuksuz bir şekilde izlenip gözetlendiğinin açığa çıkarılması ve buna ek olarak Cambridge Analytica skandalı, temel hak ve özgürlükler gibi evrensel değerlerin siber uzayda başlayarak gerçek dünyaya yansıyan bir şekilde saldırı altında olduğunu göstermiştir (NPR, 2019; The New York Times, 2018).

Günümüzde demokratik devletler teknolojinin getirdiği yeniliklerle siber uzayda izleme ve gözetleme yapabilmenin oldukça kolay hale gelmesi ve ulusal

güvenlik adı altında bu tip faaliyetlerin sürekli olarak yürütülmesi nedeniyle farklı zorluklarla karşılaşmaktadırlar. Devletler ulusal düzeyde yüksek güvenlik sağlamak adına siber uzayın getirdiği yenilikler sayesinde vatandaşları hakkında çok büyük miktarda veri toparlamaktadır. Diğer yandan, demokratik devletler siyasi yapıları gereği demokrasiyi ve hukukun özgürlüğünü korumak ve ayrıca anayasal düzenlemelere, sosyal ve siyasi haklara ve bağımsız medyaya saygı göstermek durumundadırlar. Bu durumda ortaya çıkan sorunsal ise devletlerin güvenlik kaygıları ile vatandaşlarının hakları arasında bir dengenin kurulup kuramayacağı konusudur. Bu durum ise devlet ile vatandaşları arasındaki güvenlik düzenlemelerinin yeniden ele alınmasını zorunlu hale getirmiştir (Liaropoulos, 2020: 2).

Devletler, toplumlar, kamu kurumları ve özel kuruluşlar sürekli gelişen güvenlik ortamına ve aktörlerine nasıl yaklaştıklarını, güvenilir ve etkili anlaşmalara nasıl ulaşabileceklerini yeniden düşünmek zorundadırlar. Sonuç olarak, geleneksel devlet ve vatandaşları arasındaki ilişkileri, özel ve kamusal alan arasındaki çizgileri sorgulayan siber uzay için yeni bir toplum sözleşmesine ihtiyaç duyulmaktadır.

Siyaset felsefesinin en temel kavramlarından birisi olan toplum sözleşmesi teorisi, bir toplumun kuruluşunun ve bireylerin bir hükümet veya egemen otoriteyle nasıl etkileşime girdiğinin anlaşılması temeline dayanan ve modern anlamda devletlerin toplum ve siyaset düzeninin anlaşılmasında oldukça önemli olan bir düşüncedir. Temel olarak toplum sözleşmesi teorisi, bireylerin bir hükümetin otoritesini kabul etmek için gönüllü olarak anlaştığı bir "sözleşme" fikrine dayanır. Bu sözleşme genellikle bireylerin bazı özgürlüklerini hükümete devretmeyi kabul ettikleri, hükümetin ise karşılığında bireylerin haklarını koruduğu ve genel düzeni sağladığı bir anlaşma olarak tasvir edilmektedir. Devletin ve kurumlarının kökenlerini ve amacının ne olduğunun anlaşılması bağlamında insanların karşılıklı yararları için bir toplum oluşturmayı ve birbirleriyle bir sözleşme yapmayı gönüllü olarak kabul ettikleri düşüncesi üzerine kurulan toplum sözleşmesi teorisi, birey üzerindeki otoritenin veya devletin meşruiyetini açıklamak için bir model olarak değerlendirilebilir.

Toplum sözleşmesi, bir yandan toplum üyeleri arasındaki haklar ve sorumluluklar, diğer yandan devlet ve hükümet ile ilgilidir. Siber uzay, milyarlarca

kullanıcının bağlantı ve iletişim için benzersiz bir küresel platform olarak hizmet vererek kendi sosyal yapısını oluşturmakta ve böylece yeni bir düzenleyici ekosistem ortaya çıkartmaktadır. Siber uzay tarafından kolaylaştırılan toplumsal reform, toplum sözleşmesi teorisini şekillendiren geleneksel haklar ve sorumlulukların anlaşılması konusunu karmaşık bir hale getirmektedir. Yanıltıcı bilgi kampanyaları, nefret söyleminin yayılması ve ayrımcılığın ortaya çıkması, siber uzayın tüm paydaşları arasında yeni kurallar ve sosyal anlaşmalara duyulan ihtiyacı ortaya çıkartmaktadır (Liaropoulos, 2020: 1-2)

Siber uzayın beklenmedik boyutlarda hızlı bir şekilde genişlemesi toplum sözleşmesi ile ilgili olarak yeni zorluklar ve düşünceler ortaya çıkarmıştır. Thomas Hobbes, John Locke ve Jean-Jacques Rousseau gibi düşünürlerin ortaya attığı geleneksel toplum sözleşmesi teorileri, tanımlanabilir egemen bir otoritenin altında yaşayan ve hükümetleri olan, fiziksel, coğrafi olarak sınırları bulunan toplumların egemen otorite ve hükümet ile olan ilişkilerini açıklamak adına ortaya çıkmıştır. Diğer yandan, siber uzay denilen ve insan eliyle üretilmiş küresel, fiziki sınırları olmayan ve tam anlamıyla sınırsız olan bu yeni alan, kendine özgü bir dizi özellikleri de beraberinde getirmiştir.

Siber uzayda kimin güce sahip olduğu karmaşık bir konudur. Hükümetler, çok uluslu şirketler, bireysel kullanıcılar ve aktivist gruplar gibi çok sayıda aktörün varlığını sürdürdüğü ve etkin olduğu siber uzayda tüm bu paydaşların oldukça değişken seviyelerde etkili olduğu bir gerçektir. Bu durum, geleneksel toplumların yapısından çok daha farklı ve karmaşık bir durum ortaya çıkartmaktadır. Ayrıca bireylerin siber uzayda hangi haklara sahip olduğu ve bu haklarla birlikte hangi sorumlulukları getirdiği konusu da oldukça önemlidir. İfade özgürlüğü, veri güvenliği, siber saldırı tehditleri, özel hayatın gizliliğinin korunması gibi konuların yanında yanıltıcı bilginin yayılması, nefret söylemi yayma ve bununla birlikte ortaya çıkan ırkçı söylemler, müstehcenlik v.b. gibi konular bu alanda yeni sorumlulukların ve etik düşüncelerin ortaya çıkmasına neden olmuştur. Bireylerin siber uzayın önemli mecralarından birisi olan sosyal medya platformlarında paylaştığı herhangi bir içerik kimileri için temel hak ve özgürlükler kapsamında değerlendirilebileceği gibi bir başka kesim için toplumsal düzeni bozacak nitelikte ya da toplumun ahlaki değerlerini hiçe sayan zararlı paylaşımlar olarak görülebilmektedir.

İnternetin sınırları aşan küresel ve anonim doğası, kuralların ve düzenlemelerin uygulanmasını karmaşık bir durum haline sokmaktadır. Ayrıca teknolojinin durdurulamayan hızlı gelişimi, bu teknolojilerin kullanımı hakkında genellikle yasal ve düzenleyici çerçevelerin oluşturulmasını oldukça zorlaştırmaktadır. Ortaya çıkan yeni bir teknolojik gelişme ile ilgili yapılan bir yasal düzenlemenin ortaya çıktığı süre içerisinde mevcut teknolojik gelişme birçok farklılık gösterecek şekilde geliştirilmiş ve ilerletilmiş olabilmektedir.

Siber uzayın kullanımı noktasında mevcut bulunan eşitsizlik durumu toplum sözleşmesinin önemli konularından birisini oluşturan eşit katılım konusunda da üzerine düşünülmesi gereken bir olgudur. Güvenilir internete erişim ve dijital okuryazarlık, bireylerin çevrimiçi topluma tam olarak katılma yeteneklerini büyük ölçüde etkileyen önemli konulardır. Bu nedenle, siber uzayın kendine özgü bir toplum sözleşmesine ihtiyacı olduğu açıktır. Bu sözleşme, siber uzayla birlikte ortaya çıkan siber toplumun benzersiz özelliklerini ve zorluklarını göz önünde bulundurmalıdır. Bu bağlamda hakları, yükümlülükleri ve kuralları tanımlamalı ve bireylerin özgürlüğü ile siber uzayın farklı paydaşlarının çıkarları ve genel olarak siber uzay ekosisteminin sağlığı ve güvenliği arasında bir denge sağlamalıdır. Ayrıca siber uzayda ortaya çıkacak sorumluluk ve uyuşmazlıkların çözümü adına çözüm mekanizmalarına duyulan ihtiyaç da bu bağlamda önemlidir. Böyle bir toplum sözleşmesinin geliştirilmesi, hükümetler, işletmeler, sivil toplum ve bireyler arasındaki diyalogları içeren karmaşık bir süreçtir.

3.2.1. Toplum Sözleşmesi

Toplum sözleşmesi kavramı, yönetilenler ile yöneticileri arasındaki gerçek veya varsayımsal bir anlaşmayı ifade eden ve her bir tarafın haklarını ve görevlerini tanımlayan bir kavramdır. Bu kavram, yöneticilerin (genellikle devletin) vatandaşlarına belirli haklar ve hizmetler sağlama taahhüdünde bulunduğu ve karşılığında vatandaşların belirli sorumlulukları ve yükümlülükleri olduğu bir anlaşmayı temsil etmektedir. Toplum sözleşmesi teorisine göre, başlangıçta doğa durumunda bulunan insanları düzenleyen bir hükümet ya da kanunun varlığından bahsetmek mümkün değildir. Bu doğa durumunda, bireylerin eylemleri yalnızca kişisel güçleri ve vicdanları tarafından sınırlanmaktaydı. Kısacası, toplum sözleşmesi

teorisi, rasyonel bireylerin neden doğal özgürlüklerinden gönüllü olarak vazgeçip politik düzenin faydalarından yararlanmak için bir toplum oluşturmayı kabul edeceğini açıklamaktadır (Barker, 1960: 3).

İnsanlar doğa durumundan geçiş sürecinde iki anlaşma yapmışlardır. İlk anlaşmada yaşamlarını ve mülklerini koruma arayışı içerisine girmişlerdir. Bu nedenle, insanların birbirine saygı gösterdikleri ve barışçıl bir şekilde yaşamayı kabul ettiği bir toplum oluşmuştur. İkinci anlaşmada insanlar birleşmiş ve bir otoriteye itaat etmeyi ve bunun neticesi olarak özgürlük ve haklarının tamamını ya da bir kısmını bu otoriteye teslim etmeyi kabul etmişlerdir. Yapılan ikinci anlaşma neticesinde herkese yaşam, mülkiyet ve belirli bir ölçüde özgürlük koruması garanti edilmiştir. Bu yüzden insanlar doğa durumundan çıkarak toplu olarak ortak yasalar altında birlikte yaşamayı kabul ettikleri ve toplum sözleşmesinin uygulanması için mekanizmalar oluşturdukları bir toplum oluşturmuşlardır (Matan, 2004: 43).

Bu anlaşmaların temelinde bireylerin toplumsal olarak bir arada yaşamasının doğa durumunun belirsizlik ve tehlikelerinden korunma, mülklerini koruma ve daha düzenli bir yaşam sürdürme fırsatı sağladığı düşüncesi yatmaktadır. Toplum sözleşmesi teorisinin günümüz modern toplumlarının yapısı karşısında çeliştiği birçok nokta vardır. Gerçek hayatta haklar ve özgürlükler her zaman tam olarak korunamaz ve devletin gücü bazen bireylerin çıkarlarına aykırı olarak kullanılabilmektedir. Bu yüzden modern toplumların dijital çağdaki yeni zorlukları ve fırsatları göz önünde bulundurarak toplum sözleşmesini yeniden düşünmeleri gerekmektedir. Bu durum özellikle siber toplum gibi geleneksel devlet ve vatandaş ilişkilerinin sınırlarını aşan yeni alanlarda geçerli bir konudur. Siber toplum bağlamında toplum sözleşmesi kavramı bilgiye erişim, veri gizliliği ve siber güvenlik gibi yeni haklar ve yükümlülükler ortaya çıkartmaktadır. Bu nedenle modern toplumların dijital çağın getirdiği bu yeni zorlukları ve fırsatları dikkate alarak toplum sözleşmesini yeniden düşünmeleri ve belki de yeni bir "siber toplum sözleşmesi" oluşturarak bu değişikliklere uyum sağlamaları gerekmektedir.

3.2.1.1. Thomas Hobbes ve Toplum Sözleşmesi

Toplum sözleşmesi teorisinin kökenleri Plato ve Sokrates'e kadar dayandırılabilir fakat bu düşünceyi Thomas Hobbes'un öncülüğünde ilk olarak John

Locke ve sonrasında da J.J. Rousseau 18. yüzyılda popüler hale getirmiştir. Britanya iç savaşı sırasında 1651 yılında yayınlanan Hobbes'un eseri "Leviathan" toplum sözleşmesi düşüncesinin temelini oluşturmuştur. Hobbes'a göre, doğa durumu korku ve bencillik durumu olarak tanımlanır. Yüksek bir otoritenin kontrolünün bulunmadığı bu durumda insanlar yoksul, hayvansı ve kısa yaşamlar yaşamaktaydı. İnsanların güvenlik ve düzen arzusunu doğal bir durum olarak tanımlayan Hobbes'a göre insanlar, hayatta kalmalarını güvence altına almak, acı ve ıstıraptan kaçınmak için bir sözleşme yaparlar ve haklarının bir kısmını veya tamamını onları ve mülklerini koruma görevine sahip olan bir üst otoriteye gönüllü olarak devrederler. Hobbes'a göre bu otorite mutlak itaat gerektirmektedir. Bir denge unsuru olarak Hobbes otoriteye ahlaki yükümlülükler yüklemiştir. Hobbes'a göre doğa durumu bir savaş durumudur ve bu yüzden insanlar hayatlarının egemen bir güç tarafından korunduğu tek koşulda özgürlüklerini mutlak egemene vermelidirler (Hartz ve Nielsen, 2015: 11).

Hobbes'un toplum sözleşmesi düşüncesi "Leviathan"ın yani, egemen hükümeti tanımlamasının temelidir. Leviathan ideal bir hükümet türüdür, çünkü insanların haklarını korurken aynı zamanda genel huzur ve düzeni de sağlar. Ancak bu hükümetin gücü mutlaktır. Çünkü hükümetin haklarını kısıtlamak veya ona karşı gelmek doğa durumuna geri dönme riskini ortaya çıkartır. Hükümetin otoritesi mutlak olmalıdır. Eğer hükümetin gücü sorgulanırsa veya tehdit edilirse bu durum genel düzeni bozabilir ve potansiyel olarak "herkesin herkese karşı savaş" durumuna geri dönmesine yol açabilir (Hobbes, 2017: 188-202).

Hobbes'un bu görüşü, toplum sözleşmesi teorisyenlerinin diğerlerinden (örneğin, John Locke veya Jean-Jacques Rousseau gibi) önemli ölçüde farklıdır. Bu düşünürler, hükümetin bireylerin haklarını ihlal ettiği durumlarda, bireylerin hükümeti meşru bir şekilde sorgulama veya devirme hakkına sahip olduğunu savunur. Ancak Hobbes, hükümetin gücünün mutlak olması gerektiğini savunmaktadır. Hükümetin varlığı bireyler arasındaki anlaşmazlıkları çözen ve genel düzeni sağlayan tek mekanizmadır. Hobbes'a göre hükümetin gücünü sınırlayan herhangi bir girişim toplumun genel huzur ve düzenini bozabilecek niteliğe sahiptir. Dolayısıyla Hobbes'un toplum sözleşmesi teorisi, insanların kendi doğal haklarının bazılarını bir egemen hükümete devrederek daha güvenli ve düzenli bir toplum oluşturmayı seçtiklerini savunur. Ancak bu hükümetin gücü mutlak olmalıdır, çünkü hükümetin otoritesinin

sorgulanması veya tehdit edilmesi Hobbes'a göre kaosa ve anlaşmazlığa yol açabilir (Hobbes, 2017: 189).

Hobbes'a göre tüm insanlar fiziksel ve zihinsel yapıları bakımından az veya çok birbirilerine benzerdir ve hiç kimse fiziksel ve zihinsel olarak diğerlerinin üzerinde hüküm sürme yeteneğine sahip olacak şekilde üstün değildir. Hobbes'a göre özgürlük, "*dış engellerin yokluğudur ve bu engeller insanın istediğini yapma gücünün bir kısmını sıklıkla ortadan kaldırabilir*" (Hobbes, 2017, 189). Doğa durumu, insan eylemlerine fiziksel ve doğal engeller içermektedir. Fiziksel nesneler, istediğimiz gibi hareket etme yeteneğimizi kısıtlayabilir ve diğer insanlar planlarımıza ve niyetlerimize karşı çıkabilir. Ancak, Hobbes'un iddia ettiği gibi doğa durumunda hareketlerimiz üzerinde hiçbir ahlaki, hukuki veya sosyal kısıtlama yoktur (Hobbes, 2017: 188, 202). Bu nedenle doğa durumu, insan eylemleri üzerinde hiçbir sosyal veya normatif kısıtlama içermediği bağlamında bir özgürlük durumudur.

Thomas Hobbes (1588–1679) genellikle modern siyaset felsefesinin kurucularından biri olarak görülür ve özellikle de toplum sözleşmesi teorisiyle tanınır. Hobbes *Leviathan*'da insanların doğal hallerinde yani hükümet veya başka bir düzenleyici otorite olmadan bir "herkesin herkese karşı savaşı" durumunda olacağını öne sürmektedir. Her bireyin doğal hakları vardır ve bu haklar doğası gereği sınırsızdır. Herkes hayatta kalma ve kendi çıkarlarını koruma hakkına sahiptir. Ancak, bu haklar çatışabilir ve sonuç olarak genellikle korku ve güvensizlik ortamına yol açar. Hobbes bu durumu "*bellum omnium contra omnes*" olarak adlandırır, bu da Latince'de "herkesin herkese karşı savaşı" anlamına gelir (Blackburn, 2008: 39). Bu durumda Hobbes'un söylediği gibi insanların hayatı "vahşi, acımasız ve kısa" olur. Ancak insanlar bir çeşit toplum sözleşmesi yoluyla bu durumdan kurtulmayı seçebilirler.

Hobbes, doğa durumunda insanların gerçekten birbirleriyle savaşıyor olmayabileceğini kabul eder. Ancak bu varsayımsal durumu tanımlama şekli nedeniyle doğa durumu birinin kendi amaçlarına hizmet etmek için diğerlerinden faydalanmaya çalışma riskinin sürekli olduğunu anlatmaktadır. Hobbes, böyle bir durumda yani doğa durumunda sanayiye yer olmadığını ve dolayısıyla dünyanın hiçbir kültürünün var olmadığını, denizciliğin ya da deniz yoluyla ithal edilebilecek malların kullanımının mümkün olmadığını, içerisinde yaşamak için hiçbir rahat yapının

olmadığını, çok fazla güç gerektiren şeyleri taşımak ve kaldırmak için gereken araçların bulunmadığını, dünyanın nasıl göründüğü hakkında hiçbir bilginin bulunmadığını, zaman kavramının var olmadığını, sanat ya da toplumun varlığının olmadığını ve en kötüsü sürekli korku ve şiddetli ölüm tehlikesinin olduğu ve insan hayatının yalnız, yoksul, pis, hayvansı ve kısa olduğunu söylemektedir (Hobbes, 2017: 186). Bu nedenle Hobbes'a göre doğa durumu, herkesin daha iyi bir şey karşılığında terk etmek için ilgi duyduğu berbat bir yerdir. İnsanlar doğal olarak kendi varlıklarını korumaya çalışırlar. Dolayısıyla herkes soyulmayacağı, tecavüze uğramayacağı veya öldürülmeyeceğine emin olamadığı doğa durumunu terk etmek için birçok sebebe sahiptir (Hobbes, 2017: 190).

3.2.1.2. John Locke ve Toplum Sözleşmesi

John Locke'un toplum sözleşmesi teorisi, Hobbes'un düşüncelerine paralel bir şekilde olmasına rağmen özellikle egemenlik konusu üzerinde farklılık göstermektedir. 1690'da yayınlanan "*Two Treatises of Government*" adlı eserinde Lock, Hobbes gibi insanların doğa durumunda yaşadığını kabul eder ancak doğa durumu hakkındaki görüşü Hobbes'un ortaya koyduğu doğa durumu kadar berbat değildir. Aksine, Locke doğa durumunu insanların kendi çıkarlarını takip etmekte serbest olduğu, müdahaleden uzak, makul derecede iyi ve keyifli bir durum olarak tanımlamaktadır. Locke'a göre doğa durumunun tek dezavantajı oluşturulmuş bir hukukun veya doğal kanunları uygulamak için gerekli olan doğal bir gücün olmamasıdır. Bu yüzden mülkiyet güvence altında değildir. İnsanları doğa durumunu terk etmeye ve toplum sözleşmesine girmeye zorlayan şey mülkiyetlerini koruma ihtiyacıdır. Dolayısıyla insanlar sahip oldukları tüm haklarını otoriteye teslim etmezler ve sadece düzeni koruma ve doğa kanunlarını uygulama hakkını teslim ederler. Locke'un ortaya koyduğu toplum sözleşmesinde insanlar yaşam hakkını ve özgürlüklerini korurlar. Locke'a göre, hükümetin amacı, insanların doğal haklarını korumaktır. Hükümet bu amacı yerine getirdiğinde, kanunlar geçerli ve bağlayıcıdır ancak hükümet amacını yerine getirmeyi bıraktığında kanunlar geçersiz olur ve hükümet yine toplum tarafından iktidardan atılabilir. Locke'a göre sınırsız egemenlik doğa hukukuna aykırıdır (Baumgold, 2005).

Locke'un toplum sözleşmesi teorisi, Hobbes'un mutlak egemen otorite gerekliliği üzerine kurulu olan görüşünden önemli ölçüde farklıdır. Locke, İngiltere'de 17. yüzyılın farklı dönemlerinde yaşanan iç savaş ve devrimlere bir yanıt niteliğinde ortaya çıkarttığı eserinde doğa durumunu bireylerin kendi çıkarlarına ve planlarına serbestçe devam edebilecekleri ve başkalarının hakimiyeti ve müdahalesinden bağımsız bir eşitlik ve özgürlük durumu olarak tanımlamaktadır. Ancak bu doğa durumu tamamen barışçıl değildir çünkü kaynaklar üzerindeki anlaşmazlıkları ve çatışmaları çözecek genel kabul görmüş, objektif bir hukuki otorite yoktur. Locke, insanların doğaları gereği başkalarının haklarına, özellikle de mülkiyet hakkına saygı gösterdiğini savunmuştur. Ancak ortak bir otorite olmadan anlaşmazlıkların zarara yol açabileceğini de belirtmiştir (Locke, 1988: 213).

Locke'un toplum sözleşmesi, bireylerin karşılıklı rızalarıyla bir topluluğa birleşmeyi, ortak kurallara uymayı ve birbirlerini şiddetten ve haklarının ihlalinden koruma görevlerini kabul etmeyi içerir. Locke'a göre bireyler, doğa yasasını uygulama ve toplumsal düzeni koruma yetkisini hükümete devrederler ve böylece bir sivil toplum oluştururlar. Bu toplumda, hükümetin ana işlevi Locke'un bireylerin doğal hakları olarak tanımladığı yaşam, özgürlük ve mülkiyet haklarını korumak ve muhafaza etmektir. Hobbes'un aksine Locke, bireylerin tüm haklarını egemen otoriteye teslim etmediklerini savunmuştur. Bunun yerine, temel haklara sahip olduklarını ve hükümetin yönetilenlerin rızası ile kurulduğunu söylemektedir. Hükümetin meşruiyeti, doğa yasasını ve kamusal iyiliği korumasına bağlıdır. Eğer bir hükümet bu hakları korumada başarısız olur veya kamu yararına karşı hareket ederse, halkın direnme ve hükümeti devirme hakkı vardır. Bu durum Locke'un devrim hakkını savunmasının temelini oluşturur (Locke, 1988). Dolayısıyla Locke'un toplum sözleşmesi teorisi, halkın nihai egemen olduğu ve hükümetin yönetilenlerin iradesine hizmet ettiği bir demokratik ideal üzerine kuruludur

3.2.1.3. Jean-Jacques Rousseau ve Toplum Sözleşmesi

Jean Jacques Rousseau, 1762'de yayınlanan "Toplum Sözleşmesi" adlı eserinde toplum sözleşmesi teorisine farklı bir yorum getirmiştir. Hobbes ve Locke'un aksine Rousseau, toplum sözleşmesinin tarihi bir gerçek olmadığını, daha çok varsayımsal bir yapı olduğunu savunmaktadır. Rousseau'ya göre insanlar bencil olarak

kendi gerçek çıkarlarını takip edemezler. Bunun yerine toplum tarafından oluşturulan bir kanuna tabi olmalıdırlar. İnsanlar haklarını bir bireye değil, topluluğun tamamına, yani Rousseau'nun "genel irade" olarak adlandırdığı şeye teslim ederler. Bu anlamda kanun bireysel özgürlüğün bir sınırlaması değil bir ifadesi şeklinde ortaya çıkar. Rousseau'ya göre herkes yalnızca genel iradeye tabidir ve bu yüzden genel iradeye uyan birey aynı zamanda kendine de itaat etmektedir. Kanunun uygulanması özgürlüğün bir kısıtlaması değil, doğa durumundan sivil topluma doğru bir yükseliştir ve bir medenileştirme gücüdür. Toplum sözleşmesi aracılığıyla haklarını ve özgürlüklerini koruma görevine sahip yeni bir sosyal organizasyon biçimi oluşmuştur ve bu devletin kendisidir. Toplum sözleşmesi aracılığıyla insanlar doğal haklarını teslim eder ve karşılığında ifade özgürlüğü ve eşitlik gibi medeni haklara sahip olurlar (Bertram, 2013: 190-204).

Rousseau'nun toplum sözleşmesi teorisi bireylerin özgür ve eşit bir toplumda yaşayabilmek için belli haklarını bir araya gelip bir "toplum sözleşmesi" oluşturarak topluma devretmeleri gerektiğini öne sürer. Rousseau'ya göre bu durum her bireyin özgürlüğünü korurken aynı zamanda toplumun refahını da garanti eder. Rousseau'nun teorisinin önemli bir yönü ise "genel irade" kavramıdır. Rousseau'ya göre toplum sözleşmesine taraf olan bireyler kendileri için en iyi olanı belirlemek için birlikte çalışırlar. Bu ise herkesin özgürlüklerini ve haklarını korurken aynı zamanda toplumun çıkarlarına da hizmet eder (Morris, 1999). Rousseau, genel iradeyi bir tür demokratik felsefi ilke olarak görmüştür. Rousseau'nun toplum sözleşmesi teorisi, özellikle demokratik düşünce ve toplumun yararına hizmet edecek bireysel hakların nasıl dengeleneceği konuları üzerinde oldukça büyük etkisi olmuştur.

Rousseau, Hobbes ve Locke'dan daha radikal bir yaklaşım sergiler. Rousseau'ya göre, doğa durumu insanları sadece kendilerine bağımlı olmaktan özgür kılar, ama aynı zamanda birbirlerine karşı da sorumlulukları vardır. Rousseau, insanların bir toplum sözleşmesi oluşturarak ve genel iradeye boyun eğerek bu sorumlulukları yerine getirebileceklerini öne sürer. Rousseau'ya göre, hükümetin amacı, genel iradeyi temsil etmek ve onu uygulamaktır (Morris, 1999).

Rousseau'ya göre kendisinden önceki düşünürler insanın doğa durumu ile ilgili genellikle uygarlık öncesi durumu incelemişlerdir lakin oraya ulaşamamışlardır.

Rousseau bununla birlikte bu düşünürlerin sadece uygarlık öncesi insanlığın doğa haline odaklandıklarını ve uygar insanı anlatmadıklarını savunmuştur. Rousseau'ya göre doğa hali en genel haliyle bir eşitlik ve özgürlük halidir. Bu durumda insanların genel istek ve ihtiyaçlarını fiziksel ihtiyaçlar oluşturmaktadır. Doğa durumunda insanların isteklerinin sınırlılığından bahseden Rousseau'ya göre Hobbes'un iddia ettiği gibi insanlarda gelecek kaygısı durumu söz konusu değildir. Dolayısıyla herkesin herkesle savaşı gibi bir durum da yoktur. Doğa durumunda insanların isteklerinin fiziki ve basit ihtiyaçlar olduğunu belirten Rousseau'ya göre insanlar sadece nesillerinin devamı için bir araya gelmektedir ve birbirleri arasında bir toplum oluşturacak herhangi bir bağ da yoktur. Seçim yapma konusunda özgür olan insan, karar alma ve gelişim gösterme bağlamında diğer canlılardan ayrılmaktadır. İnsanların gelişim yeteneğine sahip olması bunun her zaman iyi yönde ilerleyeceği anlamına gelmez ve bu gelişim süreci doğa halinden topluma doğru evirilen bir süreçtir. Rousseau doğa durumundan toplum durumuna geçen insanlar arasında mülkiyet kavramının geliştiği ve bununla birlikte doğa durumunda var olduğunu söylediği barış ve eşitliğin bozulduğunu belirtmiştir (Rousseau, 2013: 17-38).

Rousseau doğa durumundan insanların gelişimiyle birlikte ortaya çıkan mülkiyet kavramıyla birlikte insanların doğa durumunda kalmaları durumunda karşılaşacakları zorluklarla baş etmenin mümkün olmadığı bir hale gelmesiyle varlıklarını koruma adına yaşayış biçimlerinin değişime uğradığını ve toplumsal bir sürece doğru evirildiklerini iddia etmiştir. Rousseau'ya göre toplumsallaşmaya geçen insanların bu süreci iyi bir süreç olarak algılanmamalıdır. Çünkü insanlar bu yeni düzende doğa durumunda sahip oldukları özgürlük ve eşitlik kavramlarını kaybederler. Özel mülkiyet kavramının ortaya çıkmasıyla birlikte sınıfsal ayrımların da ortaya çıktığını belirten Rousseau, doğal kaynakların insanlar arasında adaletsiz dağılması ile bir karşılıklı ihtiyaç durumunun ortaya çıktığını ve insanların birbirlerine muhtaç duruma gelerek bir arada yaşamaya başladıklarını belirtmiştir. Rousseau, toplum sözleşmesi ile toplumsal hayata geçen insanların sınıfsal ayrılıklarla ortaya çıkan yoksul ve zengin ayrımını kurumsallaştırdıkları ve eşitsizliğin hukuki ve siyasal bir boyut kazandığını söylemektedir. İnsanların haklarını genel bir iradeye vermesiyle birlikte bir toplumun parçası haline geldiğini söyleyen Roussea'ya göre genel irade, kişilerin bireysel çıkarlarıyla toplumun çıkarlarını bir araya getiren bir kavramdır ve

genel iradenin ortaya çıkarttığı devleti tüm toplumu mutlu edecek iyiliklere yönlendiren bir olgudur (Rousseau, 2013: 53-71). Rousseau'ya göre, hükümetin başlıca görevi, toplumun genel iradesini uygulamak ve yürürlükteki yasaları uygulamaktır. Hükümetin en önemli görevi, genel iradenin yürütülmesidir. Genel irade, toplumun çıkarlarını ve haklarını koruma ve teşvik etme hedefine yöneliktir. Hükümet, yasaların uygulanmasını sağlamakla sorumludur. Yasalar, toplumun düzgün işleyişi ve vatandaşların haklarının korunması için gereklidir (Rousseau, 2013: 148-176).

3.2.2. Siber Uzayda Düzen Arayışı: Siber Toplum Sözleşmesi

Siber uzayın beraberinde getirdiği yeni kullanım alanlarının birey seviyesinden devlet seviyesine hayatın her alanına tezahür etmesiyle birlikte ortaya çıkan siber toplum, aynı zamanda bu yeni alanda bir düzenin oluşturulmasını gerekli kılmıştır. Bu bağlamda devletler, uluslararası örgütler ve özel kuruluşlar bu alanda ortaya çıkan güvenlik tehditleriyle birlikte yeni bir düzen arayışı içerisindedirler. Devletlerin geçtiğimiz son yirmi yıl içerisinde siber uzayın düzenlenmesi bağlamında yaptığı yasal düzenlemeler ve yönetsel anlamda oluşturduğu yeni kurumlar bu alanda atılan önemli adımlardır. Ancak bu durum, sürekli değişen ve gelişen siber uzayda ortaya çıkan yeni toplum düzenin oluşturulmasında siber uzayın doğasına paralel olarak devam eden bir süreç olarak karşımıza çıkmaktadır.

Tamamen insan eliyle üretilmiş ve ortaya çıkmış olan siber uzayın yasal ve yönetsel yapısı bağlamında ortaya çıkan tartışmalar bu alanın gerçek dünyanın hukuk sistemiyle yönetilemeyeceğini savunanlar ve siber alanın düzenlenmesinin benzersiz bir zorluk oluşturmadığını ve gerçek dünya yasalarının siber alanı etkili bir şekilde düzenleyebileceğini iddia edenler şeklinde ikiye bölünmüştür (Horowitz, 2006: 4). Gerçek dünya yasalarının, siber alanda gerçekleşen faaliyetler üzerinde etkili olabilmesi için bu yasaların uygulanabilirliği ve kabul edilmesi genellikle bir dizi faktöre bağlıdır. Bunlar arasında siber faaliyetin doğası, faaliyetin yer aldığı yerler, faaliyeti yürüten birey veya kurumlar ve belirli bir yasanın uygulanabilirliğini etkileyebilecek diğer çeşitli yasal ve teknik faktörlerin olduğunu söylemek mümkündür. Yine de siber alanda yürütülen faaliyetlerin karmaşık doğası, bir dizi benzersiz zorluk ortaya çıkartmaktadır. Bu durum özellikle siber suçlar, ulusal siber

güvenlik, veri koruma ve siber uzayda sahip olunan haklar gibi konuları düzenleme gereksinimlerini içermektedir. Bu nedenle gerçek dünya yasalarının siber alandaki faaliyetleri etkili bir şekilde düzenleyebilmesi için yasaların bu benzersiz zorlukları ve ihtiyaçları hesaba katması gerekmektedir.

Siber uzayın yasal ve yönetsel bağlamda düzenlenmesinde geçek dünya yasalarının çalışmayacağını iddia edenlerin bu düşünceleri, özellikle doksanlı yılların başında bilgisayar teknolojisinin batı dünyasında kullanımının artmasıyla ortaya çıkmıştır. 1990 yılında kurulan ve dijital dünyada sivil özgürlükleri savunan önde gelen kâr amacı gütmeyen bir sivil toplum kuruluşu olan "Electronic Frontier Foundation (EFF)" bu anlamda oldukça önemli bir yerde durmaktadır. EFF etkili dava süreçleri, politika analizleri, tabandan gelen aktivizm ve teknoloji geliştirme yoluyla kullanıcı gizliliğini, özgür ifadeyi ve yeniliği destekleyen bir sivil toplum kuruluşudur. Misyonlarını teknolojinin tüm dünya insanları için özgürlüğü, adaleti ve yeniliği desteklemesini sağlamak olarak tanımlayan EFF'in kurucularından John Perry Barlow'un 1996 yılında "Siber Uzayın Bağımsızlık Bildirgesi" adıyla yayınladığı deklarasyon bu düşüncelerin temelini oluşturmaktadır. Barlow yayınladığı bu bildirgede endüstriyel dünyanın hükümetlerine şu şekilde seslenmektedir:

> "*Endüstriyel dünyanın hükümetleri, et ve çelikten yorgun devler, ben aklın yeni yurdu olan siber uzaydan geliyorum. Geleceği temsilen, siz geçmişin insanlarından bizi rahat bırakmanızı talep ediyorum. Aramıza hoş gelmediniz. Toplandığımız yerde sizin egemenliğiniz yok. Seçilmiş bir hükümetimiz yok, muhtemelen olmayacak. Bu yüzden size özgürlüğün her zaman sahip olduğu otoriteyle sesleniyorum. İnşa ettiğimiz küresel toplumsal alanın bize dayatmaya çalıştığınız zorbalıklardan doğal olarak bağımsız olduğunu ilan ediyorum. Bizi yönetme hakkınız yok, ayrıca gerçekten korkmamız için geçerli bir neden olan herhangi bir uygulama yönteminiz de yok… Kimliklerimizin bedenleri yok, bu yüzden sizin aksinize, fiziksel zorla düzen sağlayamayız. Etik değerler, aydınlanmış öz çıkar ve toplum yararı üzerinden yönetimimizin ortaya çıkacağına inanıyoruz… Siber alanda zihinlerin medeniyetini yaratacağız. Umarız ki bu, hükümetlerinizin daha önce yarattığı dünyadan daha insancıl ve adil olur.*" (EFF, 1996).

Barlow'un bu bildirgesi hızla büyüyen internet üzerindeki bir üst otoritenin uygulanabilirliği veya eksikliği hakkında yayınlanmış önemli bir belgedir. 8 Şubat 1996'da İsviçre'nin Davos kentinden çevrimiçi olarak yayınlanan bu belge, erken internet ideolojisi ve siber uzayda liberal düşüncenin önemli bir kilometre taşı olmakla birlikte dijital haklar gibi sonraki kavramların tarihi bir öncülüdür. Bildirge, internetin

kendi özel ayrı alanı olarak var olduğu ve herhangi bir özel hükümetin kontrolünden bağımsız olduğu fikrini ifade etmektedir. Hükümetlerin internet üzerinde hiçbir yetkisi olmaması gerektiğini savunmakta ve bunu bireylerin kendilerini ifade etme ve birbirleriyle müdahale olmaksızın etkileşim kurma özgürlüğüne sahip oldukları bir alan olarak tanımlamaktadır.

Özellikle siber uzayın coğrafi olarak sınırsız olması ve her an her yerde varlığını sürdürebilme özelliğine sahip olması, bu alanın yasal ve yönetsel bağlamda bir üst otoriteye sahip olması noktasında zorlukları ön plana çıkartmaktadır. Johnson ve Post (1996), siber uzayın coğrafi olarak belirlenmiş sınırlarının olmadığını belirterek siber uzayın her yerde eş zamanlı olarak bulunduğu için içinde coğrafi sınırlar çizmenin mümkün olmadığını savunmuşlardır. Siber uzayla ilgili olarak güvenilir şekilde ayırt edebileceğimiz sadece iki sınır vardır. Bunlardan birincisi, gerçek dünya ile siber uzay arasındaki sınırdır. Siber uzay internetin içinde, gerçek dünya ise dışında yer alır. Bir kişi kolayca kendisinin siber uzayda mı, yoksa gerçek dünyada mı olduğunu belirleyebilir. İkincisi ise, siber alan içindeki belirgin alanları birbirinden ayıran sınırdır. Burada önemli olan konu ise siber uzayın sınırsızlığının gerçek dünya yasalarının siber alanda uygunluğu bağlamında ortaya çıkardığı zorluklardır. Çünkü ilk olarak her bireyin siber uzayda gerçekleştirdiği bir eylem neticesinde gerçek dünyada tam olarak nerede olduğunu belirlemek zor ve potansiyel olarak maliyetlidir. İkinci olarak ise siber uzay işlemlerinin gerçekleştiği alanı belirlemek neredeyse imkansızdır. (Johnson ve Post, 1996: 1368).

Gerçek dünyada ortaya çıkan eylemlerin etkisi genellikle eylemin gerçekleştiği alanla sınırlıdır. Örneğin bir bireyin bir ülke sınırları içerisinde işlediği bir suçun etkisi suçun işlendiği ülkede ortaya çıkar ve o ülkenin kanunlarına göre işlem yapılır. Fakat siber uzayda coğrafi olarak bir sınırın bulunmaması nedeniyle bu alanda ortaya çıkan eylemlerin etkisinin sınırlarını kestirmek oldukça zordur. Dolayısıyla siber uzayın gerçek dünya yasalarıyla yönetilemeyeceğini savunanlar gerçek dünya yasalarının siber uzayda meşru olmadığını ve siber uzayın ya da siber uzay içerisindeki belirli alanların kendi düzenleyici mekanizmaları oluşturabileceğini savunmaktadırlar.

Siber uzayın gerçek dünya yasalarıyla yönetilebileceğini ve düzenlenebileceğini savunanlar ise genellikle bu alanda gerçekleşen eylem ve

işlemlerin teknik ve işlevsel olarak gerçek dünya işlemlerinden çok da farklı olmadığını ve bu bağlamda siber uzayın gerçek dünya yasalarıyla düzenlenebileceğini savunmaktadırlar. Bu bağlamda siber uzayda gerçekleşen bir suçun etkisi nerde ortaya çıkıyorsa oranın kanunlarının geçerli olduğunu savunmaktadırlar (Goldsmith, 1998: 1201). Fakat günümüzde geldiğimiz noktada siber uzayda ortaya çıkan bir suç eyleminin failinin bulunması oldukça zordur. Siber uzayı suçlular için cazip kılan en önemli özellikte zaten budur. Ayrıca bir X ülkesi vatandaşının siber uzayda gerçekleştirdiği bir eylemin sonuçlarının Y ülkesinde ortaya çıkması, X ülkesinde bulunan kişinin Y ülkesinin kanunlarına göre yargılanmasını engellemektedir. Ayrıca X ülkesinin kanun uygulayıcıları tarafından Y ülkesindeki bu kişinin tevkif edilerek kanun önüne çıkartılması X ülkesi ve Y ülkesi arasında siber uzayda işlenen suçlarla alakalı olarak bu bağlamda bir anlaşma ve iş birliği söz konusu değilse mümkün değildir. Dolayısıyla her ne kadar siber uzayın yasal ve yönetsel olarak düzenlenmesi gerçek dünya yasalarıyla bir noktaya kadar mümkün görünse de bu alanın düzenlenmesi ve yönetimi yine ancak bu alana özel olarak geliştirilmiş bir düzenleme ve uluslararası iş birliği ile mümkün olabilecek bir durumdur.

Tüm bunlar ışığında değerlendirildiğinde siber uzayda bir düzenin oluşturulması yeni bir toplumsal sözleşmenin gerekliliğini ortaya koymaktadır. Daha önce de belirtildiği üzere toplum sözleşmesi kavramı, yönetilenler ile yöneticileri arasındaki gerçek veya varsayımsal bir anlaşmayı ifade eder ve her bir tarafın haklarını ve görevlerini tanımlar. Bu kavram, yöneticilerin vatandaşlarına belirli haklar ve hizmetler sağlama taahhüdünde bulunduğu ve karşılığında vatandaşların belirli sorumlulukları ve yükümlülükleri olduğu bir anlaşmayı temsil eder.

Bu anlaşmanın amacı, genellikle toplumun düzenini ve istikrarını sağlamaktır. Toplum sözleşmesi teorisi, bireylerin kendi doğal haklarından bazılarını kendilerinden üst bir otoriteye devrettiklerini kabul ettikleri bir sosyal düzenin kurulmasını açıklar. Bu şekilde, bireyler belirli bir güvenlik ve düzen seviyesini garanti altına alırken, aynı zamanda bu otoriteye belirli yetkileri kullanma hakkı verirler. Siber toplum bağlamında toplum sözleşmesi kavramı, siber uzayın ortaya çıkarttığı birçok yenilikle birlikte düzenlenmesi gereken kişisel verilerin korunması ve mahremiyet, siber güvenlik ve veri güvenliği gibi konularda düzenin oluşturulmasını konu alır. Dolayısıyla günden güne dijitalleşen günümüz toplumlarının siber uzayın getirdiği

yeni zorluklar, güvenlik tehditleri, kolaylıklar ve fırsatları dikkate alarak geleneksel anlamda ortaya çıkan toplum sözleşmesi temelinde yeni bir "siber toplum sözleşmesi" ortaya çıkartarak tüm bu değişikliklere ayak uydurması gerekebilir.

Thomas Hobbes'un toplum sözleşmesi teorisi, siber toplumu değerlendirmek için ilginç bir çerçeve sağlar. Hobbes'a göre, insanların doğal durumu kaos ve çatışma içindedir. Siber ortamda bu durum siber suç, kimlik hırsızlığı, veri ihlalleri ve diğer çeşitli tehditlerle karakterize edilebilir. Bireylerin sınırsız hakları varken, bu haklar çatışabilir ve sonuçta siber güvensizliğe yol açabilir. Siber ortamda toplum sözleşmesi, bireylerin belirli haklarını bir düzenleyici otoriteye (hükümet, siber güvenlik firmaları vb.) devretmeyi kabul ettikleri bir anlaşma şeklinde olabilir. Bu düzenleyici otorite, karşılığında bireylerin geri kalan haklarını (örneğin siber uzayda güvende olma hakkını) korur ve genel siber güvenliği sağlar.

Hobbes'un Leviathan'ı, siber ortamda bir tür egemen otorite olabilir. Bu durum siber suçla mücadele ve siber güvenliği sağlama yeteneğine sahip hükümetler veya uluslararası kuruluşlar şeklinde tanımlanabilir. Hobbes'un düşüncelerine dayanarak bu otoritenin gücünün mutlak olması gerektiğini söylemek ise yanlış olmayacaktır. Ancak bu durum siber uzayda bireylerin haklarının ve özgürlüklerinin korunması ile düzen ve güvenlik arasındaki hassas dengeyi bulmayı gerektiren bir durumdur. Hobbes, bireylerin hayatta kalma hakkına ve kendi çıkarlarını koruma hakkına önem verir. Siber ortamda, bu haklar kişisel verilerin koruması, gizlilik, mahremiyet, kimlik bilgilerinin güvenliği, banka işlemlerinin güvenliği ya da ifade özgürlüğü gibi haklar olarak değerlendirilebilir. Egemen otoritenin bu hakları koruma ve genel siber güvenliği sağlama görevi oluşturulacak olan siber toplum sözleşmesinin temel dayanağı olmalıdır. Hobbes'un teorisiyle ilgili tartışmalar, gizlilik ve güvenlik arasındaki dengenin nasıl sağlanacağı, siber suçlara nasıl yanıt verileceği, verilerin koruması ve siber güvenlikle ilgili hükümet politikalarının oluşturulması gibi siber toplumun önemli konularına ışık tutabilir.

Öte yandan, Locke'un toplum sözleşmesi teorisi siber toplumda güvenliği sağlama ve online suçları önleme sorumluluğu olan devlete de işaret etmektedir. Bu durum, devletin internet üzerinde bir tür düzenleyici rol oynamasını gerektirir. Ancak bu rol, bireylerin özgürlüklerini sınırlayıcı nitelikte olmak yerine onları korumalıdır.

Locke'un toplum sözleşmesi teorisi çerçevesinde siber toplumu değerlendirmek, bir dizi zorluğu da beraberinde getirir. Özellikle, siber alanda devletin hangi düzenlemeleri yapabileceği ve bireylerin özgürlüklerini nasıl koruyabileceği konuları oldukça karmaşıktır.

Rousseau'nun toplum sözleşmesi teorisine göre ise bireyler haklarını ve özgürlüklerini bir "genel irade" oluşturmak için topluma devrederler. Bu genel irade, her bireyin çıkarlarının ve haklarının korunmasını sağlayacak bir iradedir. Siber toplumda Rousseau'nun teorisinin gerçekleşebilmesi için bireylerin verilerinin ve dijital kimliklerinin güvenliğini ve özgürlüğünü korumak için haklarını ve özgürlüklerini bir "siber genel irade" ye devretmelerinin gerektiğini söylemek mümkündür. Bu genel irade, siber toplumun düzenini, adil erişimi ve tüm üyelerin haklarını koruyacak şekilde yönetilmesi gereken bir irade olmalıdır. Rousseau'nun teorisinde olduğu gibi siber genel irade, tüm toplumun üyelerinin en iyi çıkarına hizmet etmeli ve bireysel özgürlüklere gereksiz bir sınırlama getirmemelidir. Aksine, genel iradenin amacı, her bireyin siber toplumda eşit, adil ve güvende olmasını sağlamaktır. Bu durum bireysel hakları korurken aynı zamanda siber suçları önleme ve siber toplumun güvenliğini ve istikrarını sağlama çabasını içerecek şekilde olmalıdır.

Rousseau'nun toplum sözleşmesi teorisi ayrıca toplumun kurallarının ve normlarının, toplumun tüm üyeleri tarafından kabul edilen ve desteklenen bir "genel irade" tarafından belirlenmesi gerektiğini savunmaktadır. Siber toplumda bu durum kullanıcıların ve hükümetlerin siber alanın düzenini ve güvenliğini sağlamak için birlikte çalışmasını gerektirmektedir. Rousseau'nun toplum sözleşmesi teorisi siber toplumun düzenini ve güvenliğini sağlamak için bir çerçeve sağlayabilecek niteliktedir. Bu çerçeve, siber toplumun tüm üyelerinin haklarını ve özgürlüklerini korurken aynı zamanda siber toplumun istikrarını ve güvenliğini sağlamayı hedefler.

Rousseau'nun toplum sözleşmesi teorisi temelinde bir siber toplum sözleşmesi oluşturulacak olursa bu sözleşmenin siber toplumun tüm üyeleri tarafından eşitlik, özgürlük ve adalet ilkeleri temelinde oluşturulacak bir sözleşme olması beklenebilir. Siber toplumun üyelerinin verilerinin ve bilgilerinin güvenliği, gizliliği ve bütünlüğü için ortak bir genel irade oluşturularak toplumun üyelerinin birbirlerine karşı

sorumluluklarını ve siber topluma olan yükümlülüklerin belirleneceği bu sözleşmeye göre her birey siber toplumda bilgiye erişme, ifade özgürlüğüne sahip olma ve dijital alanı güvenli ve saygılı bir şekilde kullanma hakkına sahip olmalıdır. Tüm bireyler siber toplumda eşit haklara sahip olmalıdır. Hiçbir birey veya grup, veriye erişim, bilgi paylaşımı veya teknoloji kullanımı konusunda diğerlerinden üstün tutulmamalıdır. Siber toplumda adaletin sağlanması için veri kullanımı ve dijital kaynaklara erişim konusunda şeffaflık ve hesap verebilirlik olmalıdır. Her bireyin dijital verilerinin ve bilgilerinin güvenliğini sağlamak, toplumun tüm üyelerinin sorumluluğudur. Bu durum siber suçlara karşı koyma ve siber güvenlik önlemlerini uygulama gerekliliğini içerir. Siber toplumun tüm üyeleri, genel iradenin bütünlüğünü korumak ve toplumun tüm üyelerinin haklarını ve özgürlüklerini garanti altına almak için birlikte çalışmalıdır.

Liaropoulos'un belirttiği üzere "*doğa durumundan veri durumuna*" (Liaropoulos, 2020: 4) geçen günümüz toplumu, dijitalleşme ile siber uzayı hayatın vazgeçilmez bir parçası haline getirmiştir. Toplum sözleşmesi teorisinin temelini oluşturan doğa durumunu siber uzayla birlikte ortaya çıkan siber toplumun şu an içerisinde bulunduğu durum olarak tanımlayan Liaropoulos bu durumu siber toplumun veri durumu olarak aktarmaktadır (Liaropoulos, 2020: 6). Şu an veri durumunda olan siber toplumun, antik çağlarda doğa durumunu terk ederek toplumu oluşturan insanları bu durumdan çıkmaya iten sebepler gibi veri durumundan çıkmaya itecek sebeplerin olacağını varsaymak yanlış olmayacaktır. Özellikle siber uzayın şu anki karmaşık ve kontrol edilemez yapısı anarşinin olduğu ve tam olarak güvenliğin olmadığı bir durumu ortaya çıkartmaktadır. Siber uzayın aktörlerinin her ne kadar hükümetlerin belirli sınırlamaları olsa da neredeyse tam bir özgürlük halinde doğa durumunda olduğu siber uzayda ortaya çıkacak toplum sözleşmesinin genel hatlarının çizilmesi bir zorunluluk haline gelmektedir.

17. yüzyılda insanlık ilahi yönetimden popüler egemenliğe doğru bir otorite ve meşruiyet değişimi yaşamıştır. Korku, insanları anarşi ve belirsizliğin doğal durumundan çıkarmaya ve güvenlerini yeni bir siyasi varlık olan egemen devlete emanet etmeye teşvik etmiştir. Benzer şekilde dijital çağda bilgi, varlık ve otorite açısından benzer bir değişim yaşanmaktadır. Bugün, insanlığın büyük bir kısmı verilerin hâkim olduğu bir dijital toplumda yaşamaktadır. Veriler küresel ekonomiyi

yönlendirmekte ve bu verilerle yeni bilgiler üretilmektedir (Liaropoulos, 2020: 7). Ancak bu durum aynı zamanda korku ve eşitsizlik durumu ortaya çıkartmaktadır. Dolayısıyla siber uzayın kullanımının düzenlenmesi bir gereklilik haline gelmektedir.

Elbette toplum sözleşmesi düşüncelerinin ortaya çıktığı 17. yüzyılın şartlarıyla içerisinde bulunduğumuz 21. yüzyılın şartlarının aynı olması beklenemez. Lakin özellikle Hobbes, Locke ve Rousseau'nun toplum sözleşmesi fikirlerinde farklı şekillerde ortaya koyduğu doğa durumu, siber uzayın ve beraberinde oluşan siber toplumun içerisinde bulunduğu durumu açıklar niteliktedir. Genel kabul görmüş bir üst otoritenin olmadığı, siber kapasitenin gerçek dünyada işlenen birçok suç için kullanıldığı ve suçluların yakalanma riskinin oldukça düşük olduğu bu anarşi düzeni, aynı zamanda insanların özgürce fikirlerini beyan edebildikleri ve iletişim kurabildikleri bir alan olarak varlığını sürdürmektedir. Bu alanın düzenlenmesi adına gerek hükümetler gerekse de uluslararası örgütler ve özel kuruluşlar tarafından yapılan girişimler ise yeni bir siber toplum sözleşmesinin başlangıç süreci olarak değerlendirilebilir. Sürekli değişen ve gelişen siber uzayın düzenlenmesi noktasında ortaya çıkacak toplum sözleşmesinin de benzer şekilde gelişim ve değişime açık olması gerektiği ise oldukça açıktır.

ÜÇÜNCÜ BÖLÜM

ULUSAL VE ULUSLARARASI BOYUTTA TÜRKİYE'DE DİJİTALLEŞME VE SİBER GÜVENLİK

1990'lı yılların başından itibaren Türkiye siber uzayda ortaya çıkabilecek güvenlik tehditlerine karşı gerek yasal gerekse de yönetsel bağlamda birçok düzenlemeye gitmiştir. Yapılan bu düzenlemeler çoğu zaman birbirinden bağımsız bir şekilde gerçekleştirilmiş olsa da siber uzayın güvenliğinin sağlanmasında atılan önemli adımlar olarak değerlendirilebilir. Farklı kanun, yönetmelik, genelge ve tebliğlerle bu alanın yasal olarak düzenlenmesi konusunda atılan adımlar kimi zaman ikiliklere yol açsa da yasal temelde yapılan düzenlemeler özellikle siber uzayda ortaya çıkması muhtemel tehditlere karşı caydırıcılık oluşturması bağlamında oldukça önemlidir.

Türkiye'de siber uzayda işlenen suçların düzenlenmesi adına oluşturulmuş tek bir kanun bulunmamaktadır. Siber uzayda bilişim alanında işlenen suçların düzenlenmesi mevcut kanunlara ilgili hükümlerin eklenmesiyle düzenlenmiştir (BTK, 2017). İlk defa 6 Haziran 1991 tarihinde "3756 Sayılı Türk Ceza Kanunu'nun Bazı Maddelerinin Değiştirilmesine Dair Kanun" ile siber uzayda işlenen suçlar bağlamında bir düzenlemeye gidilmiştir. 2000'li yılların başına gelindiğinde ise siber uzayın kullanımının yaygınlaşması ile Türkiye siber güvenliğin sağlanması ve siber uzayda caydırıcılığın kazanılması adına daha somut ve ciddi adımlar atmaya başlamıştır. Bu anlamda 1991 yılında yapılan düzenlemeden çok daha kapsamlı olarak 2004 yılında siber suç kavramının kanunla tanımının yapıldığı ve "Bilişim Alanında Suçlar" başlığıyla 5237 sayılı Türk Ceza Kanunun (TCK) onuncu bölümünde siber uzayda işlenen suçlarla alakalı olarak özellikle bilişim alanında olmak üzere önemli düzenlemelere gidilmiştir.

Ülkemizde internetin yasal boyutta düzenlenmesi en kapsamlı şekilde 2007 yılında 5651 sayılı "İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu

Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun" ile gerçekleşmiştir (5651 Sayılı Kanun, 2007).

Siber uzayın güvenliğinin sağlanması adına yapılan önemli yasal düzenlemelerden bir diğeri ise 2008 yılında kabul edilen 5809 sayılı "Elektronik Haberleşme Kanunu" olmuştur. Bu kanunla elektronik haberleşme sektöründe haksız rekabetin önüne geçilmesi ve bu alanda sağlanacak hizmetlerin aktif ve etkili bir şekilde yerine getirilmesi hedeflenmiştir. Ayrıca temel hak ve özgürlüklerin korunması bağlamında bireylerin siber uzayda iletişim özgürlüğünün ve güvenliğinin tesis edilmesi noktasında atılan önemi bir adım olarak değerlendirilmesi gereken bir kanun olarak karşımıza çıkmaktadır.

Elektronik Haberleşme Kanununa ek olarak yine aynı yıl meclise sunulan ve siber güvenliğin sağlanmasında hayati önem taşıyan kişisel verilerin korunmasını sağlayacak olan 6698 sayılı "Kişisel Verilerin Korunması Kanunu" her ne kadar kabul edilmesi oldukça uzun bir süre alsa da 7 Nisan 2016 yılında kanunlaşarak yayımlanmıştır. Günümüzde e-devlet uygulamalarının oldukça yaygınlaştığı ve hemen her devlet kurumunda kişisel verilerin dijital ortamlarda saklandığı ve sadece e-devlet uygulamalarında değil aynı zamanda alışveriş sitelerinde ve sosyal medya platformlarında insanların kişisel verilerinin dijital olarak saklandığı düşünüldüğünde bu kanun özellikle özel hayatın gizliliğinin korunmasında kötü niyetli kullanıcılar için caydırıcı bir nitelik taşımaktadır.

Türkiye siber güvenlik anlamında sadece yasal düzenlemeler yapmakla kalmamış aynı zamanda kurumlar temelinde de çeşitli düzenlemelere giderek gerek bağımsız gerekse mevcut olan kurumlar içerisinde siber güvenlik birimleri oluşturmaya başlamıştır. 27 Ekim 2010 tarihli "Milli Güvenlik Kurulu (MGK) Bildirisinde" siber tehdidin küresel anlamda ulaştığı boyut ve bu tehdidin ulusal güvenliğe etkileri oldukça kapsamlı bir şekilde ele alınmış ve siber tehdidin engellenebilmesi için milli düzeyde yürütülen çalışmalar değerlendirilmiştir. Ülkenin en üst düzey ulusal güvenlik kurulunun siber uzayın güvenliği konusunda göstermiş olduğu bu hassasiyet, konunun Türkiye açısından önemini bir kez daha vurgulamıştır (Şenol, 2017: 6).

Türkiye'de siber güvenliğin sağlanmasında kurumsal bazda koordinasyonun sağlanması görevi 2011 yılında yayımlanan 655 Sayılı Ulaştırma, Denizcilik ve Haberleşme Bakanlığı'nın (UDHB) Teşkilat ve Görevleri Hakkında Kanun Hükmünde Kararname'nin (KHK) "Sürekli ve Geçici Kurulların Kurulması ve İşleyişini" düzenleyen 29'uncu maddesinin yedinci fıkrası ve "Çalışma ve Rehberlik Gruplarını" düzenleyen 30'uncu maddenin kapsamıyla bağlantılı olarak, 2012 yılında yayımlanan 2012/3842 sayılı "Ulusal Siber Güvenlik Çalışmalarının Yürütülmesi, Yönetilmesi ve Koordinasyonuna İlişkin Bakanlar Kurulu Kararı" ile Ulaştırma, Denizcilik ve Haberleşme Bakanlığı'na[16] (UDHB) verilmiştir (Resmî Gazete, 655 Sayılı KHK, 2011: Md. 29-30; Resmî Gazete, 2012/3842 sayılı Ulusal Siber Güvenlik Çalışmalarının Yürütülmesi, Yönetilmesi ve Koordinasyonuna İlişkin Bakanlar Kurulu Kararı, 2012: Md. 3-4). Bahsi geçen 2012/3842 sayılı Bakanlar Kurulu kararı ile UDHB başkanlığında "Siber Güvenlik Kurulu" kurularak siber güvenliğe yönelik ilkeler, teşkilat, görev ve sorumluluklar belirlenmiştir.

Siber Güvenlik Kurulu tarafından "Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı" kabul edilerek yayımlanmıştır. Türkiye'nin siber güvenlik alanında ilk defa hazırladığı bu eylem planında bilgi ve iletişim sistemlerinin kullanımının arttığı ve kurumların yanı sıra kritik altyapıların kontrollerinde bilgi ve iletişim sistemlerinin kullanımının hayati olduğu vurgulanmıştır (Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı, 2012). 2013-2014 Eylem Planının ardından 2016 yılında UDHB koordinasyonunda 2016-2019 Ulusal Siber Güvenlik Stratejisini açıklamıştır (UDHB, 2016). Türkiye'nin siber güvenlik stratejisi bağlamında izleyeceği yolu belirleyen bu çalışma ise siber uzayın güvenliğinin sağlanmasının ve yasal düzenlemelerin getirilmesinin gerekliliğini bir kez daha ortaya koymuş ve bu anlamda siber güvenlik stratejilerinin belirlenmesinin bir ulusal güvenlik önceliği olduğunu vurgulamıştır (2016-2019 Ulusal Siber Güvenlik Stratejisi, 2016). Türkiye son olarak 2020-2023 Ulusal Siber Güvenlik Stratejisi ve Eylem Planını yayımlamış ve daha önceki çalışmalar üzerinden yapılanlar değerlendirilerek gerekli iyileştirmeler

[16] Ulaştırma, Denizcilik ve Haberleşme Bakanlığı'nın adı Cumhurbaşkanlığı Hükümet Sistemi'ne geçilmesiyle, 10/07/2018 tarihli ve 30474 sayılı Resmî Gazetede yayımlanan 1 No'lu Cumhurbaşkanlığı Teşkilatı Hakkında Cumhurbaşkanlığı Kararnamesi ile "Ulaştırma ve Altyapı Bakanlığı" olarak değiştirilmiştir.

yapılmış ve bu planı güncellemiştir (2020-2023 Ulusal Siber Güvenlik Stratejisi ve Eylem Planı, 2020).

Siber suçlarla mücadele ve istihbari faaliyetler yürüten kurumlar içerisine kolluk kuvvetlerini oluşturan kurumların siber güvenlik ile ilgili oluşturdukları alt birimler yer almaktadır. Bu bağlamda daha önce 2011 yılında kurulan "Emniyet Genel Müdürlüğü Bilişim Suçlarıyla Mücadele Daire Başkanlığı" ve sonrasında 2013 yılında isim değiştirerek faaliyetlerine devam eden "Siber Suçlarla Mücadele Daire Başkanlığı", "Jandarma Genel Komutanlığı Muhabere Elektronik Bilgi Sistemleri Başkanlığı ve Siber Suçlarla Mücadele Daire Başkanlığı" gibi kurumlar da siber uzayda güvenliğin sağlanması adına oluşturulan birimlerdir.

Ayrıca siber savunma ve saldırı yeterliliğinin artırılmasını sağlayan kurumlar Türkiye'nin siber uzayda maruz kalabileceği saldırıların bertaraf edilmesi ve olası bir saldırı durumunda izlenecek stratejilerin belirlenmesinde uzmanlaşmaya çalışmaktadırlar. Tüm bunlardan daha da önemlisi, bu kurumlar olası bir siber saldırının başarıya ulaşmaması için gerekli olan teknolojik altyapıyı oluşturmak adına çalışmalar yapmaktadırlar. Bilgi Teknolojileri ve İletişim Kurumu (BTK), Türk Silahlı Kuvvetleri (TSK) Siber Savunma Komutanlığı, Türkiye Bilimsel ve Teknolojik Araştırmalar Kurumu (TÜBİTAK), Millî İstihbarat Teşkilâtı Başkanlığı (MİT) gibi kurumlar bu çerçevede değerlendirilmesi gereken kurumlardır.

Siber güvenliğin sağlanmasında teknoloji üreten yarı özel kurumlar Türkiye'nin siber uzayda güvenlik anlamında ihtiyacı olan teknolojik altyapıyı geliştirmek ve bu konuda yaptıkları araştırmalarla alanla ilgili faaliyette bulunan diğer kurumların teknolojik alt yapısını desteklemek üzerine çalışmaktadırlar. Bu bağlamda Askeri Elektronik Sanayi (ASELSAN), Hava Elektronik Sanayii (HAVELSAN) ve Savunma Teknolojileri Mühendislik (STM) gibi kurumlar diğer faaliyetlerine ek olarak siber güvenlik alanında da önemli faaliyetler yürütmektedirler.

Türkiye siber güvenlik alanında 2000'li yıllar itibari ile yasal düzenlemeler, yeni kurumsal yapılanmalar ve siber güvenlik stratejilerinin belirlenmesi bağlamında daha somut adımlar atmaya başlamıştır. Bu anlamda ilk defa 2003 yılında yayımlanan 2003/10 sayılı Başbakanlık Genelgesi ile bir güvenlik kültürünün oluşturulması

amaçlanmış ve bu amaç kapsamında bazı ilkeler sıralanmıştır. Bu ilkelerin bilgi sistem ve ağlarına yönelik tehditlerin önlenmesi adına izlenmesinin önemi de ayrıca belirtilmiştir (Şenol, 2017: 5). Yine aynı yıl Devlet Planlama Teşkilatı (DPT) tarafından "E-Dönüşüm Türkiye Projesi" ilan edilmiştir (DPT, 2004). 2009 yılında Bilgi Teknolojileri Kurumu (BTK) tarafından hazırlanan "Siber Güvenliğin Sağlanması: Türkiye'deki Mevcut Durum ve Alınması Gereken Tedbirler" başlıklı rapor ise siber güvenliğin sağlanması ve mevcut durumun anlaşılması anlamında atılan önemli bir adımdır (BTK, 2009).

Siber uzayın güvenliği sorunun erken farkına varan ülkelerden birisi olan Türkiye'de 1990'lı yılların başından itibaren bu alanın güvenliğinin sağlanması adına yapılan yasal ve yönetsel düzenlemeler ve bunlara ek olarak Türkiye'nin uluslararası anlamda siber güvenliğin sağlanması adına yaptığı girişimler tezin bu bölümünde detaylarıyla ele alınarak incelenecektir. Her gün daha fazla dijitalleşen Türkiye'de yapılan tüm bu düzenlemeler iki temelde değerlendirilecektir. Bu bölümde ele alınacak olan siber uzayda temel hak ve özgürlüklerin korunması ve ulusal siber güvenliğin sağlanması adına yapılan yasal düzenlemeler ilk temeli oluşturmaktadır. Daha önce teorik bağlamda soyut olarak ele alınan siber uzayın güvenliği konusu, incelenecek olan somut düzenlemelerle özellikle siber toplum sözleşmesi olgusuna bir temel oluşturacak şekilde değerlendirilmelidir. Ayrıca idealizm, liberalizm ve realizm temelinde ele alınan siber güvenlik olgusu, bu bölümde Türkiye örneği üzerinden yapılan yasal düzenlemeler bağlamında değerlendirildiğinde ortaya konulan teorik çerçevenin daha somut olarak algılanması hedeflenmektedir. Bu değerlendirmenin ikici temelini oluşturan siber uzayın güvenliğinin sağlanmasında yapılan yönetsel düzenlemeler ise dördüncü bölümde ele alınacaktır.

1. DİJİTALLEŞEN TÜRKİYE

1.1. Türkiye'de Dijital Dönüşüm

Türkiye'de ilk defa 1960 yılında Karayolları Genel Müdürlüğü'nde (KGM) kullanılmaya başlanan bilgisayar IBM firması tarafından üretilen "IBM-650 Data Processing Machine" olmuştur (KGM, 2023). Bir insanın çok uzun sürelerde yapabileceği bir işi oldukça kısa sürelerde yapabilen bu büyük, lambalı ve gürültülü

alete “Elektronik Beyin” isminin takıldığı (NTV Haber, Türkiye’de Bilişimin Öyküsü I, 2000) günlerden 1990’lı yıllara kadar birçok farklı devlet kurumu bilgisayarla tanışmış ve kendi bünyelerinde kullanmaya başlamıştır. Günümüz bilgisayarlarıyla karşılaştırıldığında oldukça basit işlemler yapabilen bu bilgisayarların devlet kurumları bünyesinde daha yaygın kullanılmaya başlanması ile bu alanda bir düzenlemenin yapılması gerekli hale gelmiştir. Türkiye’nin 1960 yılında ilk defa tanıştığı bilgisayar teknolojisi, ülkenin dijitalleşme yolunda attığı ilk adım olarak değerlendirilebilir. Bilgisayarın ilk defa kullanılmaya başlandığı 1960 yılından günümüze Türkiye, dijital dönüşüm yolunda büyük bir evrim geçirmiştir. Bilgisayar teknolojisinin birçok devlet kurumunda hizmete girmeye başlamasının ardından özellikle üretim sektöründe komuta kontrol sistemlerinin kullanımının yaygınlaşmaya başlaması ile üretimde verimliliğin artması ve iş sürelerinin azalması dijitalleşmeye olan ilginin artmasına neden olmuş ve bilgisayar teknolojisinin sürekli gelişmesi ile de dijitalleşme kamu sektöründen özel sektöre ve bireysel kullanıma kadar her alanda aktif hale gelmeye başlamıştır.

Türkiye’de dijitalleşme girişimleri ilk olarak 1990’lı yıllarda özellikle Avrupa Birliği’ne (AB) üyelik sürecinde uyum çalışmaları kapsamında başlatılmıştır. Bunun yanında tüm dünyada gelişen teknolojiye ayak uydurulması, bürokratik işlemlerde etkinlik ve süreçlerin hızlandırılması, kamu hizmetlerinde hızlı ve güvenli işlemlerin gerçekleştirilebilmesi ve bürokrasinin geleneksel ve kâğıda dayalı işlemlerinin dijital ortamda çok daha az masraf ve hızlı bir şekilde gerçekleştirilebileceğinin anlaşılması dijitalleşme yolunda atılan adımları hızlandırmıştır.

Bilgi ve iletişim teknolojilerinde (BİT) ortaya çıkan gelişmelerle belirgin hale gelen “bilgi toplumu” kavramı hayatın her alanına sirayet eden teknolojiyle birlikte küresel bağlamda toplumların girdiği dönüşüm sürecini ifade etmektedir. Kamu kurumları, özel sektör, üretim ve tüketim süreçleri, eğitim, sağlık ve siyaset gibi birçok alanda toplumsal refahı en yüksek seviyeye çıkartan bu yeni ekonomik ve sosyal düzene geçiş süreci, ilk defa 1993 yılında Dünya Bankası ile yapılan iş birliği kapsamında “Türkiye, Bilişim ve Ekonomik Modernizasyon” çalışması ile gündeme gelmiştir. 1998 yılında başlayan KamuNet projesi ve yine aynı yıl yayımlanan Başbakanlık Genelgesi ile Devlet Planlama Teşkilatı (DPT) bünyesinde “KamuNet Teknik Kurulu” kurulmuştur (DPT, e-Dönüşüm Türkiye Projesi: 2003-2007 Arası

Gelişmeler, 2007). Türkiye'nin 2001 yılında taraf olduğu "eAvrupa+ Eylem Planı" programı çerçevesinde e-Devlete geçiş sürecinin planlanması ve koordinasyonunun sağlanması amacıyla DPT çatısı altında oluşturulan "Yönetim Bilgi Merkezi Dairesi" ile Türkiye'nin dijitalleşme sürecinde bilgi toplumuna geçiş süreci ve BİT'in getirdiği fırsat ve olanaklardan toplumun maksimum seviyede faydalanması, devletin etkin, şeffaf, güvenli, hızlı ve kesintisiz bir şekilde hizmet sunması amacıyla e-kurumların oluşturulmasının sağlanması ve devlet ile vatandaş arasındaki ilişkilerin elektronik ortama taşınması amaçlanmıştır (DPT, e-Devlet'e Geçiş Sürecinde KamuNet Çalışmaları, 2002).

1999 yılında Ulaştırma Bakanlığı ve TÜBİTAK tarafından hazırlanan "Türkiye Ulusal Enformasyon Altyapısı Anaplanı", e-Ticaret Koordinasyon Kurulu'nun kurulması ve Başbakanlık tarafından 2001 yılında başlatılan "e-Türkiye Girişimi", Türkiye'nin dijitalleşme yolunda attığı en önemli adımlardan birisidir. Bu bağlamda 2002 yılında hazırlanan "e-Türkiye Girişimi Eylem Planı" taslağında bilgi toplumuna geçiş süreci, daha ucuz, daha hızlı ve daha güvenli internet erişiminin sağlanması, internet kullanımının yaygınlaştırılması, e-devlet, e-eğitim, e-ticaret, e-sağlık, e-çevre gibi konular ele alınmıştır (AB Başkanlığı, 2007). 2003 yılında 58. Hükümet tarafından hazırlanan Acil Eylem Planı'nda (AEP) "e-Dönüşüm Türkiye" projesine yer verilmiş (T.C. 58. Hükümet AEP, 2003: 2) ve bu plan kapsamında vatandaşın iş ve işlemlerinin hızlandırılması, kamu hizmetlerini vatandaşın ayağına götürmek ve bu hizmetlerde kırtasiyeciliği önlemek, şeffaflık ve hızlılığı sağlamak, elektronik veri ve imzanın yasalaştırılması, kamu kurumları arasındaki iş akışının standart ve uyumlu hale getirilmesi, her kamu kurumunun kendi veri sistemini kurması ve e-devlet uygulaması ile ilgili çalışmaların başlatılarak hayata geçirilmesi planlanmıştır (T.C. 58. Hükümet AEP, 2003: 27-28).

2003 AEP ve e-Dönüşüm Türkiye Projesi çerçevesinde DPT tarafından "2003-2004 e-Dönüşüm Kısa Dönem Eylem Planı" ve "2005 e-Dönüşüm Eylem Planı" hazırlanarak yayımlanmıştır (DPT, e-Dönüşüm Türkiye Projesi: 2003-2007 Arası Gelişmeler, 2007). Türkiye'nin dijitalleşme yolunda attığı en büyük adım ise 2006 yılında 2006/10316 sayılı Bakanlar Kurulu Kararı ile e-Devlet kapısının kurulması kararı olmuştur. İlgili Bakanlar Kurulu Kararına göre kamu hizmetlerinin tek bir platformda elektronik ortamda güvenli ve etkin bir şekilde verilmesi öngörülmüş ve

bu bağlamda e-Devlet Kapısının kurulması ve yönetilmesi görev ve sorumluluğu Başbakanlık adına Ulaştırma Bakanlığı'na verilmiştir (Resmî Gazete, 2006/10316 sayılı Bakanlar Kurulu Kararı, 2006: Md. 1). 2006/10316 sayılı Bakanlar Kurulu Kararı kapsamında yayımlanan 2006/22 sayılı Başbakanlık Genelgesi ile e-Devlet Kapısının kurulması sürecinde *"kamu hizmetlerinin elektronik ortamda, ortak bir platformda ve vatandaş odaklı sunumu için iş süreçlerinin gözden geçirilmesi, içerik yönetimi, entegrasyon ile ilgili standartlar ve gerekli hukuki düzenlemeler konusundaki çalışmalar, Ulaştırma Bakanlığının koordinasyonunda ve ilgili kamu kurum ve kuruluşlarının etkin katılımıyla Türksat Uydu Haberleşme ve Kablo TV İşletme A.Ş. tarafından yürütülecektir."* (Resmî Gazete, 2006/22 sayılı Başbakanlık Genelgesi, 2006). Yine aynı yıl DPT tarafından hazırlanan 2006-2010 Bilgi Toplumu Stratejisi dijitalleşme yolunda sosyal dönüşüm, BİT'in iş dünyasına nasıl etki ettiği ve edeceği, vatandaş odaklı hizmet dönüşümü ve kamu yönetiminde modernizasyon konularını ele alınmıştır (DPT 2006-2010 Bilgi Toplumu Stratejisi, 2006). 2007 yılında yayınlanan 2007/7 sayılı Başbakanlık Genelgesi ile de "e-Dönüşüm Türkiye Projesi Kurumsal Yapılanması" belirlenmiştir (Resmî Gazete, 2007/7 sayılı Genelge, 2007). 2001 yılında 641 sayılı Kanun Hükmünde Kararname (KHK) ile kapatılan DPT yerini Kalkınma Bakanlığı'na bırakmış ve Bakanlık tarafından konuyla ilgili olarak 2015 yılında "2015-2018 Bilgi Toplumu Stratejisi ve Eylem Planı" hazırlanarak yayımlanmıştır (Kalkınma Bakanlığı, 2015). Ayrıca 2016 yılında Ulaştırma, Denizcilik ve Haberleşme Bakanlığı tarafından hazırlanan "2016-2019 Ulusal e-Devlet Stratejisi ve Eylem Planı" yayımlanmış ve bu kapsamda eylem planı izleme modeli ve sistemi geliştirilmiştir (Resmî Gazete, 2016-2019 Ulusal e-Devlet Stratejisi ve Eylem Planı, 2016).

Son yıllarda üzerinde yoğun bir şekilde durulan dijitalleşme kavramı, "2019-2023 On birinci Kalkınma Planı" içerisinde de kendisine yer bulmuştur. Planın 2.2.1.1.6. maddesinde dijital dönüşümün hızlandırılmasıyla öncelikli sektörlerde üretkenliğin ve rekabet gücünün artırılmasının amaçlandığı belirtilmiştir. Özellikle imalat sanayisinde dijital dönüşümün önemi vurgulanmış ve bu bağlamda iş birliği ve bilgi paylaşımının güçlendirilerek ara yüzlerin ve standartların oluşturulması ve bu konuda farkındalığın artırılması hedeflenmiştir (On Birinci Kalkınma Planı, 2019: 74-75). 2021 yılında Hazine ve Maliye Bakanlığı ile Strateji ve Bütçe Başkanlığınca

hazırlanan 4633 sayılı "2022 Yılı Cumhurbaşkanlığı Yıllık Programı" kapsamında da dijital dönüşüm konusu üzerinde durulmuştur. Planda On Birinci Kalkınma Planında yer verilen öncelikli sektörlerde dijital dönüşümün hızlandırılmasıyla üretkenliğin ve rekabet gücünün artırılmasının temel amaç olduğu belirtilmiştir (Strateji ve Bütçe Başkanlığı, 2021, 2022 Yılı Cumhurbaşkanlığı Yıllık Programı).

1.2. e-Devlet Kapısının Hizmete Girmesi ve Sunulan Hizmetler

2008 yılında hizmete giren e-Devlet Kapısı, Türkiye'nin dijitalleşme tarihinin en büyük adımı olarak değerlendirilebilir. Kamu hizmetlerinin daha hızlı, etkin, şeffaf, güvenli ve kesintisiz bir şekilde vatandaşlara ulaştırılması amacıyla yapılan çalışmalar sonucu hizmete giren e-Devlet Kapısı ilk olarak 22 kamu hizmetiyle kullanıma açılmış ve zaman içerisinde sadece kamu kurumları değil aynı zamanda elektrik, doğalgaz ve su dağıtım hizmeti veren özel kuruluşlar ve telekomünikasyon hizmet sağlayıcıları gibi farklı sektörlerden birçok kuruluşun hizmet ağlarını e-Devlet sistemine entegre etmesiyle bugün 194 merkezi kamu kurumu, 201 üniversite, 438 belediye, 30 su ve kanalizasyon idaresi ve 126 özel kurumun toplamda 7.225 hizmet verdiği bir merkezi kamu hizmeti portalı haline dönüşmüştür. 2023 yılı itibariyle e-Devlet sistemi toplamda 63.651.479 kullanıcı sayısına ulaşmıştır.[17] (e-Devlet Kapısı, 2023).

e-Devlet Kapısı üzerinden verilen kamu hizmetleri, vatandaşların daha önce almak istedikleri hizmetler için ilgili kamu kurumuna bireysel başvuru yapmaları zorunluluğunu ortadan kaldırdığı gibi kağıt ve yazışma üzerine kurulu bürokrasiyi büyük oranda dijitalleştirerek devlet için oldukça büyük bir gider kalemi olan kırtasiyeciliğin de büyük oranda azalmasına ve tasarruf sağlanmasına olanak sağlamıştır. Eğitim, sağlık, konsolosluk hizmetleri, vergi ödemeleri, bankacılık işlemleri, araç ruhsat ve tapu işlemleri, sosyal güvenlik ve emeklilik işlemleri, seçimlerde yapılan seçmen kayıt işlemleri, dava dosyalarının sorgulanması, abonelik işlemleri ve ceza ödemeleri gibi birçok alanda hizmet veren e-Devlet Kapısı, Türkiye'de kamu yönetiminin dijitalleşmesinde büyük rol oynamıştır.

[17] e-Devlet Kapısı ile ilgili daha detaylı istatistikler için bkz. https://www.turkiye.gov.tr/edevlet-istatistikleri

1.3. Cumhurbaşkanlığı Dijital Dönüşüm Ofisi (CBDDO)

Türkiye'de dijital dönüşümün tek bir çatı altında toplanarak koordine edilmesi, siber güvenlik, milli teknolojiler, büyük veri ve yapay zekâ alanlarında yapılacak çalışmaların tek elden yönetilmesi amacıyla 2018 tarihinde yayımlanan "1 Sayılı Cumhurbaşkanlığı Teşkilatı Hakkında Cumhurbaşkanlığı Kararnamesi" ile kurulan T.C. Cumhurbaşkanlığı Dijital Dönüşüm Ofisi, "Dijital Türkiye" sloganıyla Türkiye'de dijitalleşme sürecine liderlik etmektedir. Kurum çatısı altında "Dijital Dönüşüm Koordinasyon Dairesi Başkanlığı, Dijital Teknolojiler, Tedarik ve Kaynak Yönetimi Dairesi Başkanlığı, Dijital Uzmanlık, İzleme ve Değerlendirme Dairesi Başkanlığı, Siber Güvenlik Dairesi Başkanlığı, Büyük Veri ve Yapay Zekâ Uygulamaları Dairesi Başkanlığı, Uluslararası İlişkiler Dairesi Başkanlığı, Bilgi Teknolojileri Dairesi Başkanlığı, Yönetim Hizmetleri Dairesi Başkanlığı ve Hukuk Müşavirliği" hizmet birimleri kurulmuştur (Resmi Gazete, 2018). Kararname kapsamında e-Devlet Kapısı'nın işletilmesi ve yönetilmesi görev ve sorumluluğu da CBDDO'ya verilmiştir.

CBDDO kurulduğu günden bu yana Türkiye'de dijitalleşme ile ilgili olarak birçok proje başlatmıştır. Projeler kapsamında ilgili kurum ve kuruluşların koordinasyonunu gerçekleştiren CBDDO, özellikle siber güvenlik, yapay zekâ, e-Devlet uygulamalarının tek bir merkezden yönetilmesi ve KamuNet Projesi alanlarında çalışmalar yürütmektedir. Bu bağlamda "Yerli Siber Güvenlik Ürünlerinin Yaygınlaştırması Platformu, Dijital İnovasyon İş Birliği Platformu, Devlet Teşkilatı Merkezi Kayıt Sistemi (DETSİS), Siber Zekâ Bilgi Yarışması, Türk Beyin Projesi (TBP) ve e-Yazışma Projesi" gibi uygulamalar hayata geçirilerek uygulanmaya konulmuştur (CBDDO, 2023).

2. TÜRKİYE'DE SİBER UZAYIN DÜZENLENMESİ ADINA YAPILAN YASAL DÜZENLEMELER

Türkiye'de siber uzayın düzenlenmesi adına yapılan tek bir düzenleme ya da bu alanın güvenliğinin sağlanması ile ilgili olarak çıkartılan tek bir kanun yoktur. Siber uzayda bilişim alanında işlenen suçların düzenlenmesi mevcut kanunlara ilgili

hükümlerin eklenmesiyle gerçekleştirilmiştir (BTK, 2017). Bu bağlamda özellikle TCK başta olmak üzere birçok diğer mevut kanunda yapılan düzenlemelerle siber uzayın güvenliğinin yasal boyutta düzenlenmesi sağlanmaya çalışılmaktadır. Sürekli değişen ve gelişen bir alan olması nedeniyle yapılan bu yasal düzenlemeler her ne kadar bu değişimi yakalama çabası içerisinde olsa da gerek uygulamada gerekse de bu alanın doğal yapısı nedeniyle yaşanan sorunlar siber uzayda işlenen suçların önlenmesi noktasında oldukça büyük zorlukları ortaya çıkartmaktadır.

2.1. Türk Ceza Kanunu'nda (TCK) Siber Uzayda İşlenen Suçların Düzenlenmesi

1990'lı yılların başından itibaren siber uzayın ve bu alanın güvenliğinin sağlanması konusunun farkında olan Türkiye, her ne kadar bu anlamda ilk düzenlemelerin yapıldığı yıllarda bu alanın kullanımı noktasında yolun oldukça başında olsa da TCK'da 1991 yılında siber uzayda işlenen suçlara dair yapılan ilk düzenleme sonraki yıllarda bu alanın güvenliği bağlamında farkındalığın oluşmasında atılan ilk adım olarak önemli bir gelişmedir. Türkiye, siber uzay ile ilgili olarak ilk defa 6 Haziran 1991 tarihinde 3756 Sayılı "Türk Ceza Kanunu'nun Bazı Maddelerinin Değiştirilmesine Dair Kanun" ile siber uzayda işlenen suçlar bağlamında bir düzenlemeye gitmiştir. Bu kanunun 20. maddesinde "Bilişim Alanında Suçlar" başlığı altında bilgileri otomatik işleme tabi tutulmuş bir sistemden programların, verilerin veya diğer unsurların hukuka aykırı olarak ele geçirilmesi veya bunların başkasına zarar vermek üzere kullanılması, nakledilmesi veya çoğaltılması yasayla ceza unsuru olarak kabul edilmiş ve bu cezanın hükümleri düzenlenmiştir (Resmî Gazete, 1991).

3756 Sayılı Kanun'un 20. maddesine göre 765 sayılı TCK'ya 525'inci maddeden sonra gelmek üzere "Bilişim Alanında Suçlar" başlığı altında "Onbirinci Bab" eklenmiştir. Yine aynı kanunun 21, 22, 23, ve 24. maddeleriyle Onbirinci Bab başlığından sonra eklenen 525a, 525b, 525c ve 525d maddeleri TCK'ya eklenmiştir. Bu maddeler içerikleri ve siber uzayın güvenliğinin sağlanması bağlamında yapılan ilk değişiklikler olması bakımından oldukça önemlidir. Bu nedenle bu maddeler aşağıda kanunda belirtildiği şekliyle şu şekilde düzenlenmiştir:

- **Madde 525 a:**

"*Bilgileri otomatik olarak işleme tabi tutmuş bir sistemden, programları, verileri veya diğer herhangi bir unsuru hukuka aykırı olarak ele geçiren kimseye bir yıldan üç yıla kadar hapis ve birmilyon liradan onbeşmilyon liraya kadar ağır para cezası verilir.*

Bilgileri otomatik işleme tabi tutmuş bir sistemde yer alan bir programı, verileri veya diğer herhangi bir unsuru başkasına zarar vermek üzere kullanan, nakleden veya çoğaltan kimseye de yukarıdaki fıkrada yazılı ceza verilir." (Resmî Gazete, 3756 Sayılı Kanun, 1991: Madde 21).

- **Madde 525 b:**

"*Başkasına zarar vermek veya kendisine veya başkasına yarar sağlamak maksadıyla, bilgileri otomatik işleme tabi tutmuş bir sistemi veya verileri veya diğer herhangi bir unsuru kısmen veya tamamen tahrip eden veya değiştiren veya silen veya sistemin işlemesine engel olan veya yanlış biçimde işlemesini sağlayan kimseye iki yıldan altı yıla kadar hapis ve beşmilyon liradan ellimilyon liraya kadar ağır para cezası verilir.*

Bilgileri otomatik işleme tabi tutmuş bir sistemi kullanarak kendisi veya başkası lehine hukuka aykırı yarar sağlayan kimseye bir yıldan beş yıla kadar hapis ve ikimilyon liradan yirmimilyon liraya kadar ağır para cezası verilir." (Resmî Gazete, 3756 Sayılı Kanun, 1991: Madde 22).

- **Madde 525 c:**

"*Hukuk alanında delil olarak kullanılmak maksadıyla sahte bir belgeyi oluşturmak için bilgileri otomatik olarak işleme tabi tutan bir sisteme, verileri veya diğer unsurları yerleştiren veya var olan verileri, diğer unsurları tahrif eden kimseye bir yıldan üç yıla kadar, tahrif edilmiş olanları bilerek kullananlara altı aydan iki yıla kadar hapis cezası verilir.*" (Resmî Gazete, 3756 Sayılı Kanun, 1991: Madde 23).

- **Madde 525 d:**

"*525 a ve 525 b maddeleri hükümlerini ihlal eden kişiler hakkında, maddelerde yazılı cezalara ek olarak, meslek icrası sırasında veya icrası dolayısıyla suçun işlendiği bir kamu hizmetinden veya meslek veya sanat veya ticaretten altı aydan üç yıla kadar yasaklanma cezası da verilir.*" (Resmî Gazete, 3756 Sayılı Kanun, 1991: Madde 24).

3756 sayılı kanun ile TCK'da yapılan değişiklikler 1993 yılında Türkiye'nin Orta Doğu Teknik Üniversitesi'nin (ODTÜ) yaptığı girişimlerle internetle tanışmasıyla daha da anlam kazanmıştır. Kanunun çıkartıldığı 1991 yılında Türkiye'nin genelinde bireysel olarak bilgisayar kullanımının oldukça düşük olduğunu söylemek mümkündür. Henüz internet denilen teknolojinin kullanılmaya

başlanmadığı bir tarihte böyle bir yasal düzenleme ile siber uzayda işlenecek suçlara karşı bir caydırıcılığın ortaya çıkartılması oldukça önemli bir gelişme olarak değerlendirilmelidir. Ayrıca burada belirtilmesi gereken bir diğer husus ise yapılan bu düzenlemenin kanunilik ilkesi kapsamında oldukça önemli olduğudur. Kanunilik ilkesi ilk defa Alman ceza hukukçusu Anselmo Feuerbach tarafından "*kanunsuz suç ve ceza olmaz"* şeklinde *"nullum crimen, nulla poena sine lege"* olarak latince ortaya konulmuştur (Eşitli, 2013: 230). Suç ve cezaların kanuniliği ilkesi ülkemizde ise 1982 Anayasası'nın 13. maddesi ile güvence altına alınmıştır. Bu maddeye göre *"temel hak ve hürriyetler, özlerine dokunulmaksızın yalnızca Anayasanın ilgili maddelerinde belirtilen sebeplere bağlı olarak ve ancak kanunla sınırlanabilir. Bu sınırlamalar, Anayasanın sözüne ve ruhuna, demokratik toplum düzeninin ve lâik Cumhuriyetin gereklerine ve ölçülülük ilkesine aykırı olamaz"* (T.C. Anayasası, md. 13) şeklinde yapılan düzenleme kanunilik ilkesinin anayasada vücut bulmuş halidir. Yine aynı şekilde Anayasa'nın "Suç ve Cezalara İlişkin Esaslar" başlıklı 38. maddesinde ise

> "*kimse, işlendiği zaman yürürlükte bulunan kanunun suç saymadığı bir fiilden dolayı cezalandırılamaz; kimseye suçu işlediği zaman kanunda o suç için konulmuş olan cezadan daha ağır bir ceza verilemez. Suç ve ceza zamanaşımı ile ceza mahkûmiyetinin sonuçları konusunda da yukarıdaki fıkra uygulanır. Ceza ve ceza yerine geçen güvenlik tedbirleri ancak kanunla konulur"* (T.C. Anayasası, md. 38)

şeklinde yapılan düzenleme ile suçların ve cezaların kanuniliği ilkesi garanti altına alınmıştır. Dolayısıyla aslında TCK'da 1991 yılında yapılan düzenleme siber uzayda ortaya çıkacak olan bir suçun hukuki olarak bir suç sayılabilmesinin ve bu eylemle ilgili soruşturma ve kovuşturma süreçlerinin başlatılabilmesinin de önünü açmıştır.

Kanunda "bilgisayar" ya da "bilişim" gibi terimler yerine "bilgileri otomatik olarak işleme tabi tutmuş bir sistem" tanımlaması kullanılmıştır. Henüz bilgisayar ve yazılım teknolojisinin yaygın olarak kullanımının başlamamış olduğu düşünüldüğünde yapılan bu tanım ile en basit bilgi işletim sisteminden dönemin en teknolojik bilgisayarlarına kadar tüm teknolojik makineleri kapsayacak bir tanımlamaya gidildiği ve bu cihazlar aracılığıyla ya da bu cihazları kullanarak işlenecek bir suçun maddi olarak bir karşılığının belirlendiği yapılan bu düzenlemeyle kanunlaşmıştır.

Bilgisayar kullanımının Türkiye'de henüz oldukça yeni sayılabileceği bir dönemde yapılan bu düzenlemenin gerçekleştiği yıllarda siber güvenlik bağlamında tehditlerin oldukça sınırlı olduğu bir gerçektir. Dolayısıyla yapılan düzenlemede suçun niteliği bağlamında herhangi bir tanım yapılmamıştır. Özellikle internet kullanımının hayatımıza girmesiyle birlikte anlam kazanan siber uzayda işlenen suçlar kavramının yasal bir zeminde yer bulmasını sağlayan bu düzenleme ile Türkiye'nin önemli bir adım attığını söylemek mümkündür.

2004 yılında 5252 sayılı "Türk Ceza Kanunun Yürürlük ve Uygulama Şekli Hakkında Kanun" ile yürürlükten kalkan 765 sayılı TCK yerini 5237 sayılı TCK'ya bırakmıştır. Yenilenen TCK'da ise 1991 yılında yapılan düzenlemeden çok daha kapsamlı bir şekilde siber uzayda işlenen suçlar ele alınmıştır. "Bilişim Alanında Suçlar" başlığıyla 5237 sayılı Türk Ceza Kanunun (TCK) onuncu bölümünde bilişim sistemine girme, sistemi engelleme, bozma, verileri yok etme veya değiştirme ile banka ve kredi kartlarının kötüye kullanılması konularında düzenleme yapılmıştır (Bıçakçı vd., 2016: 30). Bahsi geçen bu düzenlemeler TCK'nın 243, 244 ve 245'inci maddelerinde bağımsız olarak düzenlenmiştir (5237 Sayılı TCK, 2004).

TCK'nın 243. Maddesi, bilişim sistemine girme suçunu düzenlemiştir. Bu madde uyarınca bir bilişim sisteminin bütününe ya da bir kısmına hukuka aykırı olarak giren kişiler hakkında bir yıla kadar hapis ya da adli para cezası uygulanması hükme bağlanmıştır. Yine aynı maddenin ikinci fıkrasında ise birinci fıkrada tanımlanan eylemlerin bedeli karşılığı yararlanılabilen sistemler hakkında işlenmesi halinde verilecek ceza yarı oranında indirilir denilmiştir. Son olarak üçüncü fıkrada ise bu eylem nedeniyle sistemin içerdiği verilerin yok olması ya da değişmesi durumunda altı aydan iki yıla kadar hapis cezası öngörülmüştür (5237 sayılı TCK, Md. 243).

TCK'nın 244. Maddesi ise sistemi engelleme, bozma verileri yok etme veya değiştirme suçlarını ele almıştır. Bu madde 243. Maddeye kıyasla daha detaylı bir şekilde bir bilişim sistemini engelleme suçunu işlemiştir. Türk Ceza Kanunu'nun 244. maddesinde,

> *"(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 fiille bir banka veya kredi kurumuna ya da bir kamu kurum veya kuruluşun 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 aya kadar hapis ve beş bin güne kadar adli para cezasına hükmolunur." (5237 sayılı TCK, Md. 244)

hükümleri ile sistemi engelleme, bozma, verileri yok etme veya değiştirme suçu düzenlenmiştir. Bu suç tipinin düzenlenmesindeki amaç ise Budapeşte Sözleşmesinin 4. Maddesinde öngörülen "verilere müdahale" ve 5. maddesinde öngörülen "sistemlere müdahale" düzenlemelerine uyum sağlamaktır.

TCK'nın 245. Maddesine bakıldığında ise banka veya kredi kartlarının kötüye kullanılması suçunun düzenlendiği görülmektedir. Bu maddeye göre banka ve kredi kartlarının kötüye kullanılması eylemleri bağımsız bir suç tipi olarak düzenlenmekle beraber bu yolla bankaların veya bu bankaların müşterilerinin zarara sokulmasının ve çıkar sağlanmasının engellenmesi amaçlanmıştır. Yine bu maddeye göre bir başkasına ait olan banka veya kredi kartını kart sahibinin ya da kartın kendisine verilmesi gereken kişinin rızası olmadan bunu kullanarak fayda sağlaması halinde üç yıldan altı yıla kadar hapis ve beş bin güne kadar adli para cezası ile cezalandırılır hükmü yer almaktadır. Sahte banka hesapları kullanarak kredi kartı üreten, satan, devreden, satın alana veya kabul eden kişilere ise üç yıldan yedi yıla kadar hapis ve on bin güne kadar adli para cezası öngörülmüştür. Yine maddenin üçüncü fıkrasında ise sahte olan bir banka veya kredi kartının kullanılarak fayda elde edilmesi durumunda bu fiilin daha ağır bir cezayı gerektiren başka bir suç oluşturmaması durumunda ise dört yıldan sekiz yıla kadar hapis ve beş bin güne kadar adli para cezası öngörülmüştür (5237 sayılı TCK, Md. 245).

2016 yılında yapılan düzenleme ile bu bölüme eklenen 245/A "Yasak cihaz ve programlar" maddesiyle beraber Bilişim Alanında Suçlar bölümünde düzenlenen suçların işlenmesinde kullanılan cihaz ve programların kullanımı ve üretimi ile ilgili olarak önemli bir düzenleme yapılmıştır. Bu maddeye göre;

"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." (5237 sayılı TCK, Madde 245/A)

şeklinde bir düzenleme yapılarak bilişim alanında işlenen suçlarda gerekli olan donanımsal ve yazılımsal cihazların suç unsuru oluşturacak şekilde kullanımı ve üretimi konusunda cezai müeyyide belirlenmiştir.

2001 yılında Budapeşte'de imzalanan Avrupa Siber Suçlar Sözleşmesi'ne Türkiye Büyük Millet Meclisi'nin (TBMM) 2012 yılında onaylamasıyla bu sözleşmeye taraf olan Türkiye, TCK'da bu sözleşmenin hükümlerine uygun olarak düzenlemelere gitmiştir. Budapeşte Sözleşmesi Türkiye'de siber alanda işlenen suçların yasal zeminde yer bulması ve maddi anlamda cezaların belirlenmesi adına oldukça önemlidir. Siber uzayda caydırıcılık konusu kısmında daha önce de belirtildiği üzere Türk Ceza Kanunu'nda (TCK) siber suçların maddi ceza hukuku bağlamında düzenlenmesi ve ilgili maddeler sadece "Bilişim Alanında Suçlar" başlığı altında değildir. Bilişim alanında işlenen suçlara özgü düzenlemeler olarak kabul edilmese de TCK farklı konularda işlenen suçların bilişim teknolojileri kullanılarak veya bu teknolojiler aracılığıyla işlenmesini ele almıştır. Özellikle Budapeşte Sözleşmesi'nin yürürlüğe girmesi ve bu nedenle uluslararası bir sözleşmeden kaynaklanan yükümlülükler çerçevesinde iç hukukta uyum çalışmaları yapılmasını ortaya çıkartmış, geleneksel veya gerçek dünya suçlarının bilişim teknolojileri kullanılarak veya bu teknolojiler aracılığıyla da işlenebileceği gerçeği göz önünde bulundurularak ilgili maddelerde düzenlemeler yapılmıştır.

2.1.1. Türk Ceza Kanunu'nda Bilişim Teknolojileri Kullanarak veya Bu Teknolojiler Aracılığıyla İşlenen Suçlarla İlişkilendirilen ya da İlişkilendirilebilecek Maddeler

TCK'da siber uzayda işlenen suçlarla ilgili olarak bilişim suçları kapsamında yapılan 243, 244 ve 245. maddelere ek olarak bilişim teknolojileri kullanarak veya bu teknolojiler aracılığıyla işlenen suçlarla ilişkilendirilen ya da ilişkilendirilebilecek birçok madde vardır. Bu maddeler özellikle Budapeşte Sözleşmesi'nin imzalanmasından sonra yapılan düzenlemelerle TCK'nın bu sözleşmeye uyum sağlaması adına yapılmış değişiklikler olarak karşımıza çıkmaktadır. İlgili maddeler aşağıdaki gibi sıralanabilir:

Madde 123/A, Israrlı Takip (Ek:12/5/2022-7406/8 Md.): İlgili maddenin birinci fıkrasında,

> "*Israrlı bir şekilde; fiziken takip etmek ya da haberleşme ve iletişim araçlarını, bilişim sistemlerini veya üçüncü kişileri kullanarak temas kurmaya çalışmak suretiyle bir kimse üzerinde ciddi bir huzursuzluk oluşmasına ya da kendisinin veya yakınlarından birinin güvenliğinden endişe duymasına neden olan faile altı aydan iki yıla kadar hapis cezası verilir.*" (5237 sayılı TCK, Md. 123/A)

hükmü getirilmiştir. Yapılan bu düzenlemede ısrarlı takibin sadece fiziki anlamda değil aynı zamanda haberleşme ve iletişim araçlarını ve bilişim sistemlerini kullanarak temas kurmak suretiyle de yapılan takibin ele alınmış olması her ne kadar bilişim sistemlerini kullanarak yapılan takiple ilgili açık bir tanım verilmemiş olsa da siber uzayda gerçekleşecek ve kişilere huzursuzluk verecek ya da güvenlik endişesi doğuracak ısrarlı takip eylemini kapsar boyuttadır. Ayrıca bu maddenin 2022 yılında TCK'ya eklendiği göz önünde bulundurulduğunda bu durumun özellikle günümüzde bu tarz eylemlerin siber uzayda çoğunlukla gerçekleştiğini gösterir nitelikte olduğuna dair bir değerlendirme yapılabilir.

Madde 124, Haberleşmenin Engellenmesi: Bu maddede bilişim teknolojileri ya da siber uzayla ilgili herhangi bir hüküm ya da açıklama bulunmamaktadır. Buna ek olarak bu suçun nasıl veya hangi araçlarla yapılabileceğine dair de bir açıklama mevcut değildir. Lakin ilgili madde haberleşmenin engellenmesi suçunun karşılığını şu şekilde düzenlemiştir:

> *"(1) Kişiler arasındaki haberleşmenin hukuka aykırı olarak engellenmesi halinde, altı aydan iki yıla kadar hapis veya adlî para cezasına hükmolunur. (2) Kamu kurumları arasındaki haberleşmeyi hukuka aykırı olarak engelleyen kişi, bir yıldan beş yıla kadar hapis cezası ile cezalandırılır. (3) Her türlü basın ve yayın organının yayınının hukuka aykırı bir şekilde engellenmesi halinde, ikinci fıkra hükmüne göre cezaya hükmolunur."* (5237 sayılı TCK, Md. 124)

Günümüzde internet teknolojisinin geldiği boyut bağlamında düşünüldüğünde bu tarz bir engellemenin en kolay şekilde siber uzayın getirdiği teknolojilerin kullanılarak gerçekleştirilebileceğini değerlendirmek gerekmektedir. Özellikle artık birçok kişinin haberleşme aracı olarak internet teknolojisinin kullanmasına ek olarak basın ve yayın organlarının yayınlarının artık sanal ortamda yapıldığı ve geleneksel anlamda yayıncılığın oldukça düşük seviyelere geldiği düşünüldüğünde TCK'nın ilgili maddesinin doğrudan siber uzayın güvenliği ile alakalı olduğu söylenebilir.

TCK'nın dokuzuncu bölümü olan "Özel Hayata ve Hayatın Gizli Alanına Karşı Suçlar" başlıklı kısmında yapılan düzenlemeler özel hayatın gizliliğinin ihlal edilmesi suçlarının özellikle bilişim teknolojileri kullanılarak gerçekleştirilmesi durumlarını ele alarak cezai müeyyideleri belirlemiştir. Bu kısımda yer alan 132-140. maddeler aşağıdaki gibi düzenlenmiştir:

Madde 132, Haberleşmenin Gizliliğini İhlal: Bu maddede kişiler arasındaki haberleşmenin gizliliğinin ihlal edilmesi, haberleşme içeriklerinin kaydı, bu içeriklerin hukuka aykırı bir şekilde ifşa edilmesi, kişinin kendisiyle yapılan haberleşmelerin hukuka aykırı bir şekilde ifşa edilmesi durumunda uygulanacak cezai müeyyideler belirlenmiştir. İlgili madde;

> "*1) Kişiler arasındaki haberleşmenin gizliliğini ihlal eden kimse, bir yıldan üç yıla kadar hapis cezası ile cezalandırılır. Bu gizlilik ihlali haberleşme içeriklerinin kaydı suretiyle gerçekleşirse, verilecek ceza bir kat artırılır. (2) Kişiler arasındaki haberleşme içeriklerini hukuka aykırı olarak ifşa eden kimse, iki yıldan beş yıla kadar hapis cezası ile cezalandırılır. (3) Kendisiyle yapılan haberleşmelerin içeriğini diğer tarafın rızası olmaksızın hukuka aykırı olarak alenen ifşa eden kişi, bir yıldan üç yıla kadar hapis cezası ile cezalandırılır. İfşa edilen bu verilerin basın ve yayın yoluyla yayımlanması halinde de aynı cezaya hükmolunur."* (5237 sayılı TCK, Md.132)

fıkralarıyla kişiler arasındaki haberleşmenin gizliliğinin ihlal edilmesi suçunu düzenlemiştir. Akıllı telefon kullanımının ve internet teknolojisinin günümüzde eriştiği seviye ile bireyler arasındaki iletişimin en temel aracını internet üzerinden kullanılan mesajlaşma ve görüntülü konuşma uygulamaları olduğu gerçeği oldukça açıktır. Özellikle Covid19 pandemisi döneminde sokağa çıkma kısıtlamaları ile evlerinden çıkamayan insanların en önemli iletişim aracı haline gelen internet teknolojisi geleneksel iletişim yöntemlerinin unutulmasına neden olmuştur. Bu kapsamda değerlendirildiğinde TCK'nın ilgili maddesinin siber uzayda ortaya çıkacak haberleşmenin gizliliğinin ihlal edilmesi suçu ile doğrudan alakalı olduğu görülmektedir.

Madde 133, Kişiler Arasındaki Konuşmaların Dinlenmesi ve Kayda Alınması: İlgili maddede diğer maddeler için de belirtildiği üzere bilişim teknolojileri kullanarak ya da bunlar aracılığıyla bu eylemin gerçekleştirilmesi durumu ele alınmamış olsa da günümüzde bu eylemlerin gerçekleştirildiği ya da gerçekleştirilebileceği mecra siber uzaydır. Özellikle iletişim aracı olarak internet teknolojisinin yoğunlukla kullanıldığı

günümüzde kişiler arasındaki konuşmaların dinlenmesi, kayıt altına alınması ve ifşa edilmesi yine internet teknolojisi aracılığıyla gerçekleştirilen bir suç olarak karşımıza çıkmaktadır. İlgili madde;

> *"(1) Kişiler arasındaki aleni olmayan konuşmaları, taraflardan herhangi birinin rızası olmaksızın bir aletle dinleyen veya bunları bir ses alma cihazı ile kaydeden kişi, iki yıldan beş yıla kadar hapis cezası ile cezalandırılır. (2) Katıldığı aleni olmayan bir söyleşiyi, diğer konuşanların rızası olmadan ses alma cihazı ile kayda alan kişi, altı aydan iki yıla kadar hapis veya adlî para cezası ile cezalandırılır. (3) Kişiler arasındaki aleni olmayan konuşmaların kaydedilmesi suretiyle elde edilen verileri hukuka aykırı olarak ifşa eden kişi, iki yıldan beş yıla kadar hapis ve dörtbin güne kadar adlî para cezası ile cezalandırılır. İfşa edilen bu verilerin basın ve yayın yoluyla yayımlanması halinde de aynı cezaya hükmolunur."* (5237 sayılı TCK, Md. 133)

Artık hemen herkesin kullandığı ve sürekli yanında bulundurduğu akıllı telefonlar sadece bir iletişim cihazı görevi görmemekte aynı zamanda bir ses ve görüntü kayıt cihazı olarak da kullanılabilmektedir. Ayrıca siber uzayda ortaya çıkan tehditler bölümünde de bahsedildiği üzere yasa dışı bir şekilde bir ağa sızarak dinleme ve kayıt yapılması artık oldukça muhtemel bir durum olarak karşımıza çıkmaktadır. Bu bağlamda TCK'nın ilgili maddesinin doğrudan siber güvenlik tehditleri ile alakalı olduğu söylenebilir.

Madde 134, Özel Hayatın Gizliliğini İhlal: TCK'nın ilgili maddesinde kişilerin özel hayatının gizliliğinin ihlal edilmesi ve bu ihlalin görüntü veya seslerin kayda alınması suretiyle gerçekleştirilmesi, bu görüntü veya seslerin hukuka aykırı bir şekilde ifşa edilmesi düzenlenmiştir. Yapılan düzenlemede "*gizliliğin görüntü veya seslerin kayda alınması suretiyle ihlal edilmesi"* şeklinde bir açıklama yapılmıştır. Dolayısıyla ihlalin bilişim teknolojileriyle ya da aracılığıyla yapılması durumu veya hangi mecralarda gerçekleştiği konusu ele alınmamıştır. Fakat bu durumun spesifik olarak ele alınmamış olması bu suçun siber ortamda işlenmesiyle ortaya çıkan suç unsuruna uygulanamayacağı anlamına gelmemektedir ve bunun önünde de herhangi bir engel yoktur. İlgili madde,

> *"1) Kişilerin özel hayatının gizliliğini ihlal eden kimse, bir yıldan üç yıla kadar hapis cezası ile cezalandırılır. Gizliliğin görüntü veya seslerin kayda alınması suretiyle ihlal edilmesi halinde, verilecek ceza bir kat artırılır. (2) Kişilerin özel hayatına ilişkin görüntü veya sesleri hukuka aykırı olarak ifşa eden kimse iki yıldan beş yıla kadar hapis cezası ile cezalandırılır. İfşa edilen bu verilerin basın ve yayın yoluyla yayımlanması halinde de aynı cezaya hükmolunur."* (5237 sayılı TCK, Md. 134)

şeklinde özel hayatın gizliliğinin ihlali suçunu düzenlemiştir. Her türlü kişisel bilgi ve verinin artık dijital ortamlarda muhafaza edildiği günümüzde verilerin saklandığı bir cihaza yapılacak bir siber saldırı ile bu bilgiler ele geçirilebilir ve siber uzayda oldukça kısa bir süre içerisinde oldukça geniş kitlelere ulaşacak şekilde ifşa edilebilir.

Madde 135, Kişisel Verilerin Kaydedilmesi: TCK'nın bu maddesinde kişisel verilerin hukuka aykırı bir şekilde kaydedilmesi suçu düzenlenmiştir. 135. maddeye göre;

> *"(1) Hukuka aykırı olarak kişisel verileri kaydeden kimseye bir yıldan üç yıla kadar hapis cezası verilir. (2) Kişisel verinin, kişilerin siyasi, felsefi veya dini görüşlerine, ırki kökenlerine; hukuka aykırı olarak ahlaki eğilimlerine, cinsel yaşamlarına, sağlık durumlarına veya sendikal bağlantılarına ilişkin olması durumunda birinci fıkra uyarınca verilecek ceza yarı oranında artırılır."* (5237 sayılı TCK, Md. 135)

düzenlemesi yapılmıştır. İlgili maddede bahsi geçen eylemlerin bilişim teknolojileri aracılığıyla işlenmiş olması ya da olmaması gibi bir ayrım yapılmamıştır. Lakin bütün devlet kurumlarından bireylere kadar her türlü bilginin artık dijital ortamlarda saklandığı göz önünde bulundurulduğunda günümüzde bu bilgilerin ele geçirileceği mecra siber uzayın bir parçası olan bilgisayarlar olacaktır. Dolayısıyla doğrudan siber uzayda bu suçun işlenmesi halinde uygulanacak ceza düzenlenmemiş olsa da bu maddenin siber uzayda gerçekleşen bir kişisel veri hırsızlığı suçuna uygulanmasının önünde bir engel yoktur.

Madde 136, Verileri Hukuka Aykırı Olarak Verme veya Ele Geçirme: İlgili maddede siber uzayın güvenliği ile ilişkilendirilebilecek diğer birçok maddede olduğu gibi bahsi geçen suç unsurunun bilişim cihazları kullanarak veya aracılığıyla işlenmesi durumu ele alınmamış ve bununla ilgili herhangi bir açıklama da getirilmemiştir. Bu madde kişisel verilerin hukuka aykırı bir şekilde ele geçirilmesi ve bir başkasına verilmesini şu şekilde düzenlemiştir:

> *"(1) Kişisel verileri, hukuka aykırı olarak bir başkasına veren, yayan veya ele geçiren kişi, iki yıldan dört yıla kadar hapis cezası ile cezalandırılır. (2) Suçun konusunun, Ceza Muhakemesi Kanununun 236'ncı maddesinin beşinci ve altıncı fıkraları uyarınca kayda alınan beyan ve görüntüler olması durumunda verilecek ceza bir kat artırılır."* (5237 sayılı TCK, Md. 136)

Görüldüğü üzere maddede bahsedilen suçun işlenmesinde kullanılan araçlar ya da hangi alanda işlendiğine dair herhangi bir düzenleme söz konusu değildir. Maddenin ikinci fıkrasında belirtilen ve 2019 yılında yapılan düzenlemeyle eklenen bu hükümde bahsi geçen Ceza Muhakemesi Kanununun (CMK) 236'ncı maddesinin beşinci ve altıncı fıkraları ise TCK'nın 103'üncü maddesinde düzenlenen "Çocukların Cinsel İstismarı" suçunun soruşturma evresinde mağdur çocukların beyan ve görüntülerinin kayda alınması ile ilgilidir (CMK, Madde 236). Dolayısıyla TCK'nın 136'ncı maddesinin ikici fıkrasında bahsi geçen beyan ve görüntüler bunlardır.

Madde 142/2-e, Nitelikli Hırsızlık: TCK'nın onuncu bölümü olan "Malvarlığına Karşı Suçlar" kısmında ele alınan hırsızlık suçu, hırsızlık ve nitelikli hırsızlık suçları olarak ikiye ayrılarak incelenmiştir. Nitelikli hırsızlık suçunu ele alan 142. maddenin ikinci kısmının "e" bendinde göre bu suçun bilişim sistemlerinin kullanılması suretiyle işlenmesi durumunda beş yıldan on yıla kadar hapis cezasına hükmolunur (5237 sayılı TCK, Madde 142/2-e). Emniyet Genel Müdürlüğü Siber Suçlarla Mücadele Daire Başkanlığı bir siber suç olarak nitelikli hırsızlık suçunu zararlı yazılımlar aracılığıyla bir sistemde bulunan ya da sistemler arasındaki veri akışı içerisinde bu verilerin mahsup olduğu kişinin izni olmadan ele geçirilmesi suçu olarak tanımlamıştır. Çevrimiçi oynanan oyunlarda bulunan oyun karakterlerinin çalınması, banka hesaplarının ele geçirilerek başka hesaplara para aktarımı yapılması suçları bu suça örnek olarak gösterilmiştir (EGM, 2019). TCK'nın bu maddesinde nitelikli hırsızlık suçunun spesifik olarak bilişim sistemlerinin kullanılması suretiyle işlenmesi durumunun ele alınması, bu suçun siber uzayda işlenmesini önleyici nitelikte bir düzenleme olarak değerlendirilebilir.

Madde 157 ve 158/1-f, Dolandırıcılık ve Nitelikli Dolandırıcılık: TCK'nın 157. maddesinde dolandırıcılık suçu *"Hileli davranışlarla bir kimseyi aldatıp, onun veya başkasının zararına olarak, kendisine veya başkasına bir yarar sağlayan kişiye bir yıldan beş yıla kadar hapis ve beş bin güne kadar adli para cezası verilir."* şeklinde ele alınmıştır (5237 sayılı TCK, Madde 157). 158. maddede ise "Nitelikli Dolandırıcılık" suçu dolandırıcılık suçunun işlenme şekillerine bağlı olarak kategorize edilmiştir. Bu maddenin birinci kısmının "f" bendinde ise dolandırıcılık suçunun "Bilişim sistemlerinin, banka veya kredi kurumlarının araç olarak kullanılması suretiyle" işlenmesi durumu ele alınmıştır (5237 sayılı TCK, Madde 158/1-f).

Günümüzde bankacılık işlemlerinin büyük bir kısmı, alışveriş ve kurum ödemeleri gibi birçok işlem internet üzerinden kişilerin kredi kartı bilgileriyle gerçekleştirilebilmektedir. Her ne kadar bu sistemlerin güvenliği bağlamında yazılımsal anlamda birçok önlem alınıyor olsa da bu durum suçlular için bulunmaz bir fırsata dönüşmüştür. Özellikle internet üzerinden yapılan alışverişlerde kişilerin kart bilgilerinin çeşitli yöntemlerle ele geçirilerek kazanç sağlanması ya da sahte alışveriş siteleri üzerinden ürün satışı yapılması oldukça yaygın bir hale gelmiştir. Bilişim sistemleri güvenliği alanında dünyanın önde gelen kuruluşlarından birisi olan Kaspersky'nin verilerine göre 2022 yılında kişilerin ödeme bilgilerinin ele geçirilmesi suretiyle siber uzayda işlenen suçların sayısı 2021 yılına kıyasla iki kat artarak 20 milyona ulaşmıştır (AA, 2022).

Madde 213-218, Kamu Barışına Karşı Suçlar: TCK'nın Kamu Barışına Karşı Suçlar kısmında ele alınan suçlar, her ne kadar siber uzayda ortaya çıkması ya da bilişim teknolojileri kullanarak veya aracılığıyla işlenmesi durumlarını ele almamış olsa da bu suçların dijital teknolojiler vasıtasıyla işlenmesi durumunda bahsi geçen maddelerin uygulanmasının önünde herhangi bir engel yoktur. İlgili maddeler: Madde 213- Halk arasında korku ve panik yaratmak amacıyla tehdit, Madde 214- Suç işlemeye tahrik, Madde 215- Suçu ve suçluyu övme, Madde 216- Halkı kin ve düşmanlığa tahrik veya aşağılama, Madde 217- Kanunlara uymamaya tahrik, -Madde 217/A- Halkı yanıltıcı bilgiyi alenen yayma.

Bahsi geçen maddelerde belirtilen suçlar geleneksel anlamda işlenen suçlar olarak değerlendirilmiş olsa da ilgili suçların her biri kolaylıkla dijital ortamda işlenebilen türden suçlardır. Ayrıca artık hemen herkesin kullanmış olduğu sosyal medya platformları bu tür suçların işlenmesine olanak sağlayacak dijital ortamların başında gelmektedir. Her bir bireyin şahsi olarak bir basın organıymış gibi hareket edebileceği bu platformlarda yapılan bir paylaşım dakikalar içerisinde oldukça büyük kitlelere ulaşabilmektedir. Dolayısıyla TCK'nın beşinci bölümünde ele alınan suçlar bu mecralarda oldukça kolay bir şekilde ortaya çıkabilmektedir. Bu bağlamda bu tarz suçların işlenmesi durumunda verilecek olan cezaların kanunen açık bir şekilde belirlenmiş olması bir caydırıcılık unsuru olarak değerlendirilebilir. Fakat siber uzayın karmaşık yapısı, genişliği ve sınırsızlığı bu tip suçların faillerinin yakalanmasını zorlaştırmaktadır.

Siber uzayın sınırsızlığı durumu bu tip suçların ülke sınırlarını aşan coğrafyalardan işlenebilmesine olanak sağlamaktadır. Dolayısıyla ceza kanunumuzda bu tip suçlarla ilgili düzenleme bulunuyor olması kimi zaman caydırıcılık noktasında herhangi bir işlev üretmemektedir. Bu bağlamda siber uzayın sınırları aşan boyutuyla ilgili olarak işlenen suçlarla mücadelede ve caydırıcılık unsurunun oluşturulmasında uluslararası iş birliği hayati önem taşımaktadır.

Madde 226, Müstehcenlik: TCK'da "Genel Ahlaka Karşı Suçlar" kısmında ele alınan müstehcenlik suçu, siber uzayın bu suçun işlenmesine olanak sağlayacak kolaylıkları nedeniyle bu suçun sanal mecralarda işlenmesi durumunda ortaya çıkacak cezai müeyyidenin belirlenmesi bağlamında oldukça önemlidir. Her ne kadar ilgili maddede bu suçun bilişim teknolojileri kullanarak ya da bu teknolojiler aracılığıyla işlenmesi durumu açıkça ele alınmamış olsa da ilgili maddede *"müstehcen görüntü, yazı veya sözleri içeren ürünlerin satışı, kiralanması, dağıtımı ya da basın yayın yoluyla yayınlanması veya bu duruma aracılık edilmesi"* durumu suç olarak belirlenmiş ve suçun işlenme şekline bağlı olarak altı aydan beş yıla kadar hapis cezası öngörülmüştür. TCK'nın ilgili maddesi Budapeşte Sözleşmesinin dokuzuncu maddesinde ele alınan "Çocuk Pornografisiyle Bağlantılı Suçlar" kapsamında değerlendirildiğinde ise önemi daha da artmaktadır. İlgili maddede "*müstehcen görüntülerin ya da materyallerin çocukların girebileceği ya da görebileceği yerlerde sergilenmesi, okunması, okutulması ve bu tür materyallerin çocuklara servis edilmesi"* durumu ele alınarak cezai müeyyideye bağlanmıştır. Daha da önemlisi bu tür materyallerin üretiminde çocukları, temsili çocuk görüntülerini veya çocuk gibi görünen kişileri kullanan kişilere beş yıldan on yıla kadar hapis ve beşbin güne kadar adli para cezası verilmesi öngörülmüştür.

Animasyon teknolojisinin günümüzde geldiği nokta düşünüldüğünde sanal ortamda üretilen ve çocuk gibi görünen kişilerin kullanıldığı müstehcenlik içeren görüntülerin kullanılmasının suç olarak belirlenmiş olması siber uzayda işlenecek bu tarz suçların engellenmesinde önemli bir unsur olarak değerlendirilebilmektedir. Sanal çocuk pornografisi konusunun kanunda açık bir şekilde suç tanımının yapılmaması büyük bir eksiklik olsa da bu düzenleme kapsamında işlenecek bir suçun hükme bağlanmasının önünde bir engel yoktur.

Madde 228, Kumar Oynanması İçin Yer ve İmkân Sağlama: İlgili maddede *"kumar oynanması için yer ve imkân sağlayan kişiler için bir yıldan üç yıla kadar hapis ve iki yüz günden aşağı olmamak üzere adli para cezası"* öngörülmektedir. Bilişim ve internet teknolojilerinin kullanımının artması ile kumar oynanması için gerekli olan ortam oldukça kolay bir şekilde sanal ortamda oluşturulabilmektedir. 2017 yılında ilgili maddeye yapılan ek ile bu suçun bilişim sistemlerinin kullanılması suretiyle işlenmesi halinde ise üç yıldan beş yıla kadar hapis ve bin günden onbin güne kadar adli para cezasına hükmedilmesi kanuna eklenmiştir. Lakin daha önce de üzerinde önemle durulan siber uzayın sınırsızlığı sorunsalı bu suçu işleyen kişilerin yakalanmasını oldukça zorlaştırmaktadır. Sunucularının yurt dışında bulunduğu internet siteleri üzerinden kumar oynanmasına imkân sağlayan kişilerin yakalanması ve yargılanması eğer uluslararası bir iş birliği söz konusu değilse mümkün değildir. Böyle bir durumda ilgili kurumların web sitesine olan erişimin yasaklanmasını sağlamak dışında yapabileceği bir şey yoktur. Dolayısıyla bu konuda her ne kadar mevzuatımızda düzenleme olsa da daha fazla uluslararası iş birliği gerekliliği görülmektedir.

Madde 209-301, Devletin Egemenlik Alametlerine ve Organlarının Saygınlığına Karşı Suçlar: TCK'nın bu bölümünde işlenen suçlar Cumhurbaşkanına hakaret (Md. 299), Devletin egemenlik alametlerini aşağılama (Md. 300) ve Türk Milletini, Türkiye Cumhuriyeti Devletini, Devletin kurum ve organlarını aşağılama (Md. 301) suçları olarak düzenlenmiştir. Bahsi geçen suçlarla alakalı bu suçların bilişim teknolojileri kullanılarak işlenmesi durumunda uygulanacak olan hüküm düzenlemesi yapılmamıştır. Lakin günümüzde bahsi geçen suçların siber uzayda farklı mecralarda, özellikle de sosyal medya platformlarında kolaylıkla işlenebileceği düşünüldüğünde bu suçların siber uzayda ortaya çıkması durumunda ilgili maddelerin uygulanmasının önünde bir engel yoktur.

Madde 326-339, Devlet Sırlarına Karşı Suçlar ve Casusluk: TCK'nın Devlet Sırlarına Karşı Suçlar ve Casusluk kısmı genel olarak devletin güvenliğine, iç veya dış siyasal yararlarına ilişkin ve gizli kalması gereken bilgi ve belgelerin temin edilmesi, tahrip edilmesi, bunlar üzerinde sahtecilik yapılması, bu bilgilerin açıklanması gibi konuları ele almıştır. Çağımızda artık bilginin büyük bir çoğunluğunun dijital ortamlarda muhafaza edildiği, kurumlar arasındaki iletişimin ve bilgi akışının büyük

bir kısmının internete bağlı ağlar aracılığıyla gerçekleştiği düşünüldüğünde bu tür bilgi ve belgelerin sanal ortamda ele geçirilmesi oldukça muhtemeldir. İlgili maddelerde belirtilen suçların siber uzayda oluşması ya da bilişim cihazları kullanılarak veya aracılığıyla işlenmesi durumuyla ilgili herhangi bir açıklama veya düzenleme yapılmamış olsa da günümüz bilgi çağında verilerin büyük kısmının bilgisayar ortamlarında saklandığı ve bu sistemlere yapılacak bir siber saldırıyla ele geçirilmesinin mümkün olduğu gerçeği ortadadır.

Detaylarıyla belirtildiği üzere TCK'da siber uzayda işlenen suçlar hakkında açık bir düzenleme "Bilişim Alanında İşlenen Suçlar" başlığı altında 243,244 ve 245'inci maddeler kapsamında düzenlemiştir. Bu maddelere ek olarak gerçek hayatta işlenen bazı suçların bilişim sistemleri kullanılarak veya aracılığıyla işlenmesi durumu da farklı maddelerde düzenlenmiştir. Ayrıca yukarıda belirtildiği üzere TCK'nın birçok maddesinde belirtilen suçlar için içeriğinde bilişim sistemleri kullanılarak veya aracılığıyla işlenmesi durumu açık bir şekilde ele alınmamış olsa da bu suçların siber uzayda bilişim sistemleri kullanılarak veya aracılığıyla işlenmesi olasılığının yüksek olduğu durumlar sebebiyle bu düzenlemelerin de siber uzayın güvenliği ile yakından ilgili olduğu değerlendirmesi yapılabilir.

TCK'da bilişim suçlarının işlenmesi durumunda uygulanacak olan hükümlerin niteliği bakımında uygulamada var olan kararların incelenmesi de faydalı olacaktır. Ancak bu hükümlerin uygulanmasında ve suçluların kanunda belirtilen cezaları almasında "Hükmün Açıklanmasının Geri Bırakılması (HAGB)" ya da "Etkin Pişmanlık Ceza İndirimi" gibi uygulamalar bilişim alanında işlenen suçların önüne geçilmesinde büyük bir eksiklik olarak değerlendirilmektedir.

Hükmün açıklanmasının geri bırakılması uygulaması CMK madde 231'de düzenlenmiştir. Buna göre ilgili maddenin 5'inci fıkrasında;

> "*Sanığa yüklenen suçtan dolayı yapılan yargılama sonunda hükmolunan ceza, iki yıl veya daha az süreli hapis veya adlî para cezası ise; mahkemece, hükmün açıklanmasının geri bırakılmasına karar verilebilir. Uzlaşmaya ilişkin hükümler saklıdır. Hükmün açıklanmasının geri bırakılması, kurulan hükmün sanık hakkında bir hukukî sonuç doğurmamasını ifade eder."* (CMK, Md. 231)

denilmektedir. Ayrıca aynı maddenin altıncı fıkrasında ise HAGB'na karar verilebilmesi için gerekli şartlar düzenlenmiştir. İlgili maddenin altıncı fıkrasına göre ise;

> *"Hükmün açıklanmasının geri bırakılmasına karar verilebilmesi için; a) Sanığın daha önce kasıtlı bir suçtan mahkûm olmamış bulunması, b) Mahkemece, sanığın kişilik özellikleri ile duruşmadaki tutum ve davranışları göz önünde bulundurularak yeniden suç işlemeyeceği hususunda kanaate varılması, c) Suçun islenmesiyle mağdurun veya kamunun uğradığı zararın, aynen iade, suçtan önceki hale getirme veya tazmin suretiyle tamamen giderilmesi gerekir. Sanığın kabul etmemesi halinde, hükmün açıklanmasının geri bırakılmasına karar verilmez."* (CMK, Md. 231)

denilmiştir. Bu bağlamda yapılan değerlendirmede Bilişim Sistemine Girme (5237 sayılı TCK, Md. 243), Sistemi Engelleme, Bozma, Verileri Yok Etme veya Değiştirme (5237 sayılı TCK, Md. 244), Banka veya Kredi Kartlarının Kötüye Kullanılması (5237 sayılı TCK, Md. 245) suçları için HAGB uygulanabilecektir.

TCK madde 245/5'e göre *"Birinci fıkra kapsamına giren fiillerle ilgili olarak bu Kanunun malvarlığına karşı suçlara ilişkin etkin pişmanlık hükümleri uygulanır."* denilmiştir. Dolayısıyla madde 245/1'de belirtilen,

> "*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 kullandırtarak kendisine veya başkasına yarar sağlarsa, üç yıldan altı yıla kadar hapis ve beşbin güne kadar adlî para cezası ile cezalandırılır."* (5237 sayılı TCK, Md. 245/1)

hükmüyle belirtilen suç kapsamında sanığın şartları yerine getirmesi halinde sanık hakkında TCK madde 168'de düzenlenen etkin pişmanlık hükümleri uygulanarak ceza indirimine gidilebilir. Bu bağlamda ortaya çıkan bilişim suçu nedeniyle zarara uğrayan kişinin zararı soruşturma aşamasında giderildiği takdirde verilecek cezanın 2/3'üne kadarı indirilebilir. Lakin bu durum kovuşturma aşamasında ortaya çıkarsa, yani dava açıldıktan sonra mağdurun zararı karşılanırsa verilecek cezanın 1/2'si indirilir (5237 sayılı TCK, Md. 168).

TCK'de siber uzayın güvenliği ile ilgili olarak yapılan düzenlemeler her ne kadar bu alanda işlenecek suçların önüne geçilmesi bağlamında bir caydırıcı unsur olarak değerlendirse de cezaların uygulanmasında mevcut olan etkin pişmanlık ceza indirimi ve HAGB uygulamaları bu alanda işlenen suçların yasal olarak önlenmesi

adına bir zayıflık oluşturmaktadır. Ayrıca bu durum kanunda belirtilen cezaların caydırıcı olmadığı sonucunu da doğurmaktadır.

2.2. 5651 Sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun

2007 yılında kabul edilerek kanunlaşan 5651 sayılı "İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun" siber uzayda işlenen suçlarla mücadele noktasında Türkiye'nin yaptığı en önemli yasal düzenlemelerden birisidir. Özellikle TCK'da düzenlenen bilişim suçları, gerçek hayatta işlenen suçların bilişim sistemleri kullanılarak işlenmesi ve bunlara ek olarak TCK'da belirtilen bazı suçların her ne kadar bilişim sistemleri kullanılarak işlenmesi durumu ele alınmamış olsa da suç ortaya çıktığında verilecek cezaların belirlenmesi noktasında tamamlayıcı bir unsur olarak kabul edilebilecek olan 5651 sayılı kanunun amaç ve kapsamı *"içerik 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 düzenlemektir."* (5651 Sayılı Kanun, 2007) olarak belirlenmiştir.

Siber uzayı oluşturan en önemli bileşen olan internetin yasal olarak düzenlenmesi bağlamında oldukça önemli olan 5651 sayılı Kanun, yürürlüğe girdiği tarihten günümüze 2014, 2015, 2016, 2020 ve 2022 yıllarında yapılan değişiklikler ve eklenen maddelerle birlikte son halini almıştır. Ayrıca Anayasa Mahkemesi'nin (AYM) 2014 ve 2015 yıllarında bu kanunun bazı maddeleri ile ilgili olarak almış olduğu iptal kararları kanunun son halini almasında önemli rol oynamıştır. 2020 yılında 7253 sayılı "İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanunda Değişiklik Yapılmasına Dair Kanun" ve 2022 yılında 7418 sayılı "Basın Kanunu ile Bazı Kanunlarda Değişiklik Yapılmasına Dair Kanun" ile yapılan değişiklikler kamuoyunda geniş yer bulmuş ve bazı tartışmaları da beraberinde getirmiştir. 2020 yılında yapılan değişiklik kamuoyunda "*Sosyal Medya Düzenlemesi*" (Oymak, 2020:

1) olarak anılmış ve 2022 yılında yapılan değişiklik ise "*Dezenformasyon Yasası*" ya da "*Sansür Yasası*" (BBC, 2022) olarak kamuoyunda yer bulmuştur.

İnternet kullanımının oldukça yaygınlaşması ve özellikle sosyal medya platformlarının hemen herkes tarafından kullanılır hale gelmesiyle birlikte internet ortamının yasal olarak düzenlenmesi bir mecburiyet haline dönüşmüştür. Özellikle sosyal medya platformlarının kullanım sayılarının milyonları aşması ve insanların en önemli iletişim araçları arasına girmesi ve bu platformların bir haber kaynağı görevi görmeye başlamasıyla yeni bir toplumsal yapının oluştuğu bu ortamın yasal ve yönetsel olarak düzenlenmesini gerekli kılmıştır. 5651 sayılı Kanun sadece internet ortamında yapılan yayınları düzenlemekle kalmamış, aynı zamanda kullanıcı sayısı milyonlara ulaşan sosyal medya platformlarına da önemli yasal yükümlülük ve sorumlulukları beraberinde getirmiştir. Tüm bunlara ek olarak internet ortamında sıklıkla kullanılan "erişim, erişim sağlayıcı, içerik sağlayıcı, internet ortamı, izleme, veri, yayın vb." gibi bazı terimlerin yasal olarak tanımlarının bulunmaması eksikliği bu kanunla giderilmeye çalışılmıştır. Temel hak ve özgürlükler kapsamında ifade ve düşünce özgürlüğü bağlamında oldukça önemli olan Kanun, sosyal medya platformlarına getirdiği yükümlülükler, erişimin engellenmesi ve bazı içeriklerin yayından kaldırılması noktasında internette sansür tartışmalarını da ortaya çıkartmıştır.

Kanun kapsamında yapılan tanımlar, bu kanunun beraberinde getirdiği yükümlülük ve sorumlulukların anlaşılması bakımından oldukça önemlidir. Oldukça karmaşık bir yapısı bulunan internetin yasal olarak düzenlenmesinde hangi sorumlulukların kimlere yüklendiğinin ve bu bağlamda beraberinde getirdiği yükümlülüklerin anlaşılması adına bu tanımlamalar açıklayıcı bir nitelik göstermektedir. 5651 sayılı kanunun ilk kısmında yapılan bazı tanımlar aşağıdaki gibidir:

- Bilgi: Verilerin anlam kazanmış biçimi (5651 Sayılı Kanun, Md. 2/ç).
- Erişim: Bir internet ortamına bağlanarak kullanım olanağı kazanılması (5651 Sayılı Kanun, Md. 2/d).
- Erişim sağlayıcı: Kullanıcılarına internet ortamına erişim olanağı sağlayan her türlü gerçek veya tüzel kişiler (5651 Sayılı Kanun, Md. 2/e).

- İçerik sağlayıcı: İnternet ortamı üzerinden kullanıcılara sunulan her türlü bilgi veya veriyi üreten, değiştiren ve sağlayan gerçek veya tüzel kişiler (5651 Sayılı Kanun, Md. 2/f).
- İnternet ortamı: Haberleşme ile kişisel veya kurumsal bilgisayar sistemleri dışında kalan ve kamuya açık olan internet üzerinde oluşturulan ortam (5651 Sayılı Kanun, Md. 2/g).
- İnternet ortamında yapılan yayın: İnternet ortamında yer alan ve içeriğine belirsiz sayıda kişilerin ulaşabileceği veriler (5651 Sayılı Kanun, Md. 2/ğ).
- İzleme: İnternet ortamındaki verilere etki etmeksizin bilgi ve verilerin takip edilmesi (5651 Sayılı Kanun, Md. 2/h).
- Toplu kullanım sağlayıcı: Kişilere belli bir yerde ve belli bir süre internet ortamı kullanım olanağı sağlayan (5651 Sayılı Kanun, Md. 2/i).
- Trafik bilgisi: Taraflara ilişkin IP adresi, port bilgisi, verilen hizmetin başlama ve bitiş zamanı, yararlanılan hizmetin türü, aktarılan veri miktarı ve varsa abone kimlik bilgileri (5651 Sayılı Kanun, Md. 2/j).
- Veri: Bilgisayar tarafından üzerinde işlem yapılabilen her türlü değer (5651 Sayılı Kanun, Md. 2/k)
- Yayın: İnternet ortamında yapılan yayın (5651 Sayılı Kanun, Md. 2/l).
- Yer sağlayıcı: Hizmet ve içerikleri barındıran sistemleri sağlayan veya işleten gerçek veya tüzel kişiler (5651 Sayılı Kanun, Md. 2/m).
- Erişimin engellenmesi: Alan adından erişimin engellenmesi, IP adresinden erişimin engellenmesi, içeriğe (URL) erişimin engellenmesi ve benzeri yöntemler kullanılarak erişimin engellenmesi (5651 Sayılı Kanun, Md. 2/o).
- İçeriğin yayından çıkarılması: İçerik veya yer sağlayıcılar tarafından içeriğin sunuculardan veya barındırılan içerikten çıkarılması (5651 Sayılı Kanun, Md. 2/ö).
- URL adresi: İlgili içeriğin internette bulunduğu tam internet adresi (5651 Sayılı Kanun, Md. 2/p).
- Uyarı yöntemi: İnternet ortamında yapılan yayın içeriği nedeniyle haklarının ihlal edildiğini iddia eden kişiler tarafından içeriğin yayından çıkarılması amacıyla öncelikle içerik sağlayıcısına, makul sürede sonuç alınamaması

hâlinde yer sağlayıcısına iletişim adresleri üzerinden gerçekleştirilecek bildirim yöntemi (5651 Sayılı Kanun, Md. 2/r).

- Sosyal ağ sağlayıcı: Sosyal etkileşim amacıyla kullanıcıların internet ortamında metin, görüntü, ses, konum gibi içerikleri oluşturmalarına, görüntülemelerine veya paylaşmalarına imkân sağlayan gerçek veya tüzel kişiler (5651 Sayılı Kanun, Md. 2/s).

5651 sayılı Kanun özellikle Facebook, Instagram ve Twitter gibi milyonlarca kullanıcısı olan sosyal medya platformlarına önemli yükümlülükler getirmektedir. Her gün milyonlarca insanın özel hayatlarıyla ilgili bilgi paylaştığı, herhangi bir konuyla ilgili fikir beyan ettiği, fotoğraf paylaştığı, birçok kamu kurumunun ve özel kuruluşun kendi internet siteleri haricinde kamuoyuna duyurular yaptığı bu platformlar gerek kullanıcılarını bilgilendirme gerekse de kendi platformlarında yapılan paylaşımların gerekli görüldüğü taktirde kanunla belirlenen şekilde yayından kaldırılmasına kadar farklı yükümlük ve sorumluluklar altına sokulmuştur. Kanunla getirilen bu yükümlülük ve sorumluluklara uymayanlar için oldukça caydırıcı para cezaları öngörülmüştür. Sosyal medya platformları, kanunda "sosyal ağ sağlayıcıları" olarak tanımlanmıştır.

Kanunun 3'üncü maddesinde,

> *"(1) İçerik, yer ve erişim sağlayıcıları, yönetmelikle belirlenen esas ve usûller çerçevesinde tanıtıcı bilgilerini kendilerine ait internet ortamında kullanıcıların ulaşabileceği şekilde ve güncel olarak bulundurmakla yükümlüdür. (2) Yukarıdaki fıkrada belirtilen yükümlülüğü yerine getirmeyen içerik, yer veya erişim sağlayıcısına Başkan tarafından iki bin Türk lirasından elli bin Türk lirasına kadar idarî para cezası verilir"* (5651 Sayılı Kanun, Md. 3)

şeklinde içerik, yer ve erişim sağlayıcılara kullanıcılarını tanıtıcı bilgiler noktasında bilgilendirme yükümlülüğü getirmiştir. Bu yükümlülüğü yerine getirmeyenler için uygulanacak maddi cezanın karar verici mercii olarak belirlenen "başkan" ise Bilgi Teknolojileri ve İletişim Kurumu'nun (BTK) başkanıdır. Ayrıca kanun kapsamında belirtilen yönetmelik ise bu kanun yayınlandıktan sonra kanunun uygulanması adına 1 Kasım ve 30 Kasım 2007 tarihinde dönemin Başbakanlık kurumu tarafından çıkartılan "İnternet Ortamında Yapılan Yayınların Düzenlenmesine Dair Usul ve Esaslar Hakkında Yönetmelik" ile "İnternet Toplu Kullanım Sağlayıcıları Hakkında

Yönetmelik" ve 24 Ekim tarihinde Telekomünikasyon Kurumu[18] tarafından hazırlanan "Telekomünikasyon Kurumu Tarafından Erişim Sağlayıcılara ve Yer Sağlayıcılara Faaliyet Belgesi Verilmesine İlişkin Usul ve Esaslar Hakkında Yönetmelik" isimleriyle çıkartılan üç yönetmeliktir.

Kanunda belirtilen bilgilendirme yöntemi olarak ise aynı maddenin üçüncü fıkrasında *"internet sayfalarındaki iletişim araçları, alan adı, IP adresi ve benzeri kaynaklarla elde edilen bilgiler üzerinden elektronik posta veya diğer iletişim araçları ile.."* şeklinde belirlenmiştir. Bu noktada özellikle belirtilmesi gereken konu ise aynı maddenin dördüncü fıkrasında muhatabın yurt dışında bulunması halinde idari para cezasının tebligatının üçüncü fıkrada belirtilen şekilde yapılmasının uygun görülmüş olmasıdır. Fiziki olarak sınırları bulunmayan siber uzayda hizmet vericilerin belirli bir coğrafyada bulunmalarını gerektiren bir durum genellikle yoktur. Dolayısıyla hizmet sağlayıcılar ülke dışında herhangi bir yerde olabilir. Buna bağlı olarak kanuna aykırı bir şekilde davranan içerik, yer ve erişim sağlayıcıların yurt dışında bulunması durumunda bahsi geçen idari para cezasının herhangi bir yaptırım özelliğinin olmadığı söylenebilir. Ceza kanunda belirtildiği şekliyle muhatabına tebliğ edilmiş olsa dahi yurt dışında bulunan muhatabın bu cezayı ödemesi için gerekli yaptırımın uygulanması noktasında muhatabın bulunduğu ülkeyle mevcut konu hakkında bir uluslararası anlaşma mevcut değilse bu cezanın uygulanabilmesi söz konusu olmayacaktır.

5651 sayılı Kanunun yer sağlayıcılara getirdiği önemli yükümlülüklerden birisi ise her ne kadar yer sağlayıcıyı yer sağladığı içeriğin hukuka uygun olup olmamasını kontrol etme ya da araştırma yükümlülüğü yüklemese de (5651 Sayılı Kanun, Md. 5/1) bu kanunun 8'inci ve 9'uncu maddelerinde belirtilen suçlar kapsamında haberdar edilmesi durumunda içeriği yayından kaldırmakla yükümlü hale getirilmiştir (5651 Sayılı Kanun, Md. 5/2). Buna ek olarak "*yer sağladığı hizmetlere ilişkin trafik bilgilerini bir yıldan az ve iki yıldan fazla olmamak üzere"* saklamakla yükümlü olan yer sağlayıcı bu bilgileri gerektiğinde BTK ile paylaşmak zorundadır (5651 Sayılı

[18] 2813 sayılı, 5 Nisan 1983 tarihli Telsiz Kanunu'nda değişiklik yapan 27 Ocak 2000 tarihli, 4502 sayılı kanun ile "Telekomünikasyon Kurumu" kurulmuştur. 5809 sayılı ve 10 Kasım 2008 tarihli, Elektronik Haberleşme Kanunu ile kurumun adı Bilgi Teknolojileri ve İletişim Kurumu olarak değiştirilmiştir. Bkz. https://www.btk.gov.tr/tarihce

Kanun, Md. 5/3). Yapılan bu düzenlemeyle internet ortamında işlenen bir suçun soruşturulmasında ihtiyaç duyulan bilgilerin elde edilmesinin kolaylaştırılması amaçlanmıştır. Yapılan bu düzenleme internet ortamında yer ve hizmet sağlayıcıların büyük çoğunluğunun özel kuruluşlar olduğu düşünüldüğünde oldukça önemli bir düzenleme olarak değerlendirilmektedir.

Kanun aynı zamanda erişim sağlayıcılara da herhangi bir kullanıcısının hukuka aykırı olarak yayınladığı içerikler sebebiyle yükümlülük getirmektedir. Kanunun 6'ncı maddesi uyarınca erişim sağlayıcı "*Herhangi bir kullanıcısının yayınladığı hukuka aykırı içerikten, bu Kanun hükümlerine uygun olarak haberdar edilmesi halinde…"* (5651 sayılı Kanun, Md. 6) erişimi engellemekle yükümlüdür. Bu bağlamda kanunla birlikte kanun kapsamında daha önce de belirtilen 8'inci ve 9'uncu maddeler kapsamında suç olarak tanımlanan eylemlerin tespit edilmesi ve kanun hükümlerine göre erişim sağlayıcının haberdar edilmesi halinde erişimin engellenmesini bir zorunluluk haline getirmektedir.

5651 sayılı Kanun, daha önce TCK'nın ilgili bölümlerinde incelenen suçların bilişim cihazları yoluyla gerçekleştirilmesi halinde erişimin engellenmesini sağlayacak şekilde düzenleme yapmıştır. Bu bağlamda 5651 sayılı kanunun 8'inci ve 9'uncu maddeleri TCK'da belirtilen şu suçlar kapsamında içeriğin çıkarılması ve erişimin engellenmesi kararı alınabilir:

> *"…soruşturma evresinde hâkim, kovuşturma evresinde ise mahkeme tarafından verilir. Soruşturma evresinde, gecikmesinde sakınca bulunan hallerde Cumhuriyet savcısı tarafından da içeriğin çıkarılmasına ve/veya erişimin engellenmesine karar verilebilir. Bu durumda Cumhuriyet savcısı kararını yirmidört saat içinde hâkimin onayına sunar ve hâkim, kararını en geç yirmidört saat içinde verir. Bu süre içinde kararın onaylanmaması halinde tedbir, Cumhuriyet savcısı tarafından derhal kaldırılır. Erişimin engellenmesi kararı, amacı gerçekleştirecek nitelikte görülürse belirli bir süreyle sınırlı olarak da verilebilir…"* (5651 sayılı Kanun, Md. 8/2).

Aynı maddenin üçüncü fıkrasına göre ise içeriğin çıkarılması ve/veya erişimin engellenmesi kararı re'sen BTK başkanı tarafından da verilebilir şeklinde bir düzenleme de 2020 yılında yapılmış ve ortaya çıkan suç unsuru sebebiyle erişimin engellenmesi veya içeriğin çıkartılması uygulamasının daha hızlı bir şekilde yapılmasının önü açılmıştır. Bu noktada mahkeme kararı olmadan böyle bir uygulamanın yapılmasına izin veren kanunun ilgili maddesi ile kamuoyunda ifade

özgürlüğünün kısıtlanması ve keyfi olarak sansür uygulanması konularında ciddi tartışmalar ortaya çıkmıştır. İlgili maddenin birinci fıkrasında belirtilen suçlar ise şu şekilde düzenlenmiştir:

> *"(1) İnternet ortamında yapılan ve içeriği aşağıdaki suçları oluşturduğu hususunda yeterli şüphe sebebi bulunan yayınlarla ilgili olarak içeriğin çıkarılmasına ve/veya erişimin engellenmesine karar verilir:*
> *a) 26/9/2004 tarihli ve 5237 sayılı Türk Ceza Kanunu'nda yer alan;*
> *1) İntihara yönlendirme (madde 84),*
> *2) Çocukların cinsel istismarı (madde 103, birinci fıkra),*
> *3) Uyuşturucu veya uyarıcı madde kullanılmasını kolaylaştırma (madde 190),*
> *4) Sağlık için tehlikeli madde temini (madde 194),*
> *5) Müstehcenlik (madde 226),*
> *6) Fuhuş (madde 227),*
> *7) Kumar oynanması için yer ve imkân sağlama (madde 228),*
> *suçları.*
> *b) 25/7/1951 tarihli ve 5816 sayılı Atatürk Aleyhine İşlenen Suçlar Hakkında Kanunda yer alan suçlar.*
> *c) 29/4/1959 tarihli ve 7258 sayılı Futbol ve Diğer Spor Müsabakalarında Bahis ve Şans Oyunları Düzenlenmesi Hakkında Kanunda yer alan suçlar.*
> *ç) 1/11/1983 tarihli ve 2937 sayılı Devlet İstihbarat Hizmetleri ve Milli İstihbarat Teşkilatı Kanununun 27 nci maddesinin birinci ve ikinci fıkrasında yer alan suçlar."* (5651 sayılı Kanun, Md. 8/1).

Kanun kapsamında içeriğin çıkarılması ve/veya erişimin engellenmesi kararı yetkisi eğer gecikmesinde sakınca bulunan bir durum varsa BTK başkanına madde 8/A ile verilmiştir. Bu haller ise ilgili maddenin birinci fıkrasında;

> *"Yaşam hakkı ile kişilerin can ve mal güvenliğinin korunması, millî güvenlik ve kamu düzeninin korunması, suç işlenmesinin önlenmesi veya genel sağlığın korunması sebeplerinden bir veya bir kaçına bağlı olarak hâkim veya gecikmesinde sakınca bulunan hâllerde, Cumhurbaşkanlığı veya millî güvenlik ve kamu düzeninin korunması, suç işlenmesinin önlenmesi veya genel sağlığın korunması ile ilgili bakanlıkların talebi üzerine Başkan tarafından internet ortamında yer alan yayınla ilgili olarak içeriğin çıkarılması ve/veya erişimin engellenmesi kararı verilebilir. Karar, Başkan tarafından derhâl erişim sağlayıcılara ve ilgili içerik ve yer sağlayıcılara bildirilir. İçerik çıkartılması ve/veya erişimin engellenmesi kararının gereği, derhâl ve en geç kararın bildirilmesi anından itibaren dört saat içinde yerine getirilir."* (5651 sayılı Kanun, Md. 8/A)

şeklinde düzenlenmiştir. 5651 sayılı Kanun, milli güvenlik ve kamu düzeninin korunması konusuna ayrı bir önem atfederek bu düzenlemeye gitmiştir. Özellikle sosyal medya üzerinden gerçek olmayan haberlerin oldukça kısa bir süre içerisinde yayılarak toplum içerisinde kargaşaya neden olabilecek sonuçlar doğurma ihtimali düşünüldüğünde bu düzenleme siber uzayda güvenliğin sağlanması anlamında

oldukça önemlidir. Fakat temel hak ve özgürlükler kapsamında ifade özgürlüğünün sınırlandırılması bağlamında tartışmalı bir konu olarak karşımıza çıkmaktadır.

5651 sayılı kanun gerçek ve tüzel kişilere internet ortamında kişilik haklarının ihlal edilmesi durumunda içeriğin yayından çıkarılması ve erişimin engellenmesinin sağlanmasını da mümkün kılmıştır. Kanunun 9'uncu maddesinin birinci fıkrasına göre;

> *"(1) İnternet ortamında yapılan yayın içeriği nedeniyle kişilik haklarının ihlal edildiğini iddia eden gerçek ve tüzel kişiler ile kurum ve kuruluşlar, içerik sağlayıcısına, buna ulaşamaması hâlinde yer sağlayıcısına başvurarak uyarı yöntemi ile içeriğin yayından çıkarılmasını isteyebileceği gibi doğrudan sulh ceza hâkimine başvurarak içeriğin çıkarılmasını ve/veya erişimin engellenmesini de isteyebilir."* (5651 sayılı Kanun, Md. 9/1)

hükmü ile gerçek ve tüzel kişilerin kişilik haklarının internet ortamında korunmasına yönelik bir düzenleme yapılmıştır.

Kanunun 9'uncu maddesine göre ise kişilik haklarının ihlali iddiasıyla yapılan başvurularda sulh ceza hakimliğine yapılan başvurularda erişimin engellenmesi kararı sulh ceza hâkimi tarafından verilmektedir. Burada dikkat çeken birkaç hususun üzerinde durmak faydalı olacaktır. İlk olarak kişilik hakkının ihlal edildiği iddiasıyla içerik ve/veya yer sağlayıcıya doğrudan yapılan başvurularda içerik ve/veya yer sağlayıcıya yapılan başvuruya yirmi dört saat içerisinde cevap verme yükümlülüğünün yüklenmiş olmasıdır (5651 sayılı Kanun, Md. 8/2). Bu durum 2020 yılında 7253 sayılı Kanun'la eklenen Ek madde 4'ün üçüncü fıkrasında belirtilen sosyal ağ sağlayıcılara madde 9 ve 9/A kapsamında belirtilen kişilik haklarının ihlali ile ilgili yapılan başvurularda sosyal ağ sağlayıcının yirmi dört saat yerine kırk sekiz saat içerisinde cevap verme yükümlüğü ile çelişmektedir.

Dikkat çeken bir diğer husus ise sulh ceza hakimliğine yapılan başvurularda hâkimin karar verme şekli konusunda altıncı fıkrada belirtilen usul konusudur. Kanunun 9'uncu maddesinin altıncı fıkrasına göre "*Hâkim bu madde kapsamında yapılan başvuruyu en geç yirmi dört saat içinde duruşma yapmaksızın karara bağlar. Bu karara karşı 4/12/2004 tarihli ve 5271 sayılı Ceza Muhakemesi Kanunu hükümlerine göre itiraz yoluna gidilebilir."* (5651 sayılı Kanun, Md. 9/6) hükmü belirtilmiştir. Hâkimin yapılan başvuruyla ilgili vereceği kararı yirmi dört saat

içerisinde duruşma yapmaksızın karar verebilmesine izin veren bu düzenleme, özellikle ifade özgürlüğü ve adil yargılanma konuları kapsamında değerlendirildiğinde bazı sıkıntıları da beraberinde getirmektedir. Hâkimin duruşma yapmadan karar verebilmesi yetkisi karşı tarafın yapılan ihlal başvurusu ile ilgili kendisini savunma ve/veya delilleri mahkemeye sunma fırsatını elinden almaktadır. Her ne kadar CMK hükümlerine göre itiraz hakkı saklı olsa da yargılanma sürecinde tarafların eşit koşullarda dinlenmesi ve delillerin incelenmesi durumu bu düzenleme ile mümkün görünmemektedir. Ayrıca hâkimin duruşma olmaksızın vereceği kararın taraflı olabileceği ve kişilik hakkının ihlalini belirleyecek yeterli donanım ve teçhizata sahip olamayacağı konusunda da tartışmalara neden olan bu düzenleme, AYM başvurularında ve AYM'nin verdiği kararlarda da kendisine yer bulmuştur.

AYM'ye 5651 sayılı Kanun kapsamında yapılan bireysel başvurularda 9'uncu madde ile ilgili yapılan başvurular büyük çoğunluğu oluşturmaktadır. Yapılan başvurular sonucunda verilen kararlar neticesinde önemli bir içtihadın oluştuğu da söylenebilir (Işık, 2022: 975). AYM'ye yapılan 2014/5552 sayılı başvuruya verilen 14/12/2017 tarih ve 30270 sayılı AYM kararı bu bağlamda oldukça önemlidir. Verilen kararda 5651 sayılı Kanun'un 9'uncu maddesi hakkında yapılan bazı tespitler bu kapsamda büyük önem arz etmektedir. AYM'nin 5651 sayılı Kanun'un ilgili maddesi ile ilgili yaptığı bu tespitlere göre 5651 sayılı Kanun'daki erişimin engellenmesi kararları cezai ve idari yaptırım niteliğinde olmayıp tedbir niteliğindedir. Dolayısıyla koruma tedbiri kapsamında verilen kararların uygulanması, iddia edilen suçun işlendiği konusunda hukuki bir kesinlik doğurmamaktadır ve bu kesinlik ancak hükmün kesinleşmesi ile ortaya çıkacaktır (AYM, 30270 Sayılı Karar, 2017). Ayrıca yapılan tespite göre kişilik haklarının ihlal edildiği iddiasıyla sulh ceza mahkemelerine yapılan başvurularda erişimin engellenmesi kararı ile ilgili hâkimin yaptığı inceleme ve verdiği kararlar noktasında yapılan tespit oldukça dikkate değerdir. Buna göre;

> "***60.*** *Görüldüğü üzere erişimin engellenmesi talebi üzerine sulh ceza hâkimi, talep sahibinin sunduğu evrak üzerinden inceleme yapmaktadır. Dolayısıyla ilgili yayın organı ve sorumlular, yapılan başvurudan haberdar olmamaktadır. Dahası aleyhlerine erişimin engellenmesi talep edilen internet sitesinin ilgilileri, duruşma açılmayacağı için nizalı davalardaki gibi duruşmada hazır bulunamamaktadır. Hâkim de kararını yirmi dört saat içinde vermek zorunda olduğu için karşı tarafa tebligatta bulunup diyeceklerini yazılı olarak sunmasını da karşı taraftan isteyememektedir. Karşı taraf da kendisini savunamamakta;*

hâkimin kararını etkilemek amacıyla sunulan delil, mütalaa ve görüşler hakkında bilgi sahibi olamamakta ve bunlar hakkında yorum yapamamaktadır.

61. *5651 sayılı Kanun'da öngörülen erişimin engellenmesi yolu çekişmesiz bir yargı yolu olduğundan, başka bir deyişle karşı taraf bulunmadığından karardan etkilenecek basın organının temsilcileri ile sorumlu kişiler silahların eşitliği ilkesinden faydalanamamakta; talepte bulunanın iddialarına karşı delil sunmak da dâhil olmak üzere savunmalarını ortaya koymak için makul ve kabul edilebilir olanaklara sahip olamamaktadır. Özet olarak hâkim, kararını dosya üzerinden yani talepte bulunanın sunduğu bilgi ve belgelere göre vermekte; bu yargılamada karşı tarafın görüşleri alınamamaktadır.*" (AYM, 30270 Sayılı Karar, 2017).

Görüldüğü üzere AYM'nin vermiş olduğu kararda yapmış olduğu tespitler de 5651 sayılı Kanun'un 9'uncu maddesinde ele alınan kişilik haklarının korunması ile ilgili yapılan başvurularda verilen kararların adil yargılama noktasında sıkıntılı olduğu yönündedir.

5651 sayılı Kanun ile madde 6/A kapsamında 8 ve 8/A maddeleri kapsamı dışındaki tüm içeriğin çıkarılması ve/veya erişimin engellenmesine yönelik kararların uygulanmasını sağlamak üzere "Erişim Sağlayıcıları Birliği (ESB)" kurulmuştur (5651 Sayılı Kanun, Md. 6/A). Kurulan birlik özel hukuk tüzel kişiliğine sahiptir. Birliğin esas görevi 5651 sayılı Kanun'un 8 ve 8/A maddeleri kapsamı dışında kalan bütün içeriğin çıkarılması ve/veya erişimin engellenmesi kararlarının niteliklerine göre erişim sağlayıcılar ile ilgili içerik ve yer sağlayıcılara iletilmesi ve koordinasyonun sağlanması yoluyla uygulanmasıdır. Birliğin çalışma usul ve esasları BTK tarafından onaylanan tüzükle belirlenmiştir. Birliğe 5809 sayılı Elektronik Haberleşme Kanunu kapsamında yetki verilen tüm internet servis sağlayıcılarının ve internet erişim hizmeti veren diğer işletmecilerin üye olması ise zorunludur (ESB, 2021).

5651 sayılı kanunla ilgili olarak 2020 ve 2022 yılında yapılan iki önemli değişiklik daha önce de belirtildiği üzere kanunla ilgili kamuoyunda önemli tartışmaların ortaya çıkmasına neden olmuştur. 2020 yılında 7253 sayılı "İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanunda Değişiklik Yapılmasına Dair Kanun" ile 5651 sayılı kanunda yapılan değişiklikler sosyal medya platformlarına oldukça önemli yükümlülükler getirmiştir. Kamuoyunda "sosyal medya düzenlemesi" olarak anılan bu düzenleme, sosyal medya platformlarına beraberinde getirdiği yükümlülükler nedeniyle olumlu ve olumsuz anlamda birçok eleştiriye maruz kalmıştır.

Yapılan değişiklikle sosyal medya platformlarına ya da kanunda belirtildiği üzere sosyal ağ sağlayıcılara temsilci atama yükümlülüğü getirilmiştir. Bu yükümlülüğe göre;

> "*Türkiye'den günlük erişimi bir milyondan fazla olan yurt dışı kaynaklı sosyal ağ sağlayıcı; Kurum, Birlik, adli veya idari makamlarca gönderilecek tebligat, bildirim veya taleplerin gereğinin yerine getirilmesi ve kişiler tarafından bu Kanun kapsamında yapılacak başvuruların cevaplandırılması ve bu Kanun kapsamındaki diğer yükümlülüklerin yerine getirilmesini temin için yetkili en az bir kişiyi Türkiye'de temsilci olarak belirler ve bu kişinin iletişim bilgilerine kolayca görülebilecek ve doğrudan erişilebilecek şekilde internet sitesinde yer verir…"* (5651 Sayılı Kanun, Ek Madde 4/1).

Bu değişiklikle birlikte Türkiye'de milyonlarca kullanıcısı olan Facebook, Instagram ve Twitter gibi sosyal medya platformları yetkili en az bir kişiyi temsilci olarak belirlemekle zorunlu hale gelmiştir. Bu yükümlülüğü yerine getirmeyen sosyal ağ sağlayıcıya BTK tarafından yapılan bildirim sonrasında otuz gün içerisinde bu yükümlülüğün yerine getirilmemesi halinde BTK başkanı tarafından on milyon Türk lirası para cezası verilmesi hükmü getirilmiştir. Para cezası verildikten sonraki otuz gün içerisinde bu yükümlülüğün yerine getirilmemesi halinde otuz milyon Türk lirası daha idari para cezası verilmesi öngörülmüştür. Verilen ikinci idari para cezasının ardından otuz gün içerisinde gerekli yükümlülüğün yerine getirilmemesi halinde ise BTK başkanı tarafından ilgili sosyal ağ sağlayıcıya Türkiye'de vergi mükellefi olan gerçek ve tüzel kişilerin yeni reklam vermesinin yasaklanacağı hükmü getirilmiştir. Eğer reklam yasağı kararının ardından üç ay içerisinde bu yükümlülük yine yerine getirilmezse sosyal ağ sağlayıcının internet trafiği bant genişliğinin yüzde elli oranında daraltılması için sulh ceza hakimliğine BTK başkanlığı tarafından başvurulabilir. Başvurunun kabul edilmesinin ardından otuz gün içerisinde yükümlülüğün yerine getirilmemesi halinde ise yine aynı şekilde, bu sefer ilgili sosyal ağ sağlayıcının internet trafiği bant genişliğinin yüzde doksan oranında daraltılması için sulh ceza hakimliğine başvuruda bulunulabileceği öngörülmüştür (5651 Sayılı Kanun, Ek Madde 4/2).

Aynı maddenin üçüncü fıkrasına göre ise günlük erişimi bir milyondan fazla olan yurt içi ve yurt dışı kaynaklı sosyal ağ sağlayıcıya daha önce de belirtilen madde 9 ve 9/A kapsamında belirtilen içeriklere yönelik olarak kişiler tarafından yapılan başvurulara en geç kırk sekiz saat içerisinde cevap verilmesi yükümlülüğü getirilmiştir

(5651 Sayılı Kanun, Ek Madde 4/3). Bu düzenlemeyle sosyal medya platformlarında gerçek ve tüzel kişilerin kişilik haklarının korunması ve özel hayatın gizliliği konularında güvenlik tedbirleri alınmıştır.

2022 yılında 7418 sayılı "Basın Kanunu ile Bazı Kanunlarda Değişiklik Yapılmasına Dair Kanun" ile 5651 sayılı kanunda yapılan değişiklikler ise daha önce 2020 yılında yapılan değişikliklere benzer şekilde kamuoyunda birçok tartışmayı da beraberinde getirmiştir. Yapılan bu değişiklik kamuoyunda "dezenformasyon yasası" ya da "sansür yasası" olarak anılmıştır. Yapılan değişiklikle daha önce 2020 yılında eklenen Ek Madde 4'e eklenen beşinci fıkraya göre TCK'da yer alan bazı suçlarla alakalı olarak internet içerikleri oluşturan veya yayan faillere ulaşmak için gerekli bilgilerin soruşturma aşamasında Cumhuriyet savcısına, kovuşturma aşamasında ise yargılamanın yürütüldüğü mahkemeye sosyal ağ sağlayıcısının Türkiye'deki temsilcisi tarafından verilmesi zorunlu hale getirilmiştir. Ek Madde 4 beşinci fıkra şu şekilde düzenlenmiştir:

> *"(5) Türk Ceza Kanunu'nda yer alan;*
> *a) Çocukların cinsel istismarı (madde 103),*
> *b) Halkı yanıltıcı bilgiyi alenen yayma (madde 217/A),*
> *c) Devletin birliğini ve ülke bütünlüğünü bozmak (madde 302),*
> *ç) Anayasal Düzene ve Bu Düzenin İşleyişine Karşı Suçlar (madde 309, 311, 312, 313, 314, 315, 316),*
> *d) Devlet Sırlarına Karşı Suçlar ve Casusluk (madde 328, 329, 330, 331, 333, 334, 335, 336, 337),*
> *suçlarına konu internet içeriklerini oluşturan veya yayan faillere ulaşmak için gerekli olan bilgiler soruşturma aşamasında Cumhuriyet savcısı, kovuşturma aşamasında yargılamanın yürütüldüğü mahkeme tarafından talep edilmesi üzerine ilgili sosyal ağ sağlayıcının Türkiye'deki temsilcisi tarafından adli mercilere verilir. Bu bilgilerin talep eden Cumhuriyet Başsavcılığı veya mahkemeye verilmemesi durumunda, ilgili Cumhuriyet savcısı tarafından, yurt dışı kaynaklı sosyal ağ sağlayıcının internet trafiği bant genişliğinin yüzde doksan oranında daraltılması talebiyle Ankara Sulh Ceza Hâkimliğine başvurulabilir. İnternet trafiği bant genişliğinin daraltılması kararı verilmesi hâlinde, bu karar erişim sağlayıcılara bildirilmek üzere Kuruma gönderilir. Kararın gereği, bildirimden itibaren derhâl ve en geç dört saat içinde erişim sağlayıcıları tarafından yerine getirilir. Sosyal ağ sağlayıcının, bu fıkra kapsamındaki yükümlülüklerini yerine getirmesi hâlinde yaptırımlar kaldırılır ve Kuruma bildirilir."* (5651 Sayılı Kanun, Ek Madde 4/5).

Fıkranın sonunda belirtilen *"Kurum"* kavramı ile kastedilen BTK'dır. Eklenen bu madde özellikle internet ortamında çocukların korunması ve gerçek olmayan bilginin sosyal medya platformlarında yayılması ile toplumsal olarak kamuoyunu

yanlış yönlendirilmesini engelleme çabası olarak yorumlanmıştır. Bununla bağlantılı olarak yine aynı kanunun 29'uncu maddesi ile 5237 sayılı TCK'ya yapılan eklemeyle

> *"Halkı yanıltıcı bilgiyi alenen yayma, MADDE 217/A- (1) Sırf halk arasında endişe, korku veya panik yaratmak saikiyle, ülkenin iç ve dış güvenliği, kamu düzeni ve genel sağlığı ile ilgili gerçeğe aykırı bir bilgiyi, kamu barışını bozmaya elverişli şekilde alenen yayan kimse, bir yıldan üç yıla kadar hapis cezasıyla cezalandırılır. 2) Fail, suçu gerçek kimliğini gizleyerek veya bir örgütün faaliyeti çerçevesinde işlemesi hâlinde, birinci fıkraya göre verilen ceza yarı oranında artırılır."* (7418 sayılı Kanun, Md. 29)

hükmü kanuna eklenmiştir. Bu noktada özellikle bu düzenlemeyle ifade özgürlüğünün kısıtlanacağı ve sansür uygulamalarının yaygınlaşacağı, sosyal medyada yapılan birçok paylaşımla ilgili soruşturma açılarak adalet sisteminin meşgul edileceği, toplumun bu düzenlemeyle karşıt görüşlerini açıklamasının önüne geçilmeye çalışıldığı, seçimlerde haksız rekabetin ortaya çıkacağı, bu düzenlemenin Anayasanın 13'üncü maddesi olan "*Temel hak ve hürriyetler, özlerine dokunulmaksızın yalnızca Anayasanın ilgili maddelerinde belirtilen sebeplere bağlı olarak ve ancak kanunla sınırlanabilir. Bu sınırlamalar, Anayasanın sözüne ve ruhuna, demokratik toplum düzeninin ve lâik Cumhuriyetin gereklerine ve ölçülülük ilkesine aykırı olamaz."* (T.C. Anayasası, Md. 13) hükmünü ihlal ettiği ve bu maddenin değerlendirmesinin çok açık olmaması nedeniyle kötüye kullanımının müsait olması gibi konular nedeniyle tartışmalara neden olmuştur (Oymak, 2022: 13).

5651 sayılı Kanun, sosyal medya platformlarının kullanımının tahmin edilemeyecek boyutlarda kullanımının yaygınlaşması ile ortaya çıkan yeni toplumsal yapının düzenlenmesi bağlamında önemli bir yasal zemin oluşturmuştur. Kanunla ilgili yapılan değişiklikler ifade ve düşünce özgürlüğü kapsamında oldukça sert eleştirilere maruz kalmış olsa da artık kontrol edilmesi oldukça güç bir boyuta ulaşan internet ortamında bireylerin temel hak ve özgürlüklerinin ve kişilik haklarının korunmasıyla birlikte ulusal güvenlik ve toplum düzeninin korunması bağlamında oldukça önemli bir düzenleme olarak değerlendirilmektedir. Kanun kapsamında sosyal medya platformlarına getirilen yükümlülükler ve bu yükümlülüklerin yerine getirilmediği durumlarda bu kurumlara yüklenecek olan idari para cezaları yaptırım gücü bakımından önemlidir. Fakat bu yükümlülükleri yerine getirmeyen sosyal ağ sağlayıcılarına idari para cezası, reklam cezası veya internet erişim bant kısıtlaması uygulanmasının haricinde erişimin yasaklanması ya da tamamen kapatılması gibi bir

yaptırım öngörülmemiştir. Ayrıca internet erişim bant kısıtlaması kullanıcılar tarafından VPN[19] uygulamalarıyla aşılabilmektedir.

2.3. 5809 Sayılı Elektronik Haberleşme Kanunu

2008 yılında yasalaşarak yürürlüğe giren 5809 sayılı Elektronik Haberleşme Kanunu, elektronik haberleşme sektörünün yasal olarak düzenlenmesini ve bu sektörde teknolojinin gelişimi ile hizmet sağlayıcıların sayısındaki artış sebebiyle sektörde denetleme yoluyla haksız rekabetin önüne geçilmesini amaçlamıştır. Kanunun giriş kısmında amacı şu şekilde belirtilmiştir:

> *"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"* (5809 sayılı Kanun, Md. 1).

Kanun özellikle elektronik haberleşme sektöründe rekabetin düzenlenmesi, hizmetlerin yürütülmesi ve bu sektörde alt yapı ve teknolojinin geliştirilmesinin sağlanması adına önemli bir düzenlemedir. Türkiye'ye 1990'lı yılların başında gelen cep telefonu teknolojisinin oldukça kısa süre içerisinde yaygınlaşarak temel iletişim aracı haline gelmesi ve bu konuda hizmet sağlayıcı kuruluşların sayısındaki artış düzenlemeyi mecbur hale getirmiştir. Ayrıca devlet seviyesinde kurumların dijital altyapıya geçişi, e-devlet uygulamalarının artışı ve devlet kurumlarının elektronik haberleşme bağlamında ihtiyacı olan alt yapı ve teknolojinin geliştirilmesi adına gerekli olan düzenleme ihtiyacını karşılama niteliğinde olan bir yasal düzenleme olarak da karşımıza çıkmaktadır. Her ne kadar Kanun'un temel amacı elektronik haberleşme sektörünün düzenlenmesi olsa da bu tezin ana konusunu oluşturan siber uzayın güvenliği noktasında, özellikle kullanıcıların hak ve menfaatlerinin gözetilerek

[19] VPN, Virtual Private Network (Sanal Özel Ağ) kelimesinin kısaltmasıdır. VPN, internet bağlantısını kullanıcıların bilgisayarları, akıllı telefonları veya diğer cihazları arasında özel bir ağ oluşturarak şifreli bir tünel oluşturur. Bu şifreli tünel, kullanıcının internet trafiğini güvenli bir şekilde iletmek için kullanılır. VPN'ler, kullanıcıların internete girdiği yerden bağımsız olarak güvenli ve gizli bir bağlantı sağlar. VPN kullanıcıları, internete bağlandıklarında gerçek IP adreslerini gizleyebilir ve konumlarını değiştirebilir. VPN'ler ayrıca, kullanıcıların coğrafi olarak kısıtlanmış içeriklere erişmesine yardımcı olabilir. Örneğin, bir ülkede bulunmanız gereken bir web sitesine erişmek istiyorsanız, o ülkede bir VPN sunucusu kullanarak sanal olarak orada bulunabilir ve kısıtlamaları aşabilmeyi sağlar. Daha fazla bilgi için bkz. https://www.kaspersky.com/resource-center/definitions/what-is-a-vpn

korunması ve hizmetlerin kesintisiz ve eşit bir şekilde tüm Türkiye'de sağlanması bağlamında kanunda yapılan düzenlemeler oldukça önemlidir.

Kanun aynı zamanda elektronik haberleşme sektöründe yeni teknolojik gelişmelere ayak uydurulması ve bu konuda hizmet sağlayıcıların desteklenmesi ile birlikte bu sektörde verilen hizmet kalitesinin artırımı ve siber güvenliğin geliştirilmesi bağlamında teşvik edici bir nitelik göstermektedir. Kanunun 4'üncü maddesinde belirtilen ilkeler bağlamında bu kanun elektronik haberleşme sektöründe her türlü cihaz sistem ve şebekelerinin kurulması, işletilmesi ve kaynak tahsislerinin yapılması ile düzenlenmesi yetkisi ve sorumluluğunu Devletin yetki ve sorumluluğu altına sokmuştur. Bu bağlamda sektörde serbest piyasa ekonomisi ilkeleri benimsenerek etkin bir rekabet ortamının oluşturulması ve korunması, tüketicilerin hak ve menfaatlerinin gözetilmesi, herkesin makul ve adil bir ücret karşılığında elektronik haberleşme hizmetlerinden yararlanmasını sağlayacak uygulamaların teşvik edilmesi, kurulan sistemlerin uluslararası normlara uygunluğun gerçekleştirilmesi, elektronik haberleşme sektöründe teknolojik yeniliklerin uygulanması ile araştırma-geliştirme faaliyet ve yatırımların desteklenmesi, hizmet kalitesinin geliştirilmesi noktasında teşvik, hizmetlerin sunulmasında ve bu bağlamda yapılacak düzenlemelerde tarafsızlığın sağlanması, engelli, yaşlı ve sosyal açıdan korumaya muhtaç bireylerin özel ihtiyaçlarının dikkate alınarak karşılanması ve bilgi güvenliği ile haberleşme gizliliğinin gözetilmesi konuları kanunun temel ilkeleri olarak belirlenmiştir (5809 sayılı Kanun, Md. 4/1).

Kanun kapsamında elektronik haberleşme sektöründe belirtilen ilkelerin uygulanması ve gözetilmesi noktasında yetkili merciler olarak Ulaştırma ve Altyapı Bakanlığı (UAB) ile Bilgi Teknolojileri ve İletişim Kurumu (BTK) belirlenmiştir (5809 sayılı Kanun, Md. 5). Özellikle Kanun'a 2014 yılında 6518 sayılı Kanun ile 5'inci maddeye yapılan eklemede UAB'ye siber uzayın güvenliğinin sağlanması noktasında önemli görevler yüklenmiştir. Bu düzenlemeye göre UAB;

> *"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."* (5809 sayılı Kanun, Md. 5/1-h)

konularında görevlendirilmiş ve yetkili mercii olarak belirlenmiştir.

UAB'yle birlikte BTK'ya da siber güvenliğin sağlanması anlamında görev ve yetki veren kanun, BTK'ya 5651 sayılı Kanun çerçevesinde verilen görev ve yetkilere paralel olarak kanunun 6'ncı maddesinde siber güvenlikle alakalı olarak *"Elektronik haberleşme sektörüne yönelik olarak, millî güvenlik, kamu düzeni veya kamu hizmetinin gereği gibi yürütülmesi amacıyla mevzuatın öngördüğü tedbirleri almak."* (5809 sayılı Kanun, Md. 6/1-ş) ve *"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."* (5809 sayılı Kanun, Md. 6/1-v) şeklinde görev ve yetkilendirme yapılmıştır.

Ayrıca kanunun 6'ncı maddesine ek olarak 2016 yılında çıkartılan 671 sayılı Kanun Hükmünde Kararname (KHK) ve 6756 sayılı Kanun ile 5809 sayılı Kanun'da yapılan düzenlemeyle BTK'ya *"..., 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."* (5809 sayılı Kanun, Md. 60/11) fıkrasıyla siber uzayda caydırıcılığın oluşturulması görev ve yükümlülüğü de verilmiştir. Aynı sayılı KHK ve Kanun'la yapılan düzenlemede yapılan bir diğer ekleme ise 5651 sayılı Kanun'la bağlantılı olarak oldukça önemlidir. Yapılan bu ekleme ile

> *"Anayasanın 22 nci maddesinde sayılan sebeplerden biri veya birkaçına bağlı olarak, gecikmesinde sakınca bulunan hâllerde Cumhurbaşkanlığı, alınması gereken tedbirleri belirler ve uygulanmak üzere Kuruma bildirir. Kurum Başkanı, Cumhurbaşkanlığının gerekli gördüğü tedbirlere ilişkin kararını derhal işletmecilere, erişim sağlayıcılara, veri merkezlerine ve ilgili içerik ve yer sağlayıcılara bildirir. Bu kararın gereği, derhal ve kararın bildirilmesi anından itibaren en geç iki saat içinde yerine getirilir. Bu karar, yirmidört saat içinde sulh ceza hakiminin onayına sunulur. Hâkim kararını kırksekiz saat içinde açıklar, aksi halde karar kendiliğinden kalkar.*" (5809 sayılı Kanun, Md. 60/10)

hükmü getirilmiştir. Bu fıkrada belirtilen Anayasa'nın 22'nci maddesi ise herkesin haberleşme hürriyetine sahip olduğunu ve haberleşmenin gizliliğinin esas olduğunu belirtmektedir. Ayrıca Anayasa'nın ilgili aynı maddesine göre;

> *"Millî güvenlik, kamu düzeni, suç işlenmesinin önlenmesi, genel sağlık ve genel ahlâkın korunması veya başkalarının hak ve özgürlüklerinin korunması sebeplerinden biri veya birkaçına bağlı olarak usulüne göre verilmiş hâkim kararı olmadıkça; yine bu sebeplere bağlı olarak gecikmesinde sakınca bulunan hallerde de kanunla yetkili kılınmış merciin yazılı emri bulunmadıkça; haberleşme engellenemez ve gizliliğine dokunulamaz. Yetkili merciin kararı yirmi dört saat içinde görevli hâkimin onayına sunulur. Hâkim, kararını kırk sekiz saat içinde açıklar; aksi halde, karar kendiliğinden kalkar. İstisnaların uygulanacağı kamu kurum ve kuruluşları kanunda belirtilir."* (T.C. Anayasası, Md. 22)

denilmiştir. Burada dikkat çeken husus ise 5651 sayılı Kanun'da üzerinde durulan erişimin engellenmesi ve/veya içeriğin çıkartılması kararının verilmesinde yine aynı şekilde BTK yetkilendirilmiştir. Lakin Anayasa'nın ilgili maddesi gereği Cumhurbaşkanlığının yapacağı başvurularda hâkim kararı aranmaksızın erişimin engellenmesi ya da gerekli tedbirlerin alınmasının en geç iki saat içerisinde yerine getirilmesi zorunlu hale getirilmiştir. Karar verildikten ve gerekli tedbir alındıktan sonra ise sulh ceza hakimliğine yapılan başvurunun hâkim tarafından onaylanması ya da onaylanmaması işlemi gerçekleştirilmektedir. Bu uygulamada ortaya çıkan sorun ise daha önce 5651 sayılı Kanun'un 9'uncu maddesinin uygulama usulleriyle ilgili olarak ortaya çıkan sorunlarla aynı muhteviyata sahiptir.

Daha önce Bakanlar Kurulu tarafından 2022/3842 sayılı "Ulusal Siber Güvenlik Çalışmalarının Yürütülmesi, Yönetilmesi ve Koordinasyonuna İlişkin Karar" ile kurulan Siber Güvenlik Kurulu'nun görevleri, 2014 tarihinde yayımlanan 6518 sayılı kanun ile eklenen Ek Madde 1 ile 5809 sayılı Kanun'da yer bulmuştur. Ek Madde 1'e göre Siber Güvenlik Kurulunun görevleri

> *"a) Siber güvenlik ile ilgili politika, strateji ve eylem planlarını onaylamak ve ülke çapında etkin şekilde uygulanmasına yönelik gerekli kararları almak. b) Kritik altyapıların belirlenmesine ilişkin teklifleri karara bağlamak. c) Siber güvenlikle ilgili hükümlerin tamamından veya bir kısmından istisna tutulacak kurum ve kuruluşları belirlemek. ç) Kanunlarla verilen diğer görevleri yapmak."* (5809 sayılı Kanun, Md. Ek Madde 1/2)

olarak belirlenmiştir. 5809 sayılı Kanun, siber uzayın güvenliği ile alakalı olarak "Kişisel verilerin işlenmesi ve gizliliğinin korunması" başlığı altında madde 51'de bir düzenleme de yapmıştır. Buna göre elektronik haberleşmede kişisel verilerin

işlenmesinde hukuka ve dürüstlük kurallarına uygunluk, elektronik haberleşmenin ve ilgili trafik verisinin gizliliği, kişilerin kullandığı elektronik haberleşme cihazlarında sakladığı kişisel verilere işletmecilerin kişilerin rızası dışında ulaşımının engellenmesi, işletmecilerin şebekelerinin kullanıcılara ait kişisel verilerin güvenliğinin sağlanması adına gerekli tedbirleri alması ve Kanun kapsamında kişisel verilerin gizliliğinin, güvenliğinin ve amacı doğrultusunda kullanılmasının temininden işletmecilerin sorumlu tutulması gibi kişisel verilerin işlenmesi ve gizliliğinin korunması tedbirleri alınmıştır (5809 sayılı Kanun, Md. 51).

5809 sayılı Kanun bahsi geçen siber uzayın güvenliğinin sağlanması ile ilgili olarak yaptığı düzenlemelerin yanında elektronik haberleşme sektöründe yetkili merciler ve görevlerin belirlenmesi, elektronik haberleşme sektöründe hizmet veren işletmelerin yetkilendirilmesi ve bunun usul ve yöntemleri, elektronik haberleşme sektöründe hizmet veren işletmelerin kullanıcılarına uyguladığı tarifelerin düzenlenmesi, erişim ve ara bağlantı konuları, elektronik haberleşme hizmeti veren işletmelerin bu konuda kuracakları alt yapı ve bunları destekleyici ekipmanlarını kamu ve/veya özel mülkiyete konu taşınmazların altından geçirmeleri konusunda geçiş hakkı, numaralandırma ve internet alan adları, tüketici ve son kullanıcı hakları, onaylanmış kuruluşlar ve piyasa gözetimi gibi konuları da detaylı bir şekilde ele almıştır (5809 sayılı Kanun).

5809 sayılı Kanun, siber uzayın güvenliğinin sağlanması noktasında önemli bir yasal düzenleme olarak değerlendirilmektedir. Lakin daha önce de belirtildiği üzere siber güvenlik ile alakalı olarak tek bir yasal düzenlemenin olmaması ve siber uzayın güvenliğiyle alakalı olarak mevcut kanunlarda yapılan değişiklikler ve eklemelerle yasal düzenleme yoluna gidilmesi durumu bu kanun için de geçerli olan bir durumdur. Kanunla siber uzayın güvenliği noktasında önemli yasal düzenlemeler yapılmış olsa da yapılan bu düzenlemeler siber uzay ile ilgili oluşturulan yasal altyapıyı düzenlemenin yanında daha karmaşık bir hale getirmesi anlamında da katkıda bulunmuştur.

2.4. 5070 Sayılı Elektronik İmza Kanunu

Her türlü bilgi ve belgenin dijital ortamda işlenebildiği, bireyler ve kurumlar arasında gönderilip alınabildiği günümüzde 2000'li yıllar itibariyle imzalar da

dijitalleşmeye başlamıştır. Elektronik imza ya da "e-imza" olarak anılan bu uygulama, özellikle devlet kurumları içerisinde veya arasında bilgisayar ortamında hazırlanmış resmî belgelerin yine dijital ortamda imzalanarak ilgili makamlara iletilmesini kolaylaştırmakla beraber işlemlerin ilerleyişine hız kazandırmış ve aynı zamanda fiziki olarak kâğıt ihtiyaç olmadığı için kırtasiye ürünlerinin kullanımında da tasarruf sağlanmasını mümkün kılmıştır. Elektronik imza kullanımının yaygınlaşmaya başlamasıyla bu konunun da yasal olarak düzenlenmesi, güvenli bir şekilde dijital ortamda imza atılması ve sahteciliğin önüne geçilmesi bağlamında bir gereklilik haline gelmiştir.

2004 yılında kabul edilerek yürürlüğe giren 5070 sayılı Elektronik İmza Kanunu, elektronik imza kullanımına dair işlemlerin yasal olarak düzenlenmesini amaçlamıştır. Kanunun amacı *"elektronik imzanın hukukî ve teknik yönleri ile kullanımına ilişkin esasları düzenlemektir."* (5070 sayılı Kanun, Md. 1) olarak belirtilmiştir. Kanunun kapsamı ise 2'nci maddesinde *"elektronik imzanın hukukî yapısını, elektronik sertifika hizmet sağlayıcılarının faaliyetlerini ve her alanda elektronik imzanın kullanımına ilişkin işlemleri kapsar."* (5070 sayılı Kanun, Md. 2) şeklinde düzenlenmiştir.

Kanun kapsamında elektronik imza ile ilgili olan terimlerin tanımı da yapılmıştır. Kanunun 3'üncü maddesinde elektronik imza *"Başka bir elektronik veriye eklenen veya elektronik veriyle mantıksal bağlantısı bulunan ve kimlik doğrulama amacıyla kullanılan elektronik veri"* (5070 sayılı Kanun, Md. 3-b) şeklinde tanımlanmıştır. Yine buna bağlı olarak kişiye özel olarak üretilen elektronik imza için imza sahibi *"Elektronik imza oluşturmak amacıyla bir imza oluşturma aracını kullanan gerçek kişi"* (5070 sayılı Kanun, Md. 3-c) olarak tanımlanmıştır. Elektronik imza, elle atılan imza ya da ıslak imza olarak bilinen imza ile aynı hukuki sonuçları doğurur. Kanunda bunun istisnası ise 5'inci maddede *"Kanunların resmî şekle veya özel bir merasime tabi tuttuğu hukukî işlemler ile banka teminat mektupları ve Türkiye'de yerleşik sigorta şirketleri tarafından düzenlenen kefalet senetleri dışındaki teminat sözleşmeleri, güvenli elektronik imza ile gerçekleştirilemez."* (5070 sayılı Kanun, Md. 5) şeklinde düzenlenmiştir. Elle atılan imza ile aynı hukuki sonuçları doğuran elektronik imzanın kullanılabilmesi için ise kanunda belirtildiği şekliyle bu imzanın "güvenli elektronik imza" olması gerekmektedir. Güvenli elektronik imza ise

4'üncü maddede *"münhasıran imza sahibine bağlı olan, sadece imza sahibinin tasarrufunda bulunan güvenli elektronik imza oluşturma aracı ile oluşturulan, nitelikli elektronik sertifikaya dayanarak imza sahibinin kimliğinin tespitini sağlayan, imzalanmış elektronik veride sonradan herhangi bir değişiklik yapılıp yapılmadığının tespitini sağlayan"* (5070 sayılı Kanun, Md. 4) elektronik imza şeklinde tanımlanmıştır.

5070 sayılı Kanun, elektronik imza bağlamında bilgilerin korunması adına elektronik sertifika hizmet sağlayıcılarına da yükümlülükler vermiştir. Elektronik imzalar sadece BTK tarafından yetkilendirilmiş kuruluşlar tarafından oluşturulabilmektedir. Kanunun 12'nci maddesine göre elektronik hizmet sağlayıcısı,

> *"a) Elektronik sertifika talep eden kişiden, elektronik sertifika vermek için gerekli bilgiler hariç bilgi talep edemez ve bu bilgileri kişinin rızası dışında elde edemez, b) Elektronik sertifika sahibinin izni olmaksızın sertifikayı üçüncü kişilerin ulaşabileceği ortamlarda bulunduramaz, c) Elektronik sertifika talep eden kişinin yazılı rızası olmaksızın üçüncü kişilerin kişisel verileri elde etmesini engeller. Bu bilgileri sertifika sahibinin onayı olmaksızın üçüncü kişilere iletemez ve başka amaçlarla kullanamaz."* (5070 sayılı Kanun, Md. 12)

şeklinde yaptığı düzenlemeyle elektronik imza talebinde bulunan kişilerin bilgilerinin güvenliği noktasında hizmet sağlayıcıya yükümlülük vermektedir. Türkiye'de elektronik sertifika hizmet sağlayıcıları, kanunda belirtildiği üzere BTK tarafından yetkilendirilmekte, ayrıca faaliyet ve işlemlerinin denetim de yapılmaktadır (5070 sayılı Kanun, Md. 15). Buna göre ülkemizde yetkilendirilmiş elektronik hizmet sağlayıcıları Elektronik Bilgi Güvenliği A.Ş. (E-Güven), TÜBİTAK-UEKAE (Kamu Sertifikasyon Merkezi), TürkTrust Bilgi, İletişim ve Bilişim Güvenliği Hizmetleri A.Ş., EBG Bilişim Teknolojileri ve Hizmetleri A.Ş. (E-Tugra), Emniyet Genel Müdürlüğü Sertifikasyon Merkezi (EGMSM), E-İmza Bilgi Güvenliği Hizmetleri A.Ş. (e-İmzaTR), Ayyıldız İmza Bilgi Güvenliği ve Teknolojileri A.Ş. (AYYILDIZ İMZA) ve Arksinger Yazılım ve Donanım Sanayi Ticaret A.Ş. olarak belirlenmiştir. Bahsi geçen kuruluşlardan TÜBİTAK Kamu Sertifikasyon Merkezi sadece kamu çalışanları için elektronik imza hizmeti vermektedir (BTK, 2017).

Elektronik imza kullanımında sahteciliğin önüne geçmek ve bu konuda caydırıcı bir unsur oluşturmak adına 2008 yılında 5728 sayılı Kanun ile 5070 sayılı Kanuna üç madde eklenmiş ve bu maddeler kapsamında imza oluşturma verilerinin

izinsiz kullanımı ve elektronik sertifikalarda sahtekarlık suçları düzenlenerek idari para cezaları belirlenmiştir. Kanunun 16'ncı maddesine göre;

> *"Elektronik imza oluşturma amacı ile ilgili kişinin rızası dışında; imza oluşturma verisi veya imza oluşturma aracını elde eden, veren, kopyalayan ve bu araçları yeniden oluşturanlar ile izinsiz elde edilen imza oluşturma araçlarını kullanarak izinsiz elektronik imza oluşturanlar bir yıldan üç yıla kadar hapis ve elli günden az olmamak üzere adlî para cezasıyla cezalandırılırlar."* (5070 sayılı Kanun, Md. 16)

şeklinde yapılan düzenlemede bahsi geçen suçlar hizmet sağlayıcısı çalışanları tarafından işlendiği takdirde bu cezaların yarısına kadar artırılacağı belirtilmiştir. Ayrıca 17'nci maddede sahte elektronik sertifika oluşturulması halinde ya da mevcut olan sertifikaların kopyalanması veya zarar verilmesi durumunda veya taklit edilen ve zarar verilen elektronik sertifikaların bilerek kullanılması halinde iki yıldan beş yıla kadar hapis cezası ve yüz günden az olmamak üzere adli para cezası öngörülmüştür. 16'ncı maddede olduğu gibi bu suçların hizmet sağlayıcısı çalışanları tarafından işlenmesi halinde ise bu cezaların yarısına kadar artırılacağı belirtilmiştir (5070 sayılı Kanun, Md. 17).

2.5. 6698 Sayılı Kişisel Verilerin Korunması Kanunu (KVKK)

6698 sayılı Kişisel Verilerin Korunması Kanunu 2008 yılında TBMM'ye sunulmuş ve kabul edilmesi oldukça uzun bir süre aldıktan sonra 2016 yılında kabul edilerek yürürlüğe girmiştir. Kanunun Meclis'e sunulmasından sonra ise kişisel verilerin korunması anayasal bir hak olarak tanımlanarak 2010 yılında yapılan anayasa değişikliği ile Anayasa'nın 20'nci maddesine eklenerek güvence altına alınmıştır. Özel hayatın gizliliği başlığı altında madde 20'ye eklenen fıkrayla kişilerin kendilerine ait verilerin korunması hakkını istemesi anayasal bir hak olarak güvence altına alınmıştır. İlgili düzenlemeye göre Anayasa'ya eklenen fıkra;

> *"Herkes, kendisiyle ilgili kişisel verilerin korunmasını isteme hakkına sahiptir. Bu hak; kişinin kendisiyle ilgili kişisel veriler hakkında bilgilendirilme, bu verilere erişme, bunların düzeltilmesini veya silinmesini talep etme ve amaçları doğrultusunda kullanılıp kullanılmadığını öğrenmeyi de kapsar. Kişisel veriler, ancak kanunda öngörülen hallerde veya kişinin açık rızasıyla işlenebilir. Kişisel verilerin korunmasına ilişkin esas ve usuller kanunla düzenlenir."* (T.C. Anayasası, Md. 20)

şeklinde düzenlenmiştir. Bu bağlamda kişisel verilerin işlenmesi ve korunmasının kanunda belirtildiği şekilde gerçekleştirilmesi gerektiği Anayasa'ya eklenmiştir. İlgili maddede belirtilen kişisel verilerin işlenmesi ve korunmasını güvence altına alacak bir yasal düzenleme, bu düzenlemenin Anayasa'ya eklendiği tarihte henüz TBMM'de görüşme aşamasında bulunmaktaydı ve daha önce de belirtildiği üzere yapılan anayasa değişikliğinden altı yıl sonra 2016 yılında kabul edilerek yürürlüğe girmiştir.

KVKK, sadece siber uzayda işlenen kişisel verilerin korunması kapsamında hazırlanmış bir kanun değildir. Kanun, kişilerin temel hak ve özgürlüklerinin korunması bağlamında oluşturulmuş ve özel hayatın gizliliği kapsamında anayasal bir hak olan kişisel verilerin korunması hakkını düzenleyen bir kanun olarak yürürlüğe girmiştir. Kanunun amacı *"kişisel verilerin işlenmesinde 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 düzenlemektir."* (6698 sayılı Kanun, Md. 1) olarak belirtilmiştir. Kanunun kapsamı 2'nci maddesinde *"kişisel verileri işlenen gerçek kişiler ile bu verileri tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla işleyen gerçek ve tüzel kişiler hakkında uygulanır."* (6698 sayılı Kanun, Md. 2) olarak açıklanmıştır. Bu maddeden de anlaşılacağı üzere, kanun hükümlerinin kısmen veya tamamen otomatik ya da otomatik olmayan veri işleme sistemlerinin parçası olarak belirtildiği üzere dijital ya da dijital olmayan her türlü veriyi işleyen gerçek ve tüzel kişiler üzerinde uygulanacağı belirtilmiştir. Dolayısıyla tezin konusu bağlamında değerlendirildiğinde 6698 sayılı Kanun'un sadece siber uzayın yasal olarak düzenlenmesi adına çıkartılmış bir kanun olduğunu söylemek mümkün değildir. Fakat günümüzde kişisel verilerin büyük çoğunluğunun dijital ortamlarda saklanarak işlendiği düşünüldüğünde, kanunun doğrudan siber uzayla alakalı olduğunu söylemek yanlış olmayacaktır. Ayrıca burada üzerinde durulması gereken bir diğer husus ise ilgili maddede kanun hükümlerinin gerçek ve tüzel kişiler üzerinde uygulanacağının belirtilmiş olmasına rağmen kamu veya özel sektör ayrımının yapılmamış olmasıdır (TBMM, 6698 sayılı Kanun Gerekçesi, 2016: s. 6). Kişisel verilerin son dönemde özel sektör kuruluşları tarafından yoğunlukla işlenerek farklı amaçlarla kullanıldığı düşünüldüğünde bu ayrımın yapılmamış olması oldukça önemlidir.

Kanun'da belirtilen "veri" kavramı daha önce 5651 sayılı Kanunda incelenen kavramdan farklı olarak kullanılmaktadır. 5651 sayılı Kanun'da veri kavramı, bilgisayar tarafından üzerinde işlem yapılabilen her türlü değer olarak tanımlanmıştır. 6698 sayılı KVKK'da belirtilen veri kavramı ise "bilgi" anlamında kullanılmıştır ve "kişisel bilgiler" olarak algılanması gerekmektedir. Kanunun 3'üncü maddesinde yapılan tanımlamalar bu bağlamda açıklayıcı niteliktedir. Kanunda kişisel veri, *"Kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgi."* (6698 sayılı Kanun, Md. 3-d) olarak tanımlanmaktadır. Bu tanımlamadan da anlaşılacağı üzere kanunda düzenlemesi yapılan kişisel verilerin hukuki boyutu sadece gerçek kişilere ait verilerdir. Kişisel verilerin işlenmesi ise;

> *"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 işlem."* (6698 sayılı Kanun, Md. 3-e)

şeklinde tanımlanmıştır. Kişisel veri, bireyleri tanımlayan her türlü bilgiyi ifade etmektedir. Dolayısıyla sadece kişilerin ad, soy ad, adres, doğum tarihi ve doğum yeri gibi bilgiler değil, aynı zamanda kişiyi tanımlamada kullanılabilecek ailevi bilgiler, dini tercihler, cinsel yönelimler, siyasi düşünceler, ekonomik bilgiler, sağlık bilgileri, eğitim bilgileri, hobiler, giyim tercihleri ve fiziki ayırt edici özellikler gibi her türlü bilgi kişisel veri dahilinde değerlendirilebilir özelliğe sahiptir. 6698 sayılı kanunun gerekçesinde de belirtildiği üzere;

> *"Bir kişinin belirli veya belirlenebilir olması, mevcut verilerin herhangi bir şekilde bir gerçek kişiyle ilişkilendirilmesi suretiyle, o kişinin tanımlanabilir hale getirilmesini ifade eder. Yani verilerin; kişinin fiziksel, ekonomik, kültürel, sosyal veya psikolojik kimliğini ifade eden somut bir içerik taşıması veya kimlik, vergi, sigorta numarası gibi herhangi bir kayıtla ilişkilendirilmesi sonucunda kişinin belirlenmesini sağlayan tüm halleri kapsar. İsim, telefon numarası, motorlu taşıt plakası, sosyal güvenlik numarası, pasaport numarası, özgeçmiş, resim, görüntü ve ses kayıtları, parmak izleri, genetik bilgiler gibi veriler dolaylı da olsa kişiyi belirlenebilir kılabilme özellikleri nedeniyle kişisel verilerdir."* (TBMM, 6698 sayılı Kanun Gerekçesi, 2016: s. 7).

Kanunun 4'üncü maddesinde kişisel verilerin ancak bu Kanun'da ve diğer kanunlarda öngörülen usul ve esaslara uygun olarak işlenebileceği belirtilmiştir. Bu bağlamda kişisel verilerin işlenmesinde genel ilkeler belirlenmiş ve verilerin

işlenmesinde hukuka ve dürüstlük kurallarına uygun olma, doğru ve gerektiğinde güncel olma, belirli, açık ve meşru amaçlar için işlenme, işlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma ve ilgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilme zorunlulukları getirilmiştir (6698 sayılı Kanun, Md. 4/2). Kanun'da kişisel verilerin işlenmesinde genel olarak ilgili kişinin açık rızasının olması gerektiği vurgulanmaktadır. İlgili kişinin açık rızası aranmadan verilerin işlenebilmesi durumu ise bazı şartlar dahilinde mümkündür. Bu şartlar ise Kanun'un 5'inci maddesinde;

> "*a) Kanunlarda açıkça öngörülmesi. b) Fiili imkânsızlık nedeniyle rızasını açıklayamayacak durumda bulunan veya rızasına hukuki geçerlilik tanınmayan kişinin kendisinin ya da bir başkasının hayatı veya beden bütünlüğünün korunması için zorunlu olması. c) Bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla, sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması. ç) Veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması. d) İlgili kişinin kendisi tarafından alenileştirilmiş olması. e) Bir hakkın tesisi, kullanılması veya korunması için veri işlemenin zorunlu olması. f) İlgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması."* (6698 sayılı Kanun, Md. 5/2)

olarak belirlenmiştir. Dolayısıyla Kanun'da belirtildiği üzere kişisel verilerin işlenmesi için ilgili kişinin açık rızasının aranmaması durumu kanunlarla açıkça öngörülmüş olmasının haricinde bir zorunluluk durumu teşkil etmesi durumunda mümkündür. Bu zorunluluk durumlarının neler olduğunun açıkça belirtilmiş olması ise kişisel verilerin keyfi olarak işlenmesinin önüne geçilmesi amacı taşımaktadır.

Kanunda ayrıca özel nitelikli kişisel veriler olarak tanımlanan verilerin işlenme şartları da düzenlenmiştir. Bu bağlamda özel nitelikli kişisel veriler 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 olarak belirlenmiş ve bu verilerin ilgili kişinin açık rızası olmadan işlenmesi yasaklanmıştır. Bahsi geçen özel nitelikli kişisel verilerden sağlık ve cinsel hayat dışındaki kişisel veriler kanunlarda öngörülmesi halinde kişilerin açık rızası aranmadan da işlenebilir. Sağlık ve cinsel hayata ilişkin kişisel veriler ise ancak kamu sağlığının korunması, koruyucu hekimlik, tıbbî teşhis, tedavi ve bakım hizmetlerinin yürütülmesi, sağlık hizmetleri ile finansmanının planlanması ve yönetimi amacıyla, sır saklama

yükümlülüğü altında bulunan kişiler veya yetkili kurum ve kuruluşlar tarafından ilgili kişinin açık rızası aranmadan işlenebilir (6698 sayılı Kanun, Md. 6).

Kanun'da ayrıca kişisel verilere ilişkin suçların hangi usullerde değerlendirilip hangi kanun hükümlerinin uygulanacağı da belirlenmiştir. Bu kapsamda kişisel verilere ilişkin suçlar 5237 sayılı TCK'nın 135 ila 140'ıncı madde hükümleri kapsamında değerlendirilerek cezalandırılacaktır. 6698 sayılı Kanun'un 7'nci maddesinde verilerin silinmesi ve anonim hale getirilmesi koşullarına aykırı olarak kişisel verileri silmeyen veya anonim hale getirmeyenlerin ise TCK'nın 138'inci maddesine göre cezalandırılacağı belirtilmektedir (6698 sayılı Kanun, Md. 18).

6698 sayılı KVKK kapsamında bu Kanunla verilen görevleri yerine getirmek üzere, idari ve mali özerkliğe sahip ve kamu tüzel kişiliğini haiz Kişisel Verileri Koruma Kurumu ve buna ek olarak kanunla verilen görev ve yetkilerini kendi sorumluluğu altında, bağımsız olarak yerine getirecek olan Kişisel Verileri Koruma Kurulu oluşturulmuştur. 6698 sayılı Kanun tüm bunlara ek olarak oluşturulan Kurum ve Kurulun görev ve yetkileri, çalışma esasları ve bu kurum ve kurullarda çalışacak personelin özlük haklarına ilişkin hükümler de dahil olmak üzere birçok detayı ele almıştır.

Günümüzde bireylere ait her türlü bilginin dijital ortamlarda saklandığı ve işlendiği göz önünde bulundurulduğunda KVKK, temel hak ve özgürlükler bağlamında kişisel verilerin korunması adına geç kalınmış olsa da oldukça önemli bir düzenlemedir. Gerçek hayatta yapılan resmi ve özel işlemlerin birçoğu artık internet üzerinden bilgisayarlar ya da akıllı telefonlar aracılığıyla gerçekleştirilebilmektedir. Bankacılık işlemleri, alışveriş, sağlık kuruluşlarında verilen her türlü test sonucu, mahkeme kararları, okul kayıtları, iş başvuruları, adres değişikliği bildirimi, vergi borçları bilgileri, vergi borçlarının ödenmesi ve buna benzer daha birçok işlem özellikle e-devlet uygulamaları sayesinde kolayca gerçekleştirilebilmektedir. Dolayısıyla tüm bu işlemlerin gerçekleştirilebilmesi için gerekli olan kişisel veriler de dijital olarak ilgili veri merkezlerinde saklanmaktadır. Bu bağlamda, bu sistemlere gerçekleştirilecek bir siber saldırı ile bu verilerin ele geçirilerek işlenmesi ve amacı dışında hukuksuz olarak kullanılması oldukça muhtemel bir tehlike olarak varlığını korumaktadır. Tüm bunlara ek olarak sosyal medya platformlarının kullanımının

artması ile bireylerin birçok kişisel verisi bu platformlarda görülebilmektedir. Bu veriler kişilerin rızası dışında işlenerek özellikle pazarlama ve satış stratejilerinin belirlenmesinde oldukça sıklıkla kullanılmaktadır. Ayrıca tüm bu veriler bir açık kaynak istihbaratı olarak da değerlendirilmelidir. Bir topluma ait yönelimler ve sosyokültürel yapı hakkında oldukça önemli bilgiler verebilecek olan bu verilerin kişilerin rızası dışında işlenerek bilgi üretilmesi teknolojinin geldiği noktada oldukça mümkündür. Bu bağlamda kişisel verilerin korunması her ne kadar kanunla koruma altına alınmış olsa da bireylerin bu konuda bilgilendirilmesi ve verilerini nasıl güvenli bir şekilde saklayabilecekleri konusunda bir farkındalık oluşturulması bir gereklilik olarak görülmelidir.

2.6. 3713 Sayılı Terörle Mücadele Kanunu

İnternet teknolojisine erişilebilirliğin artması ve aynı zamanda bilgisayar teknolojisinin durdurulamaz gelişimi ile git gide dijitalleşen dünyada gerçek hayatta işlenen birçok suç siber uzayda ya da siber uzayın getirdiği olanaklarla da işlenebilir hale gelmiştir. Terör suçları ise bu anlamda gerek siber uzayın sınırsızlığı, anonim olması, yakalanma ve kayıp verme riskinin düşük olması, maliyetlerinin oldukça düşük olması ve aynı zamanda eğitim, propaganda ve finans sağlama ihtiyaçlarının karşılanmasına etkili bir şekilde cevap verebilecek nitelikte olması sebebiyle terör örgütleri için eylemlerini daha az risk ve maliyetle daha etkili bir şekilde gerçekleştirebilecekleri bir alan haline dönüşmüştür. Terör faaliyetlerinin siber uzayda bilişim teknolojisinin beraberinde getirdikleriyle gerçekleştirilebileceğinin anlaşılması, siber uzay ve terörizm kavramlarını yan yana getirmiş ve siber terörizm olgusunun ortaya çıkmasını sağlamıştır. Özellikle IŞİD ve El-Kaide gibi uluslararası terör örgütlerinin internet teknolojisini oldukça aktif kullanarak eylemlerini gerçekleştirmede kendilerine avantaj sağlamaları, daha kolay bir şekilde finansman sağlamaları ve interneti bir propaganda aracı olarak kullanmaya başlamalarıyla birlikte siber terörizm kavramı önemini artırmıştır. Daha önce siber terörizm kısmında detaylı bir şekilde incelenen terörizm ve siber terörizm kavramlarının tanımları uluslararası bağlamda hala oldukça tartışmalı bir konudur.

Ülkemizde siber terör konusunu münferit olarak düzenleyen bir kanun bulunmamakla birlikte terörizm suçunu ve terörle mücadeleyi yasal olarak düzenleyen

kanun 12/04/1991 tarihli 3713 sayılı Terörle Mücadele Kanunudur (TMK). Kanun genel olarak incelendiğinde siber terör, siber terör eylemleri, potansiyel siber terör tehditleri ya da siber teröristler gibi konularda herhangi bir düzenleme içermemektedir. TMK, en son 2003 yılında 4928 sayılı Kanunla yapılan düzenlemeyle birinci bölümünde terörü;

> "*Terör; cebir ve şiddet kullanarak; baskı, korkutma, yıldırma, sindirme veya tehdit yöntemlerinden biriyle, Anayasada belirtilen Cumhuriyetin niteliklerini, siyasî, hukukî, sosyal, laik, ekonomik düzeni değiştirmek, Devletin ülkesi ve milletiyle bölünmez bütünlüğünü bozmak, Türk Devletinin ve Cumhuriyetin varlığını tehlikeye düşürmek, Devlet otoritesini zaafa uğratmak veya yıkmak veya ele geçirmek, temel hak ve hürriyetleri yok etmek, Devletin iç ve dış güvenliğini, kamu düzenini veya genel sağlığı bozmak amacıyla bir örgüte mensup kişi veya kişiler tarafından girişilecek her türlü suç teşkil eden eylemlerdir.*" (3713 sayılı TMK, Md.1)

şeklinde tanımlamaktadır. Her ne kadar terör kavramı TMK'da oldukça detaylı ve açıklayıcı bir şekilde tanımlanmış olsa da siber terör ya da siber terörist gibi kavramlarla ilgili herhangi bir tanımlama ya da bu suçlarla alakalı olarak bir düzenlemenin mevcut olmaması siber uzayda terörle mücadele bağlamında oldukça önemli bir eksiklik olarak değerlendirilmektedir.

Siber uzayın terör örgütleri tarafından artan bir şekilde kullanımının bilinen bir gerçek olmasına rağmen siber terörün tanımının yapılmamış olması ya da spesifik olarak siber terör suçlarıyla alakalı olarak herhangi bir düzenlemenin bulunmaması oldukça büyük bir eksiklik olarak değerlendirilebilir. Bu bağlamda bu alanda gerçekleştirilecek olan terör faaliyetleriyle yasal bir zeminde mücadele anlamında yapılan en yakın düzenleme 5237 sayılı TCK'da "Bilişim Alanında Suçlar" başlığı altında 243, 244, 245, 245/A ve 246. maddeleriyle yapılan düzenlemelerdir. 5532 sayılı Kanunla 2006 yılında yapılan değişiklikle TCK'nın 243 ve 244'üncü maddelerinde düzenlenen suçların TMK'nın 1'inci maddesinde belirtilen yani terör tanımında bulunan amaçlara ulaşmak doğrultusunda suç işlemek üzere kurulmuş bir terör örgütünün faaliyeti çerçevesinde işlendiği takdirde terör suçu sayılacağı belirtilmiştir (3713 sayılı TMK, Md. 4-a). Bu bağlamda TCK'nın 243'üncü maddesi olan "*Bilişim sistemine girme*" suçu ve 244'üncü maddede düzenlenen "*Sistemi engelleme, bozma, verileri yok etme veya değiştirme*" suçu kanunda yapılan terör tanımı içerisinde belirtilen amaçlar kapsamında yapıldığı takdirde bir terör suçu olarak

sayılabilecektir. Fakat ilgili bölümde düzenlenen "*Banka veya kredi kartlarının kötüye kullanılması*" (5237 sayılı TCK, Md. 245) ve "*Yasak cihaz ve programlar*" (5237 sayılı TCK, md 245/A) suçlarıyla ilgi terör suçuyla bağlantılı olarak herhangi bir düzenleme bulunmamaktadır.

TMK'da terör suçları TCK'nın 302, 307, 309, 311, 312, 313, 314, 315 ve 320'nci maddeleri ile 310 uncu maddesinin birinci fıkrasında yazılı suçlar olarak belirlenmiştir (3713 sayılı TMK, Md. 3). Buna ek olarak madde 4'de "*Terör amacı ile işlenen suçlar*" başlığı altında terör tanımında belirtilen amaçlar doğrultusunda suç işlemek üzere kurulmuş bir terör örgütünün faaliyeti çerçevesinde TCK'nın 79, 80, 81, 82, 84, 86, 87, 96, 106, 107, 108, 109, 112, 113, 114, 115, 116, 117, 118, 142, 148, 149, 151, 152, 170, 172, 173, 174, 185, 188, 199, 200, 202, 204, 210, 213, 214, 215, 223, 224, 243, 244, 265, 294, 300, 316, 317, 318 ve 319 uncu maddeleri ile 310 uncu maddesinin ikinci fıkrasında yer alan suçların işlenmesi durumunda bu suçların terör suçu sayılacağı belirtilmiştir (3713 sayılı TMK, Md. 4-a). Ayrıca 6136 sayılı "Ateşli Silahlar ve Bıçaklar ile Diğer Aletler Hakkında Kanun'da tanımlanan suçlar (3713 sayılı TMK, Md. 4-b), 6831 sayılı Orman Kanunu'nun 110'uncu maddesinin dördüncü ve beşinci fıkralarında tanımlanan "kasten orman yakma" suçları (3713 sayılı TMK, Md. 4-c), 4926 sayılı Kaçakçılıkla Mücadele Kanunu'nda tanımlanan ve hapis cezasını gerektiren suçlar (3713 sayılı TMK, Md. 4-ç), Anayasanın 120'nci maddesi gereğince olağanüstü hâl ilan edilen bölgelerde, olağanüstü halin ilanına neden olan olaylara ilişkin suçlar (3713 sayılı TMK, Md. 4-d) ve 2863 sayılı Kültür ve Tabiat Varlıklarını Koruma Kanunu'nun 68'inci maddesinde tanımlanan suç (3713 sayılı TMK, Md. 4-d) terör tanımında belirtilen amaçlar doğrultusunda suç işlemek üzere kurulmuş bir terör örgütünün faaliyet çerçevesinde işlendiği takdirde terör suçu sayılmaktadır.

TCK'da bahsi geçen terör suçu sayılan ve terör amacı ile işlendiği takdirde terör suçu olarak sayılacak olan suçları daha detaylı olarak belirtmek gerekirse bu suçlar başlıklarıyla birlikte şu şekildedir:

Terör Suçları:

- Devletin birliğini ve ülke bütünlüğünü bozmak suçu (5237 sayılı TCK, Md. 302).
- Askerî tesisleri tahrip ve düşman askerî hareketleri yararına anlaşma suçu (5237 sayılı TCK, Md. 307).
- Anayasayı ihlal suçu (5237 sayılı TCK, Md. 309).
- Cumhurbaşkanına suikast ve fiilî saldırı suçu (5237 sayılı TCK, Md.310/1). TMK'da bu maddenin birinci fıkrasındaki suç terör suçu olarak kabul edilmektedir. Birinci fıkra ise Cumhurbaşkanına suikast ve bu fiile teşebbüs etme suçu düzenlenmiştir.
- Yasama organına karşı suç (5237 sayılı TCK, Md. 311).
- Hükûmete karşı suç (5237 sayılı TCK, Md. 312).
- Türkiye Cumhuriyeti Hükûmetine karşı silâhlı isyan suçu (5237 sayılı TCK, Md. 313).
- Silahlı örgüt suçu (5237 sayılı TCK, Md. 314).
- Silah sağlama suçu (5237 sayılı TCK, Md. 315).
- Yabancı hizmetine asker yazma, yazılma suçu (5237 sayılı TCK, Md. 320).

Terör Amacı ile İşlenen Suçlar

- Göçmen kaçakçılığı suçu (5237 sayılı TCK, Md. 79).
- İnsan ticareti suçu (5237 sayılı TCK, Md. 80).
- Kasten öldürme suçu (5237 sayılı TCK, Md. 81).
- Nitelikli haller (5237 sayılı TCK, Md. 82).
- İntihara yönlendirme suçu (5237 sayılı TCK, Md. 84).
- Kasten yaralama suçu (5237 sayılı TCK, Md. 86).
- Neticesi sebebiyle ağırlaşmış yaralama suçu (5237 sayılı TCK, Md. 87).
- Eziyet suçu (5237 sayılı TCK, Md. 96).
- Tehdit suçu (5237 sayılı TCK, Md. 106).
- Şantaj suçu (5237 sayılı TCK, Md. 107).
- Cebir suçu (5237 sayılı TCK, Md. 108).
- Kişiyi hürriyetinden yoksun kılma suçu (5237 sayılı TCK, Md. 109).
- Eğitim ve öğretim hakkının engellenmesi suçu (5237 sayılı TCK, Md. 112).

- Kamu hizmetlerinden yararlanma hakkının engellenmesi suçu (5237 sayılı TCK, Md. 113).
- Siyasi hakların kullanılmasının engellenmesi suçu (5237 sayılı TCK, Md. 114).
- İnanç, düşünce ve kanaat hürriyetinin kullanılmasını engelleme suçu (5237 sayılı TCK, Md. 115).
- Konut dokunulmazlığının ihlali suçu (5237 sayılı TCK, Md. 116).
- İş ve çalışma hürriyetinin ihlali suçu (5237 sayılı TCK, Md. 117).
- Sendikal hakların kullanılmasının engellenmesi suçu (5237 sayılı TCK, Md. 118).
- Nitelikli hırsızlık suçu (5237 sayılı TCK, Md. 142).
- Yağma suçu (5237 sayılı TCK, Md. 148).
- Nitelikli yağma suçu (5237 sayılı TCK, Md. 149).
- Mala zarar verme suçu (5237 sayılı TCK, Md. 151).
- Mala zarar vermenin nitelikli helleri (5237 sayılı TCK, Md. 152).
- Genel güvenliğin kasten tehlikeye sokulması suçu (5237 sayılı TCK, Md. 170).
- Radyasyon yayma suçu (5237 sayılı TCK, Md. 172).
- Atom enerjisi ile patlamaya sebebiyet verme suçu (5237 sayılı TCK, Md. 173).
- Tehlikeli maddelerin izinsiz olarak bulundurulması veya el değiştirmesi (5237 sayılı TCK, Md. 174)
- Zehirli madde katma suçu (5237 sayılı TCK, Md. 185).
- Uyuşturucu veya uyarıcı madde imal ve ticareti suçu (5237 sayılı TCK, Md. 188).
- Kıymetli damgada sahtecilik suçu (5237 sayılı TCK, Md. 199).
- Para ve kıymetli damgaları yapmaya yarayan araçlar (5237 sayılı TCK, Md. 200).
- Mühürde sahtecilik suçu (5237 sayılı TCK, Md. 202).
- Resmî belgede sahtecilik suçu (5237 sayılı TCK, Md. 214).
- Resmî belge hükmünde belgelerde sahtecilik yapma suçu (5237 sayılı TCK, Md. 210).
- Halk arasında korku ve panik yaratmak amacıyla tehdit suçu (5237 sayılı TCK, Md. 213).
- Suç işlemeye tahrik etme suçu (5237 sayılı TCK, Md. 214).

- Suçu ve suçluyu övme suçu (5237 sayılı TCK, Md. 215).
- Ulaşım araçlarının kaçırılması veya alıkonulması suçu (5237 sayılı TCK, Md. 223).
- Kıt'a sahanlığında veya münhasır ekonomik bölgedeki sabit platformların işgali suçu (5237 sayılı TCK, Md. 224).
- Bilişim sistemine grime suçu (5237 sayılı TCK, Md. 243).
- Sistemi engelleme, bozma, verileri yok etme veya değiştirme suçu (5237 sayılı TCK, Md. 244).
- Görevi yaptırmamak için direnme (5237 sayılı TCK, Md. 265).
- Kaçmaya imkân sağlama (5237 sayılı TCK, Md. 294).
- Devletin egemenlik alametlerini aşağılama (5237 sayılı TCK, Md. 300).
- Suç için anlaşma (5237 sayılı TCK, Md. 316).
- Askerî komutanlıkların gasbı (5237 sayılı TCK, Md. 317).
- Halkı askerlikten soğutma (5237 sayılı TCK, Md. 318).
- Askerleri itaatsizliğe teşvik (5237 sayılı TCK, Md. 319).
- Cumhurbaşkanına fiilî saldırı (5237 sayılı TCK, Md. 310/2).

Yukarıda listelenen suçlardan TCK 243 ve 244'üncü maddelerde belirtilen suçların haricindeki suçlar doğrudan siber uzayla alakalı değildir. Lakin daha önce TCK'da siber uzayın güvenliğinin sağlanması ile alakalı olarak "Bilişim Teknolojileri Kullanarak veya Bu Teknolojiler Aracılığıyla İşlenen Suçlarla İlişkilendirilen ya da İlişkilendirilebilecek Maddeler" başlığı altında incelenen suçlar bağlamında değerlendirildiğinde bu suçlardan "İntihara yönlendirme suçu (5237 sayılı TCK, Md. 84), Şantaj suçu (5237 sayılı TCK, Md. 107), Eğitim ve öğretim hakkının engellenmesi suçu (5237 sayılı TCK, Md. 112), Nitelikli hırsızlık suçu (5237 sayılı TCK, Md. 142), Mala zarar verme suçu (5237 sayılı TCK, Md. 151), Para ve kıymetli damgaları yapmaya yarayan araçlar (5237 sayılı TCK, Md. 200), Mühürde sahtecilik suçu (5237 sayılı TCK, Md. 202), Resmî belgede sahtecilik suçu (5237 sayılı TCK, Md. 214), Suç işlemeye tahrik etme suçu (5237 sayılı TCK, Md. 214), Suçu ve suçluyu övme suçu (5237 sayılı TCK, Md. 215), Devletin egemenlik alametlerini aşağılama (5237 sayılı TCK, Md. 300), Halkı askerlikten soğutma (5237 sayılı TCK, Md. 318) ve Askerleri itaatsizliğe teşvik (5237 sayılı TCK, Md. 319)" suçlarının her ne kadar bilişim teknolojileri kullanarak veya aracılığıyla işlenmesi ile alakalı olarak herhangi bir

düzenleme olmamasına rağmen, bu suçlar siber uzayda bilişim teknolojileri aracılığıyla oldukça kolay bir şekilde işlenebilir niteliktedir. Dolayısıyla siber uzayda bu suçların vuku bulması halinde suçu işleyen kişilerin TMK'nın birinci maddesinde belirtilen terör tanımında geçen amaçları gerçekleştirmek doğrultusunda bu suçları işlediği durumlarda ortaya çıkan terör fiilinin siber terörizmle ilişkilendirilmesinin önünde bir engel yoktur. Fakat kanunlarımızda siber terörizm ile ilgili bir düzenleme bulunmaması ve siber terörizm diye bir suç düzenlemesinin mevcut olmaması sebebiyle bu suçlar terör suçu kapsamında ele alınarak gerekli soruşturma ve kovuşturma süreçleri yönetilecektir. Siber uzayın beraberinde getirdiği kolaylıkların farkında olan terör örgütleri ise bu alanı aktif bir şekilde kullanmakta ve operasyonel kapasitelerini genişletmektedirler. Bu bağlamda siber terörün kanunlarımızda münferit olarak düzenlenmemiş olması siber uzayın güvenliğinin sağlanmasında oldukça büyük bir eksiklik olarak değerlendirilmektedir.

2.7. Ulusal Siber Güvenlik Çalışmalarının Yürütülmesi, Yönetilmesi ve Koordinasyonuna İlişkin Bakanlar Kurulu Kararı

2012 yılında yayımlanan 2012/3842 sayılı "Ulusal Siber Güvenlik Çalışmalarının Yürütülmesi, Yönetilmesi ve Koordinasyonuna İlişkin Bakanlar Kurulu (BK) Kararı" Türkiye'de siber uzayın güvenliğinin sağlanmasında gerek kurumlar arası koordinasyonun sağlanması gerekse de bu konuda gerekli olan eğitim, yatırım ve altyapı faaliyetlerinin gerçekleştirilmesi adına oldukça önemli bir karar olarak karşımıza çıkmaktadır. Verilen bu karar ile Türkiye'de siber güvenliğin sağlanmasında kurumsal bazda koordinasyonun sağlanması görevi ile siber güvenliğin sağlanmasında ihtiyaç duyulan politikaların belirlenmesi, altyapının geliştirilmesi ve çözüm önerileri sunulması görevi 2011 yılında yayınlanan 655 Sayılı UDHB'nin Teşkilat ve Görevleri Hakkında Kanun Hükmünde Kararname'nin (KHK) ilgili maddeleriyle[20] de bağlantılı olarak UDHB'na verilmiştir.

[20] 655 Sayılı 655 Sayılı UDHB'nin Teşkilat ve Görevleri Hakkında Kanun Hükmünde Kararname'nin bu konudaki ilgili maddeleri "*Bakanlıkça teknik ve ekonomik gelişmelerin ortaya çıkardığı yeni ulaştırma, denizcilik, haberleşme, posta, evrensel hizmet, havacılık ve uzay teknolojileri iş, hizmet ve sistemleriyle ilgili olarak oluşturulacak politika ve stratejilerin tespitiyle ilgili çalışmalarda bulunmak, araştırma, inceleme ve değerlendirme yapmak üzere Bakanlık dışından bu alanlarda uzman kişiler ile faaliyet gösteren kuruluş temsilcilerinin katılımıyla görev süresi bir yılı geçmemek üzere geçici kurullar da oluşturabilir. Geçici kurulların görev süresi ihtiyaç halinde en fazla bir yıl ve bir kez uzatılabilir. Aynı anda en fazla iki adet geçici kurul çalıştırılabilir. Geçici kurullar, Bakanın doğrudan kendisinin*

Kararın giriş kısmında amaç ve kapsamı genel olarak kamu kurum ve kuruluşları tarafından bilgi teknolojileri kullanılarak verilen her türlü hizmet, işlem ve veri ile bunlarla bağlantılı olarak kullanılan sistemlerin güvenlik ve gizliliğinin sağlanması, bu konuyla ilgili gerekli tedbirlerin alınması ve bilgi iletişim teknolojilerine ilişkin kritik altyapıların işletiminde yer alan gerçek ve tüzel kişilerce uyulması gereken usul ve esasların düzenlenmesi şeklinde belirtilmiştir (2012/3842 sayılı BK Kararı). Siber uzayın güvenliğinin sağlanmasında izlenecek olan yol haritasının oluşturulması ve bu görevi yerine getirecek olan kurum ve kuruluşların görev ve yetkilerinin belirlenmesi anlamında değerlendirildiğinde oldukça kritik bir yerde duran bu karar, önceki kısımlarda incelenen kanunlarda siber güvenlik bağlamında yapılan yasal düzenlemelerin de önünü açmıştır.

Kararın beraberinde getirdiği en önemli yenilik 4'üncü maddede belirtilen bir "Siber Güvenlik Kurulu" oluşturulmasının kararlaştırılması olmuştur. Ayrıca siber güvenliğe yönelik ilkeler, teşkilat, görev ve sorumlulukları resmi olarak belirlenmiştir. İlgili madde siber güvenlik kurulunun oluşturulması kararını;

> *"Siber güvenlikle ilgili olarak alınacak önlemleri belirlemek, hazırlanan plan, program, rapor, usul, esas ve standartlar onaylamak ve bunların uygulanmasını ve koordinasyonunu sağlamak amacıyla; Ulaştırma, Denizcilik ve Haberleşme Bakanının başkanlığında Dışişleri, İçişleri, Milli Savunma, Ulaştırma, Denizcilik ve Haberleşme bakanlıkları müsteşarları, 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 oluşan Siber Güvenlik Kurulu kurulmuştur"* (2012/3842 sayılı BK Kararı, Md. 4).

şeklinde belirtmiştir. Siber güvenliğin sağlanmasına yönelik atılan en önemli adımlardan bir tanesi olan bu kararın ardından bakanlık ve kamu kurumlarının üst düzey yöneticilerinden oluşan 12 kişilik Siber Güvenlik Kurulu oluşturulmuştur.

Kararın 5'inci maddesi ise UDHB'na siber uzayın güvenliğinin sağlanması adına verilen görev ve yetkileri açıklamaktadır. Bu tarihe kadar siber güvenliğin

---

belirlediği konularda verdiği görevleri yerine getirirler." (Md. 29/7) ve *"Bakanlık, görev alanına giren konularla ilgili olarak çalışmalarda bulunmak üzere diğer bakanlıklar, kamu kurum ve kuruluşları, meslek odaları, sivil toplum kuruluşları, özel sektör temsilcileri ve konuyla ilgili uzmanların katılımıyla çalışma grupları oluşturabilir."* (Md. 30/1) şeklinde düzenlenmiştir.

sağlanmasıyla alakalı olarak görevlendirilmiş spesifik bir kurum veya kuruluşun bulunmaması, bu görevi kurumların kendi içlerinde oluşturdukları bilgi işlem daireleri aracılığıyla yürütmeye çalışıyor olmaları ve ulusal anlamda bir siber güvenlik stratejisinin bulunmaması eksiği UDHB'na verilen bu görev yetkilerle giderilmeye çalışılmıştır. Bakanlığa bu bağlamda ulusal siber güvenliğin sağlanması için gereken politika, strateji ve eylem planlarının hazırlanması, kamu kurum ve kuruluşlarına ait bilgi ve veri güvenliğinin sağlanmasında izlenecek olan usul ve esasların belirlenmesi, siber güvenliğin sağlanmasında ihtiyaç duyulan altyapı ve teknolojinin geliştirilmesi, kritik alt yapıların belirlenerek bu yapılara düzenlenebilecek potansiyel siber saldırı tehditlerinin belirlenmesi, önleme ve müdahale sistemleri ile bu konularla ilgili merkezlerin kurulması, ulusal siber güvenliğin sağlanmasında her türlü milli çözümlerin ve siber saldırılara müdahale araçlarının geliştirilmesi ve üretilmesini teşvik etmek, konuyla ilgili uzman personel temini yaparak eğitim ve gelişimini planlamak, siber güvenlikle ilgili olarak uluslararası alanda işbirliği çalışmaları yapmak, ulusal siber güvenlik konusunda bilinçlendirme, eğitim ve farkındalığı artırma çalışmaları yürütmek gibi önemli görev ve yükümlülükler verilmiştir (2012/3842 sayılı BK Kararı, Md. 5/1).

İlgili Bakanlar Kurulu Kararı oldukça karmaşık bir yapıya sahip olan siber uzayın bir o kadar karmaşık olan güvenliğinin sağlanması konusuyla ilgili gerekli olan koordinasyonun sağlanması, politika ve strateji üretilmesi, kurumlar arasında konuyla ilgili işbirliğinin oluşturulması, siber güvenlik konusunda eğitim politikalarının ve programlarının üretilmesi, siber güvenlik alanında farkındalığın oluşturulması ve her şeyden önemlisi siber güvenliğin teknolojinin geldiği noktada bir ulusal güvenlik meselesi olduğunun kabul edilmesi anlamında büyük önem taşımaktadır. Fakat tüm bu önemine rağmen kararda Türkiye'de siber uzayı düzenleyen tek ve kapsamlı bir yasal düzenleme oluşturulması adına bir adım atılmamış olması büyük bir eksiklik olarak değerlendirilmektedir. Ayrıca karar siber güvenliğin sağlanması için her ne kadar farkındalık oluşturmuş olsa da sonrasında karar kapsamında oluşturulan siber güvenlik kurulu ve yapılan yasal düzenlemeler siber uzayın sürekli değişen yapısına ayak uydurmakta zorlanmaktadır.

2.8. Kamu Kurum ve Kuruluşlarının KamuNet'e Dahil Edilmesi Hakkında Genelge

KamuNet Projesi, kamu kurum ve kuruluşları arasında gerçekleşen iletişim ve veri akışının daha güvenli bir siber ortamda gerçekleşmesini sağlamak amacıyla ortaya çıkmıştır. Bu bağlamda kamu kurum ve kuruluşları arasındaki iletişim ve veri akışının internete kapalı, fiziksel ve siber saldırılara karşı daha güvenli sanal bir ağ üzerinden gerçekleştirilmesi planlanmıştır. 5809 sayılı Elektronik Haberleşme Kanunu, 2012/3842 sayılı Ulusal Siber Güvenlik Çalışmalarının Yürütülmesi, Yönetilmesi ve Koordinasyonuna İlişkin Bakanlar Kurulu Kararı ve 2013-2014 Ulusal Siber Güvenlik Stratejisi ve Eylem Planı kapsamında oluşturulan Siber Güvenlik Kurulu kararları çerçevesinde

> "*...kamu kurum ve kuruluşları arasındaki veri iletişiminin kamu tarafından yeni güvenli bir altyapı sağlanıncaya kadar, kurumlar arası veri iletişiminin, internete kapalı, fiziksel ve siber saldırılara karşı daha güvenli sanal bir ağ üzerinden yapılarak siber güvenlik risklerinin azaltılması, kurumlar arasında iletişimde standart sağlanması, ortak uygulamalar için uygun alt yapının oluşturulması, planlanan ortak veri merkezi/merkezlerinin dahil edilmesi, e-Devlet uygulamalarının güvenli olarak ortak kullanılabilmesi, kamu kurumları arasında mevcut durumda internet üzerinden gerçekleştirilen bulut uygulamalarının internetten bağımsız daha güvenli olarak sağlanması amacıyla Kamu Sanal Ağı (KamuNet)'nın kurulmasına"*

karar verilmiştir (Resim Gazete, 2016/28 sayılı Genelge). KamuNet'in kurulmasına dair "KamuNet İş birliği Protokolü" ise 25 Şubat 2015 tarihinde Ulaştırma ve Altyapı Bakanlığı ile Türk Telekomünikasyon A.Ş. arasında imzalanmıştır (UAB, 2015).

KamuNet projesi kamu kurum ve kuruluşları arasında gerçekleştirilen iletişim ve veri akışında güvenliğin sağlanması adına oldukça önemli bir projedir. Siber uzayda internete erişimi olan her cihazın meydana gelebilecek siber saldırılara maruz kalabileceği gerçeği özellikle kamu kurum ve kuruluşlarının bu konuda daha dikkatli ve hazırlıklı olmasını gerektirmektedir. Dolayısıyla internete kapalı ve sadece ilgili kuruluşların kendi aralarında oluşturduğu bir kapalı ağ sistemi üzerinden iletişim ve veri akışını sağlayacakları temeline dayanan KamuNet sanal ağı, siber uzayda kamu kurum ve kuruluşlarının uğrayacağı siber saldırılara karşı alınacak nemli bir tedbir uygulamasıdır.

2.9. KamuNet Ağına Bağlanma ve KamuNet Ağının Denetimine İlişkin Usul ve Esaslar Hakkında Tebliğ

Kamu kurum ve kuruluşları arasındaki iletişim ve veri akışının daha güvenli bir şekilde gerçekleştirilebilmesi amacıyla oluşturulan KamuNet Ağına ya da diğer adıyla Kamu Sanal Ağına bağlanacak olan kurumlar için asgari şartların belirlenmesi amacıyla yayınlanan 30103 sayılı KamuNet Ağına Bağlanma ve KamuNet Ağının Denetimine İlişkin Usul ve Esaslar Hakkında Tebliğ, 5809 sayılı Elektronik Haberleşme Kanunu'na dayanarak hazırlanmıştır. Tebliğe göre KamuNet ağına bağlanacak olan kurum ve kuruluşların "*bilginin gizliliğini, bütünlüğünü ve erişilebilirliğini sağlamak üzere; sistemli, kuralları koyulmuş, planlı, yönetilebilir, sürdürülebilir, dokümante edilmiş, kurumun yönetimince kabul görmüş ve uluslararası güvenlik standartlarının temel alındığı faaliyetler bütünü"* olarak tanımlanan Bilgi Güvenliği Yönetim Sistemi (BGYS) kurması zorunlu kılınmıştır (Resmî Gazete, 30103 sayılı Tebliğ: Md. 4/1-a). Ayrıca kurulacak olan BGYS'nin hangi standartları sağlaması gerektiği ve alınması gereken belgelerin hangi akreditasyon kurumlarından temin edileceği de belirtilmiştir. Bu bağlamda değerlendirildiğinde her kurumun kendi BGYS'sini oluşturması ve bunu belirli standartlar dahilinde gerçekleştirecek olması öncelikle KamuNet Ağının daha sağlıklı ve kesintisiz bir şekilde işlemesine yardımcı olacak ve aynı zamanda siber tehditlere karşı daha kurumların daha hazırlıklı ve donanımlı olmasını sağlayacak bir gelişmedir.

Tebliğ aynı zamanda KamuNet'e bağlanacak olan kurum ve kuruluşlarda çalışan personelin BGYS ve siber güvenlik hakkında bilgilendirme ve eğitimlere tabi tutulmasını, ortaya çıkabilecek siber tehditlere karşı KamuNet ağının güvenliğinin sağlanması amacıyla önlemlerin alınmasını, KamuNet ağının olumsuz etkilenmemesi adına kullanılan modem ve cihazların güncel tutulması gerektiği ve verilerin yedeklenmesi zorunluluğunu da getirmiştir. Kısacası tebliğ, KamuNet Ağına bağlanacak olan kuruluşların bu ağın güvenliğinin sağlanması adına alması gereken önlemleri ve yapılması gerekenleri sıralamıştır. KamuNet'e dahil olacak kurum ve kuruluşların denetlenmesi görevi ise UDHB'ye verilmiştir (Resmî Gazete, 30103 sayılı Tebliğ).

KamuNet Ağı projesi daha önce de belirtildiği üzere kamu kurum ve kuruluşları arasındaki iletişim ve veri akışının güvenliği bağlamında oldukça önemli ve gerekli bir proje olarak değerlendirilmektedir. Burada dikkat edilmesi gereken konu ise her ne kadar bu ağı güvenli ve internete erişimin olmadığı kapalı devre bir ağ olsa da bu ağa bağlanacak olan kurum ve kuruluşlarda çalışan personele siber güvenlik ile ilgili yeteri kadar eğitim ve bilgilendirme yapılmadığı sürece hiçbir zaman tam anlamıyla güvenli olmayacaktır. Unutulmamalıdır ki siber güvenliğin en zayıf halkasını oluşturan unsur insan unsurudur. Dolayısıyla 30103 sayılı tebliğde de belirtildiği üzere BGYS ve siber güvenlik hakkında KamuNet Ağına bağlanacak olan kurum ve kuruluşlarda çalışan tüm personelin bu konunun ciddiyeti ve ulusal güvenliğin sağlanmasında ne kadar önemli olduğu yapılacak eğitimlerle anlatılmalıdır. Ayrıca periyodik olarak personelin ağın güvenliğinin sağlanması adına uyulması gereken kurallara ne derece uyduğu kontrol edilmeli ve gerekirse konuyla ilgili uyarılar yapılmalıdır.

2.10. 2019/12 Sayılı Bilgi ve İletişim Güvenliği Tedbirleri Hakkında Cumhurbaşkanlığı Genelgesi

Bilgi ve iletişim teknolojilerinin artan kullanımı ve dijitalleşmenin hız kazanmasıyla birlikte ortaya çıkan yeni tehditler ve güvenlik riskleri, ulusal güvenliğin tam anlamıyla sağlanabilmesi adına siber uzayda güvenliğin sağlanmasını gerekli kılmıştır. Yapılan yasal düzenlemeler, oluşturulan yeni kurumlar ve alınan önlemler bu bağlamda oldukça büyük önem taşımaktadır. Bu minvalde 2019 yılında Cumhurbaşkanlığı tarafından yayınlanan "Bilgi ve İletişim Güvenliği Tedbirleri Hakkında Genelge" ile dijital ortamlarda bilginin güvenliğinin sağlanması adına alınacak tedbirler belirtilmiştir.

Genelgeye göre kritik olan nüfus, sağlık ve iletişim kayıt bilgilerinin internete kapalı ve fiziksel olarak güvenliği sağlanmış olan ağlarda depolanması, kamu kurum ve kuruluşlarında bulunan ve kritik öneme sahip verilerin yine aynı şekilde internete kapalı ve fiziksel olarak güvenliği sağlanmış ağlarda tutulması gerektiği belirtilmiştir. Ayrıca bu verilerin kurumların kendi özel sistemleri haricinde bulut sistemlerinde depolanmaması gerektiği de vurgulanmıştır. Genelge ayrıca günümüzde hemen herkesin akıllı telefonlar aracılığıyla kullandığı mobil uygulamalar üzerinden veri

paylaşımını yasaklamıştır. Genelgenin üzerinde durduğu diğer bir önemli konu ise sosyal medya platformları üzerinden gizlilik dereceli veri paylaşımının ve haberleşmenin yapılmasının yasaklanması olmuştur (Resmî Gazete, 2019/12 sayılı Genelge, 2019).

Genelgenin getirmiş olduğu bir diğer önemli tedbir ise kritik veri ve belgelerin bulunduğu ve/veya görüşmelerin yapıldığı çalışma odalarında ya da ortamlarda mobil cihaz ve veri transferi özelliğine sahip cihazların bulundurulamayacağı hükmüdür. Hemen herkesin kullandığı ve internet erişimi olan akıllı telefonlar aynı zamanda hem bir fotoğraf makinesi hem de bir veri aktarım cihazı olarak kullanılabilmektedir. Dolayısıyla alınan bu tedbir milli güvenliği tehlikeye sokacak bilgi ve belgelerin güvenliğinin ve gizliliğinin sağlanması adına oldukça önemlidir (Resmî Gazete, 2019/12 sayılı Genelge, 2019).

Genelge aynı zamanda kaynağından emin olunmayan her türlü veri depolama cihazının kullanımını da yasaklamaktadır. Bilgi ve iletişim güvenliği açısından hayati önem taşıyan kriptolama sistemlerinin milli imkanlarla geliştirilmesi adına teşviklerin sağlanacağını belirten genelge bu bağlamda geliştirilecek olan yazılımların güvenli bir şekilde geliştirilmesi adına tedbirler alınacağını da belirtmektedir. Kamu kurum ve kuruluşlarında personelin siber güvenlik eğitimlerinden geçirilmesinin gerekliliğiyle birlikte sistemlere erişimin üst düzey yöneticiler de dahil olmak üzere yetkilendirilmiş kişiler tarafından yapılacağı kuralı genelge de vurgulanan diğer bir önemli konudur (Resmî Gazete, 2019/12 sayılı Genelge, 2019).

Milli güvenliğin sağlanmasında oldukça büyük önem taşıyan endüstriyel kontrol sistemlerinin siber güvenliğinin sağlanması konusu üzerinde de duran genelge, endüstriyel kontrol sistemlerinin internete erişiminin kapatılmasını, internete erişimin zorunlu olduğu hallerde ise gerekli güvenlik tedbirlerinin alınması gerektiğini belirtmiştir. Genelgede kamu e-posta adreslerinin güvenlik ayarlarının yapılması gerektiği, kamu personelinin kurumsal olmayan şahsi e-posta adresleri ile kurumsal iletişim yapamayacağı, kritik veri iletişiminde sadece fiber optik kablolar ile oluşturulmuş ağların kullanılacağı fakat zorunlu hallerde bu ağların dışında kullanılacak yöntemlerde milli kriptolama cihazları kullanılarak kritik veri iletişiminin gerçekleştirileceği belirtilmiştir (Resmî Gazete, 2019/12 sayılı Genelge, 2019).

Genelge, son kısmında kamu kurum ve kuruluşları ile kritik altyapı niteliğinde hizmet veren işletmelerde uygulanmak üzere farklı güvenlik seviyeleri içeren Bilgi ve İletişim Güvenliği Rehberi hazırlanmasını öngörmüştür. Hazırlanacak olan rehberin Cumhurbaşkanlığı Dijital Dönüşüm Ofisi (CBDDO) tarafından hazırlanacağını belirtilen genelgede bu rehberin gelişen teknolojiler ile Ulusal Siber Güvenlik Stratejisi ve Eylem Planlarında yapılacak olan değişiklikler göz önünde bulundurularak güncelleneceği de belirtilmiştir.

Genelge kapsamında hazırlanması öngörülen Bilgi ve İletişim Güvenliği Rehberi CBDDO tarafından 2020 yılında hazırlanarak onaylanmıştır. Oldukça kapsamlı bir şekilde hazırlanan rehberde ağ ve sistem güvenliği, uygulama ve veri güvenliği, taşınabilir cihaz ve ortam güvenliği, nesnelerin interneti cihazlarının güvenliği, personel güvenliği, fiziksel mekanların güvenliği, kişisel verilerin güvenliği, anlık mesajlaşma güvenliği, bulut bilişim güvenliği, kripto uygulamaları güvenliği ve kritik altyapılar güvenliği konuları detaylı bir şekilde ele alınarak bu konularda güvenliğin sağlanmasında yapılması gerekenler ve alınacak tedbirler açıklanmıştır (CBDDO, Bilgi ve İletişim Güvenliği Rehberi, 2020).

3. SİBER GÜVENLİK STRATEJİSİ VE EYLEM PLANLARI

3.1. Ulusal Siber Güvenlik Stratejisi (USGS) ve 2013-2014 Eylem Planı

2012 yılında 2012/3842 sayılı "Ulusal Siber Güvenlik Çalışmalarının Yürütülmesi, Yönetilmesi ve Koordinasyonuna İlişkin Bakanlar Kurulu Kararı" ile UDHB başkanlığında kurulan "Siber Güvenlik Kurulu" tarafından siber uzayda güvenliğin sağlanmasına yönelik atılan en önemli adımlardan bir tanesi olan "Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı" (UDHB, 2012) 2012 yılında kabul edilerek yayımlanmıştır. Bu plan kapsamında ulusal siber güvenlik politikalarında alınması gereken önlemler ve yapılması elzem olan yasal düzenlemeler ile siber caydırıcılığın oluşturulmasına yönelik atılması gereken adımlar belirlenmiştir. Ayrıca Ulusal Siber Olaylara Müdahale Merkezi'nin (USOM) oluşturulması ile Siber Olaylara Müdahale Ekipleri'nin (SOME) faaliyete başlaması da kararlaştırılmıştır.

Türkiye'nin siber güvenlik alanında ilk defa hazırladığı bu eylem planında bilgi ve iletişim sistemlerinin kullanımının arttığı ve kurumların yanı sıra kritik altyapıların kontrollerinde bilgi ve iletişim sistemlerinin kullanımının hayati olduğu vurgulanmıştır.

2013-2014 Eylem Planının amacı, kamu kurum ve kuruluşlarının siber uzayda kullandığı her türlü bilgi işlem sisteminin güvenliğinin sağlanması, kritik altyapılara ait bilişim sistemlerinin güvenliğinin sağlanması ve siber güvenlik olaylarının daha aktif bir şekilde araştırılarak en düşük düzeyde kalmasının sağlanarak stratejik siber güvenlik eylemlerinin belirlenmesi olarak bildirilmiştir. Bu bağlamda yasal düzenlemelerin yapılması, siber olayların nitelendirilmesi, kritik altyapılarda bilgi güvenliği yönetimi programının uygulanması, siber güvenlik eğitim altyapısının güçlendirilmesi, siber güvenlik tatbikatlarının düzenlenmesi, siber güvenlik konusunda akademisyen yetiştirilmesi gibi 29 ayrı eylem belirlenmiştir (USGS ve 2013-2014 Eylem Planı, 2012).

Türkiye'nin siber uzayda güvenliğin sağlanması adına hazırladığı bu ilk eylem planında siber ortam, ulusal siber ortam, kritik altyapılar, siber güvenlik ve ulusal siber güvenlik gibi kavramların tanımlarına da yer verilmiştir. Bu bağlamda siber ortam genel bir tanımlamayla tüm dünyada ve uzaya yayılmış durumda bulunan bilişim sistemlerinden ve bunları birbirine bağlayan ağlardan oluşan ortam olarak tanımlanmıştır. Ulusal siber ortam ise kamu bilişim sistemleri ile gerçek ve tüzel kişilere ait bilişim sistemlerinden oluşan ortam olarak tanımlanmıştır. Yapılan bu tanımlarda dikkat çeken unsur ise yapılan tanımların detaylı bir şekilde yapılmadığı, bunun yerine en genel şekliyle yapılan tanımlar olmasıdır. Ulusal siber güvenlik konusunda hayati öneme sahip kritik altyapılar için yapılan tanım da bu yapıların neler olduğunu vurgulamak yerine genel anlamda işlediği bilginin gizliliği, bütünlüğü veya erişilebilirliği bozulduğu takdirde can kaybına, büyük ölçekli ekonomik zarara ve ulusal güvenlik açıklarına veya kamu düzeninin bozulmasına sebep olabilecek bilişim sistemlerini barındıran altyapılar olarak tanımlanmıştır. (USGS ve 2013-2014 Eylem Planı, 2012: 2-3).

Belgede aynı zamanda ilk defa resmi olarak siber güvenlik kavramının tanımı da yapılmıştır. Yapılan bu tanıma göre siber güvenlik, "*siber uzayı oluşturan bilişim*

sistemlerinin saldırılardan korunması, bu ortamda işlenen bilginin gizlilik, bütünlük ve erişilebilirliğinin güvence altına alınması, saldırıların ve siber güvenlik olaylarının tespit edilmesi, bu tespitlere karşı tepki mekanizmalarının devreye alınması ve sonrasında ise sistemlerin yaşanan siber güvenlik olayı öncesi durumlara geri döndürülmesi" şeklinde tanımlanmıştır. (USGS ve 2013-2014 Eylem Planı, 2012: s. 3). Yapılan bu tanım her ne kadar kapsayıcı olarak görünüyor olsa da siber tehditlerin neler olduğu, ortaya çıkabilecek saldırı türleri ve bu saldırılar meydana geldiği takdirde alınacak önlemler gibi detaylara yer verilmemiş olması ve bu bağlamda atılması gereken adımların neler olduğunun üzerinde durulmamış olması bir eksiklik olarak değerlendirilebilir.

Belgede aynı zamanda siber güvenlik stratejisinin gelişen teknoloji ve şartlara ayak uydurulması amacıyla yılda en az bir kere olmak üzere kamu ve özel sektörden gelecek talepler doğrultusunda güncelleneceği belirtilmiştir (USGS ve 2013-2014 Eylem Planı, 2012: 4). Siber uzayın sürekli değişen yapısı ve bilişim teknolojilerinin günden güne gelişmesi sebebiyle ulusal siber güvenlik stratejilerinin de bu değişim ve gelişime ayak uydurması zorunluluğunun üzerinde durulmuş olması oldukça önemlidir. Fakat ilk defa 2012 yılında 2013-2014 yıllarını kapsayacak şekilde hazırlanan eylem planı daha sonrasında 2015 yılında 2016-2019 ve 2020-2023 için dört senelik planlar olmak üzere hazırlanarak yayımlanmıştır. Bu bağlamda siber uzay için dört sene oldukça uzun bir süredir. Günden güne değişen ve gelişen bilişim teknolojisi alanında ortaya çıkan yeni bir ürün, yazılım ya da olay çok kısa bir süre içerisinde demode olabilmekte ve ortaya çıkan yeni teknolojiler bir önceki teknolojiden çok daha üstün özellik ve kapasitelere sahip olabilmektedir. Ayrıca hazırlanan ilk eylem planı ve strateji belgesinden sonra bir yıllık süreler içerisinde güncellenmesi kararı alınmış olmasına rağmen sonrasında dörder yıllık eylem planları ve stratejilerin hazırlanmış olması ulusal siber güvenliğin sağlanmasında istikrarsız bir yönetim anlayışının bir göstergesi olarak kabul edilebilir

Belgenin önemli olan bir diğer kısmı ise siber güvenlik konusunda en doğru adımların atılması adına siber güvenlik risklerinin neler olduğunun belirtilmiş olmasıdır. Bu bağlamda siber uzayın anonimliği, saldırıları düzenleyenlerin yakalanma risklerinin düşük olduğu, saldırganlar için maliyetsiz olması ve coğrafi olarak sınırlamaların bulunmaması, siber uzayı oluşturan sistemlerin ağlarla birbirine

bağlı olması nedeniyle ortaya çıkabilecek bir güvenlik tehdidinin tüm bilişim sistemlerine zarar verebilme potansiyelinin bulunduğu, kritik altyapıların bir çoğunun bilişim sistemleri tarafından kontrol ediliyor olması ve internete bağlı olması nedeniyle siber saldırı risklerine açık olması, siber uzayı düzenleyen yasal düzenlemelerin yetersiz olması, gerek kurumlarda gerekse de kritik altyapılarda siber güvenlik için gerekli altyapıya sahip olunmaması, yapılanmanın eksikliği, çalışanların siber güvenlik konusunda yeteri kadar bilgi ve tecrübeye sahip olmaması ve bu konuda yetişmiş personel eksikliği konuları siber güvenlik riskleri olarak belirlenmiştir. Bir öz eleştiri niteliğinde sıralanan bu riskler siber uzayın güvenliğinin sağlanması noktasında atılması gereken adımların belirlenebilmesi açısından oldukça önemlidir. Bu bağlamda ulusal siber güvenliğin sağlanmasında sıralanan genel ilkeler ise ortaya konulan riskler temelinde ele alınarak bu risklerin ve eksikliklerin giderilmesi üzerine oluşturulmuştur. Siber güvenliğin sağlanmasında takip edilecek ilkelere bakıldığında siber güvenliğin sağlanmasında kamu ve özel sektör işbirliğinin gerekliliğinin, uluslararası anlaşmalara uyulması gerekliliği ve uluslararası işbirliğinin öneminin, hukukun üstünlüğü ve temel insan hak ve hürriyetleri ile mahremiyetin korunmasının temel esas olarak kabul edilmesinin, siber uzayda şeffaflık, hesap verilebilirlik, etik değerler ve ifade özgürlüğünün desteklendiğinin vurgulanması ise bu alanda güvenliğin sağlanmasında izlenecek olan yolun hukukun üstünlüğü temelinde gerçekleştirilmesi gerektiğinin altının çizilmesi anlamında oldukça önemlidir (USGS ve 2013-2014 Eylem Planı, 2012: 4-6).

Siber güvenliğin toplumun huzur ve refahı, ekonomik kalkınma, istikrar ve ulusal güvenliğin sağlanmasındaki stratejik önemini vurgulayan belge, siber güvenliğin sağlanmasında belirlediği ilkeler çerçevesinde 2013-2014 dönemi için izlenecek stratejik siber güvenlik eylemlerinin neler olacağını da sırlamıştır. Bu bağlamda kurum ve kuruluşların siber güvenliğin sağlanmasında görev, yetki ve sorumluluklarının belirlenmesi ve ihtiyaç duyulan alanlarda yasal düzenlemelerin yapılması adına gerekli çalışmaların başlatılacağı, uluslararası hukuka bağlı kalınarak adli süreçlere yardımcı olacak çalışmaların yürütülmesi, ulusal siber olaylara müdahale organizasyonunun oluşturulması, ulusal siber güvenlik altyapısının güçlendirilmesi, siber güvenliğin sağlanmasında ihtiyaç duyulan personelin yetiştirilmesinin sağlanması ve bilinçlendirme faaliyetlerinin eğitim sisteminin her

seviyesinde olmak üzere başlatılması adına çalışmaların yapılması, siber güvenliğin sağlanmasında yerli teknolojilerin geliştirilmesi ve kullanılmasına teşvik edilmesi ve ulusal güvenlikten sorumlu kurumların faaliyetlerini siber uzayı da kapsayacak şekilde genişletmesi adına çalışmaların başlatılacağı belirtilmiştir (USGS ve 2013-2014 Eylem Planı, 2012: 6-8).

Bahsi geçen stratejik eylemlerden ulusal siber olaylara müdahale organizasyonunun oluşturulması, siber uzayda ulusal güvenliğin sağlanması ve uluslararası alanda siber güvenlik ile ilgili gelişmelerin takip edilerek ortaya çıkabilecek siber tehditlere yerinde, zamanında ve doğru bir şekilde müdahale edilebilmesi, saldırıların durdurulması ve saldırı sonrasında sistemlerin en az zararla eski haline döndürülebilmesi adına oldukça önemlidir. Bu bağlamda yedi gün yirmi dört saat esasına göre çalışacak "Ulusal Siber Olaylara Müdahale Merkezi (USOM)" kurulması ve bu merkezin koordinasyonunda çalışacak olan sektörel "Siber Olaylara Müdahale Ekiplerinin (SOME)" kurulması kararlaştırılmıştır (USGS ve 2013-2014 Eylem Planı, 2012: 7-10).

Belge, 2013-2014 dönemi için hazırlamış olduğu siber güvenlik eylem planında 29 adet eylem maddesi belirlemiş ve bu maddelerde eylemin ne olduğu, bu eylem kapsamında gerçekleştirilecek alt eylemler, eylemin bitirileceği tarih ve bu eylemden sorumlu ve ilgili kuruluşları sıralamıştır. Yukarıda belirtilen ilkeler çerçevesinde hazırlanan stratejik eylemler kapsamında hazırlanan eylem planında bu stratejilere ek olarak, siber olayların delillendirilmesi noktasında gerekli olan bilgi ve teknolojiye sahip olunması adına çalışmaların başlatılması, kritik altyapıların siber uzaydaki güvenliğinin sağlanması adına bilgi güvenliği yönetimi programının uygulanması, siber güvenlik eğitim altyapısının güçlendirilerek teknik personel eğitilmesi, siber güvenlik tatbikatlarının düzenlenmesi, Türk Dil Kurumu (TDK) siber güvenlik terimleri sözlüğünün oluşturulması, kamu güvenli iletişim kurallarının belirlenmesi, yazılım güvenliği programının yürütülmesi, siber güvenlik konusunda akademisyen yetiştirilmesi, üniversitelerde siber güvenlik eğitimlerinin yaygınlaştırılması, ulusal ve uluslararası siber güvenlik etkinliklerinin düzenlenmesi, siber güvenliğin sağlanmasında yerli ürün ve çözüm çalışmalarının yapılması ve teşviki ile bunlardan belki de en önemlisi olan ulusal siber güvenliğin milli güvenliğe

entegrasyonunun sağlanması noktasında gerekli adımların atılmasının gerekliliği üzerinde durulmuştur (USGS ve 2013-2014 Eylem Planı, 2012: 10-30).

USGS ve 2013-2014 Eylem Planı Türkiye'nin ulusal siber güvenlik stratejilerinin ve bu anlamda atılması gereken adımların belirlenmesinde oldukça önemli bir belgedir. Her ne kadar kapsamının sınırlı olması ve bahsi geçen eylemlerin gerçekleştirilmesi anlamında belirlenen sürenin gerçekçi olmaması, siber güvenlik farkındalığının oluşturulması, gerekli yasal ve yönetsel düzenlemelerin başlatılması, konuyla ilgili eğitim politikalarının geliştirilmesi ve eylem planının son maddesinde belirtildiği üzere ulusal siber güvenliğin milli güvenliğe entegrasyonunun sağlanması adına kritik öneme sahip bir belge olarak değerlendirilmektedir.

3.2. 2016-2019 Ulusal Siber Güvenlik Stratejisi ve Eylem Planı

2013-2014 Eylem Planının ardından 2016 yılında UDHB koordinasyonunda 2016-2019 Ulusal Siber Güvenlik Stratejisini açıklanmıştır (UDHB, 2016). Türkiye'nin siber güvenlik stratejisi bağlamında izleyeceği yolu belirleyen bu çalışma ise siber uzayın güvenliğinin sağlanmasının ve yasal düzenlemelerin getirilmesinin gerekliliğini bir kez daha ortaya koymuş ve bu anlamda siber güvenlik stratejilerinin belirlenmesinin bir ulusal güvenlik önceliği olduğunu vurgulamıştır. 2016-2019 Ulusal Siber Güvenlik Stratejisi ve Eylem Planı belgesi siber uzayda geçekleştirilen saldırıların konvansiyonel saldırılarla kıyaslandığında saldırıyı gerçekleştirenler için anonimlik ve inkâr edilebilirlik gibi fırsatların var olduğunu vurgulamış ve bu durumun siber uzayda güvenliğin sağlanmasının daha da karmaşık hale getirdiğini ve tehditlerle mücadelenin zorlaştığını bildirmiştir. Bu durum, siber uzayın karmaşıklığının ve bu alanda güvenliğin sağlanmasının ne kadar önemli olduğunun anlaşılması bakımından oldukça önemli bir adım olarak değerlendirilebilir. 2016-2019 USGS ve Eylem Planı çalışmasının amacı "*Siber güvenliğin, gizliliğin ve mahremiyetin sağlanmasında kritik teknolojilerin ve ürünlerin ülkemizde üretilmesine, üretilemiyorsa, dışarıdan alınan teknoloji ve ürünlerin salt bu maksatla ve güvenle kullanılabilmesini sağlayacak önlemlerin alınmasına yönelik bileşenler bu planda yer almaktadır.*" (2016-2019 USGS ve Eylem Planı, 2016) olarak tanımlanmıştır. Bu durum, siber uzayı oluşturan teknolojilerin neredeyse tamamının ithal edildiği

düşünüldüğünde bu farkındalığın oluşturulması ve bu yönde güvenlik çalışmalarının yapılması bağlamında oldukça önemlidir (2016-2019 USGS ve Eylem Planı, 2016: 9).

2016-2019 USGS ve Eylem Planında, 2013-2014 dönemi için hazırlanan eylem planı üzerinde durulan siber güvenlik stratejileri ve eylem planında belirtilen konular üzerinde tekrar durulmuş ve bazı eklemeler yapılmıştır. Ayrıca daha önce siber ortam olarak tanımlanan kavram bu çalışmada siber uzay olarak belirtilmiş ve daha önce genel olarak yapılan kritik altyapılar bu belgede yine aynı şekilde tanımlanmakla beraber ek olarak kritik altyapı sektörlerinin neler olduğu üzerinde de durulmuştur. 2016-2019 USGS ve Eylem Planı, Elektronik Haberleşme, Enerji, Su Yönetimi, Kritik Kamu Hizmetleri, Ulaştırma, Bankacılık ve Finans sektörlerini kritik altyapı sektörleri olarak tanımlamaktadır (2016-2019 USGS ve Eylem Planı, 2016: 7).

Ulusal siber güvenliğin sağlanmasında göz önünde bulundurulacak ilkeler kısmında 2013-2014 USGS ve Eylem Planında belirtilen ilkelere ek olarak ya da farklı bir şekilde herhangi bir ilke eklenmemiştir. Bir önceki belgede üzerinde durulan siber güvenlik riskleri bu belge de de belirtilmiş ve önceki belgeden farklı olarak kamu ve kritik altyapıların kullandığı bilişim sistemlerine gerçekleştirilecek bir siber saldırı sonrasında kişisel verilerin ele geçirilmesi ve kamuya ait gizli bilgilerin ele geçirilerek ifşa edilmesi, ticari sırların ele geçirilerek ifşa edilmesi, değiştirilmesi ya da yok edilmesi, propaganda amaçlı bilgisayar korsanlığı saldırıları sonucu kurum ve kuruluşların yaşayabileceği itibar zedelenmesi ve hassas bilgilerin ele geçirilmesi, internet üzerinden hizmet veren ya da alan kuruluşlara yapılacak siber saldırılar sonucunda hizmet veremiyor hale gelmeleri nedeniyle maddi zarara uğramaları, sanayi ve hizmet sektörlerinde bilişim sistemlerine gerçekleşecek saldırılar ya da kullanıcı hatalarından dolayı üretimin ve hizmetin kesintiye uğraması, bireylerin siber güvenlik ile ilgili yeterli bilgiye sahip olmamaları nedeniyle siber uzayda zarara uğramaları ve her türlü kurum ve kuruluşlara gerçekleştirilecek olan siber saldırılar, kullanıcı hataları ya da doğal afetler sonucunda bilişim sistemleri aracılığıyla verilen hizmetlerin kesintiye uğraması veya bu kurum ve kuruluşların dolandırıcılık faaliyetleriyle karşı karşıya gelmesi durumları siber güvenlik riskleri olarak belirtilmiştir. Belgede üzerinde durulan stratejik siber güvenlik amaçları ve bu amaçlara ulaşmak için gerçekleştirilmesi planlanan eylemler beş ana başlık altında oldukça kısa ve detaylandırılmadan sıralanmıştır. Bu başlıklar "*Siber Savunmanın Güçlendirilmesi ve*

Kritik Altyapıların Korunması, Siber Suçlarla Mücadele, Farkındalık ve İnsan Kaynağı Geliştirme, Siber Güvenlik Ekosisteminin Geliştirilmesi ve Siber Güvenliğin Milli Güvenliğe Entegrasyonu" olarak belirlenmiştir (2016-2019 USGS ve Eylem Planı, 2016: 11-20).

2016-2019 USGS ve Eylem Planı genel itibari ile kapsamı bir önceki belgeyle hemen hemen aynı olmakla beraber daha genel bir anlayışla daha dar kapsamlı bir şekilde hazırlanmıştır. Özellikle son kısımda belirtilen ve gerçekleştirilmesi planlanan stratejik eylemlerin içeriğinin ne olduğu, hangi düzenlemelerin yapılacağı veya nasıl bir süreç işleneceği konusunda herhangi bir kapsam belirtilmemiştir. Belirtilen başlıklar arasında siber savunmanın güçlendirilmesinden bahsedilmiş olmasına rağmen siber savunma kavramının ne olduğuna dair herhangi bir tanım yapılmamıştır. Yine aynı şekilde siber suçlarla mücadeleye vurgu yapılmış olmasına rağmen hangi suçların veya eylemlerin siber suç kapsamı altında değerlendirildiği ya da TCK'da belirtilen suçlardan hangilerinin siber suç olarak kabul edildiği konusunda herhangi bir açıklama mevcut değildir. Bu bağlamda değerlendirildiğinde yapılan çalışma siber uzayda güvenliğin sağlanması adına hazırlanmış bir eylem planından çok bilgilendirme amaçlı bir çalışma niteliği göstermektedir.

3.3. 2020-2023 Ulusal Siber Güvenlik Stratejisi ve Eylem Planı

Türkiye son olarak 2020-2023 Ulusal Siber Güvenlik Stratejisi ve Eylem Planını yayınlamış ve daha önceki çalışmalar üzerinden yapılanlar değerlendirilerek gerekli iyileştirmeler ile planı güncellemiştir. Bu bağlamda belirlenen stratejik amaçlar 8 ana başlık altında toplanmıştır. Daha önceki eylem planlarına benzer şekilde belirlenen bu amaçlar, 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 ve uluslararası iş birliğinin geliştirilmesi şeklinde belirlenmiştir. Ayrıca siber güvenliğin öneminin COVID-19 pandemisi sürecinde bir kez daha anlaşıldığı vurgulanarak bu süreç içerisinde hayatın her alanının giderek dijitalleştiği ve güvenli bir dijital ortamın sağlanmasının yolunun insan ve süreç bileşenlerinin güvenliğine bağlı olduğu belirtilmiştir (2020-2023 USGS ve Eylem Planı, 2020).

2020-2023 USGS ve Eylem Planı önceki çalışmalarla kıyaslandığında daha kapsamlı ve açıklayıcı bir çalışma olarak karşımıza çıkmaktadır. Siber güvenlik olgusuna daha ciddiyetle ve akademik olarak yaklaşan bu çalışmada siber uzayda gerçekleşen son gelişmeler ve önceki belgelerde ele alınmayan bazı konular ele alınarak Türkiye'nin siber güvenlik konusunda atacağı adımlar hakkında açıklayıcı bilgiler verilmiştir. Belgenin en dikkat çeken özelliği ise Ulusal Siber Güvenlik Eylem Planı bölümünün "Hizmete Özel" nitelikte hazırlanmış olmasıdır. Dolayısıyla 2020-2023 arası dönemi kapsayan bu belgede Türkiye'nin siber güvenliğin sağlanması noktasında izleyeceği eylem planı sadece ilgili kurum ve kuruluşlarla paylaşılmıştır. Bu durum, ulusal güvenlik kapsamında diğer ülkeler için istihbari bir nitelik taşıması bağlamında değerlendirildiğinde olumlu bir adım olarak değerlendirilebilir. Lakin Türkiye'nin siber güvenliğinin sağlanması adına çalışmalar yürüten araştırmacı ve akademisyenlerin bu eylem planı hakkında bilgi sahibi olmasını engellemekte ve bu bağlamda eylem planı ile ilgili yapılacak değerlendirmelerin önüne geçmektedir.

2020-2023 USGS ve Eylem Planında özellikle üzerinde durulan konu ise kritik altyapıların kullandığı bilişim sistemlerinin siber uzayda güvenliğinin sağlanması konusu olmuştur. Bu bağlamda siber tehditlerin bu altyapıları daha fazla hedef aldığı ve bu durumun bireysel ve toplumsal güvenliğe karşı riskler oluşturduğu belirtilmiştir. Belgede önceki çalışmalarla kıyaslandığında üzerinde önemle durulan bir diğer konu ise siber güvenliğin sağlanmasında ulusal siber güvenlik kapasitesi inşasının gerekliliği ve bu bağlamda yerli ve milli teknolojilerin geliştirilmesi adına Araştırma ve Geliştirme (AR-GE) çalışmalarına verilmesi gereken desteğin önemi olmuştur. Geçtiğimiz yıllarda oldukça büyük önem kazanan yapay zekâ, nesnelerin interneti, 5G teknolojisi ve blok zincir gibi siber uzayı oluşturan önemli teknolojilerin siber güvenliğin sağlanmasında izlenecek planlamalarda öncelikli olarak yer alacağının vurgulanması ise sürekli değişen ve gelişen teknolojiye ayak uydurmanın ve uluslararası alanda meydana gelen teknolojik gelişmelerin takibinin siber güvenliğin sağlanmasında hayati önem taşıdığının farkına varıldığı sonucunu ortaya çıkartmaktadır.

Belgede ulusal siber güvenliğin sağlanmasında izlenecek strateji ve eylemlerin hangi ilkeler çerçevesinde gerçekleştirileceği de belirtilmiştir. Bu bağlamda siber güvenliğin bir milli güvenlik meselesi olduğu ve ulusal güvenliğin tam olarak

sağlanabilmesi için siber güvenlik alanında belirlenen hedeflere ulaşılması gerektiği vurgulanmıştır. Ayrıca siber güvenliğin sağlanmasında izlenen politikalarda süreklilik, sürdürebilirlik ve kurumsallık ilkelerinin önemiyle birlikte şeffaflık, hesap verilebilirlik ve etik değerlerin göz önünde bulundurulması gerektiği de belirtilmiştir. Kritik altyapıların güvenliği ile yerli ve milli ürün kullanımının teşvik edilmesi ilkeleri üzerinde duran belge, aynı zamanda siber güvenliğin güçlü hukuki temeller üzerine oturtulması gerekliliğini de belirtmiştir.

Belirlenen ilkeler çerçevesinde ulusal siber güvenlik hedefleri olarak kritik altyapıların siber güvenliğinin sürekli olarak sağlanması, ulusal siber güvenliğin sağlanmasında çağa uygun en son teknoloji ürünlerine sahip olunması, siber güvenlikte yerli ve milli teknolojilerin geliştirilebilmesi adına imkanların geliştirilmesi, proaktif bir siber savunma anlayışının geliştirilmesi, SOME ekiplerinin yetkinliklerinin artırılması, kritik altyapıların siber güvenliğinin sağlanması adına denetim ve düzenlemeye dayalı bir sistem geliştirilmesi, siber güvenlik farkındalığının toplumun tüm kesimlerini kapsayacak şekilde yaygınlaştırılması, ulusal ve uluslararası düzeyde işbirliği ve anlaşmalarla koordineli bir siber güvenlik ağı oluşturulması, siber suçların en aza indirilerek siber caydırıcılığın artırılması ve siber güvenlik alanında eğitim faaliyetlerinin artırılarak bu alanda ihtiyaç duyulan yetişmiş personel ihtiyacının giderilmesi hedefleri belirlenmiştir.

Belgede daha önce belirtilen sekiz stratejik amaç detaylandırılarak açıklanmıştır. Bu bağlamda 2016-2019 USGS ve Eylem Planı belgesinde detaylandırılmayan stratejik amaçların ve hedeflerin bu belgede daha kapsayıcı ve açıklayıcı bir nitelikte ele alınması konuyla ilgili daha ciddiyetli bir yaklaşımın olduğunu göstermektedir. Çalışmanın belirlediği sekiz stratejik amacın gerçekleştirilmesi için 40 eylem maddesi belirlenmiştir. Belirlenen eylem maddeleri 75 uygulama adımından oluşmakta ve 14 farklı kamu kurumun sorumluluğunda 34 farklı kamu kurumunun çalışmalarıyla yürütülmesi planlanmıştır. Bunlara ek olarak bazı uygulama adımları için düzenleyici ve denetleyici kuruluşlar, üniversiteler ve sivil toplum kuruluşları (STK) ile iş birliği yapılacağı da belirtilmiştir. Belgede bahsi geçen eylem planları, uygulama adımları ve hangi kamu kurum ve kuruluşlarıyla bu işlemlerin yürütüleceği bilgisi hizmete özel nitelikte hazırlandığı için yayımlanmamıştır.

2.4. Ulusal Siber Güvenlik Stratejileri ve Eylem Planlarının Değerlendirilmesi

İlk kez 2013 yılında hazırlanan ve Türkiye'nin siber uzayda güvenliğinin sağlanması adına izleyeceği yol haritasını belirleyen Ulusal Siber Güvenlik Stratejisi ve Eylem Planı çalışmaları, ulusal güvenliğin tam olarak sağlanabilmesi adına oldukça büyük önem taşıyan belgelerdir. Hayatın her alanının dijitalleştiği ve bilişim teknolojilerinin her alanda kullanıldığı günümüzde bu teknolojilerin kullanımının artışına paralel olarak tehditlerin de arttığı bir gerçektir. Dolayısıyla insan eliyle oluşturulmuş bu yeni ve karmaşık alanın güvenliğinin sağlanması USGS belgelerinde de belirtildiği üzere bir milli güvenlik meselesi olarak ele alınmalıdır.

Her üç dönem için de yapılan çalışmalar siber güvenlik alanında yapılması gerekenler, hedefler ve atılacak adımların belirlenmesi adına olumlu olarak değerlendirilmektedir. Siber uzayı oluşturan en önemli bileşenlerden internet, bilgisayar ve bilişim teknolojilerinin durdurulamayan gelişimi ve değişimi göz önünde bulundurulduğunda ilk olarak iki, sonrasında ise 4'er yıllık süreçler için hazırlanan USGS ve Eylem planlarının, her saniyesi önemli olan siber güvenlik alanında çok uzun süreler için hazırlandığı söylenebilir. Dolayısıyla uzun vadeli planlar yapılması bağlamında her ne kadar milli güvenliğin sağlanması adına olumlu bir durum olarak görülse de siber uzayın doğası gereği sürekli güncellenmeye tabi tutulması gereken stratejilerin ve eylem planlarının bu kadar uzun süreler için hazırlanması bir eksiklik olarak değerlendirilmektedir.

USGS ve Eylem Planı belgeleri, içerikleri bakımından ulusal siber güvenliğin sağlamasında olumlu ve doğru adımları içermektedir. Fakat çalışmalarda belirtilen hedeflerin ne kadarına ulaşıldığı ya da ne derecede tamamlandığı konusuna dair herhangi bir açıklama ya da bir çalışma yayımlanmamış olması, ilk olarak 2013-2014 dönemi için hazırlanan eylem planının ardından 2016-2019 dönemi için hazırlanan çalışmada bir önceki çalışmada belirtilen hedeflere ne derecede ulaşıldığına dair herhangi bir verinin sunulmamış olması ve bu durumun yine aynı şekilde 2020-2023 dönemi için yapılan çalışmada da tekrarlanması, bu çalışmalarda ulusal siber güvenliğin sağlanabilmesi için belirlenen ilkelerde şeffaflık ve hesap verilebilirlik ilkeleriyle çelişen uygulamalar olarak karşımıza çıkmaktadır. Ayrıca özellikle 2020-

2023 dönemi için hazırlanan çalışmada izlenecek olan eylemler ve bu eylemlerin gerçekleştirilmesi için yapılacak uygulamaların hizmete özel nitelikte olarak hazırlanıp kamuya açıklanmamış olması da aynı şekilde değerlendirilebilir.

Hazırlanan tüm çalışmalarda ulusal siber güvenliğin sağlanmasında yetişmiş personel ihtiyacı üzerinde önemle durulmuş ve bu anlamda Ar-Ge faaliyetleri ve bu ihtiyacın karşılanması adına eğitim programlarının oluşturulmasına destek sağlanması gerektiği belirtilmiştir. İlk olarak hazırlandığı günden itibaren 2023 yılına kadar üniversitelerde açılan ve daha çok teorik anlamda eğitim veren siber güvenlik lisans üstü eğitim programları bir kenara koyulursa, yetişmiş teknik eleman ihtiyacını karşılayacak ön lisans programları ilk defa 2023 yılı güz döneminde öğrenci kabul edecektir. Ankara Üniversitesi, Ege Üniversitesi, Gebze Teknik Üniversitesi ve İstanbul Teknik Üniversitesi bünyesinde kurulan Siber Güvenlik Meslek Yüksekokulları, Türkiye'nin siber güvenlik alanında yetişmiş teknik personel ihtiyacının karşılanmasında önemli rol oynayacaktır (YÖK, 2023). Bu bağlamda bu kurumların açılmasının ilk çalışmanın ardından 10 sene sonrasında kurulması bu belgelerin güvenirliliği noktasında soru işaretleri doğurmaktadır.

Son dönemde siber uzayın her alana sirayet etmesiyle birlikte terör faaliyetlerinin de siber uzayda artış gösterdiği bir gerçektir. Daha önce detaylarıyla incelenen siber terörizm konusu gerek siber terörle mücadele noktasında yapılması gereken yasal düzenlemeler gerekse de atılması gereken adımlar anlamında USGS ve Eylem Planı belgesinde kendisine yer bulamamıştır.

Yapılan tüm çalışmalarda siber güvenliğin sağlanabilmesi için gereken yasal zeminin oluşturulması adına ihtiyaç duyulan yasal düzenlemelerin yapılması gerekliliği üzerinde durulmuş olmasına rağmen bunların neler olduğu, hangi kanunlarda değişiklik yapılması gerektiği ya da nasıl bir uyum içerisinde olunması gerektiği noktasında bir değerlendirme mevcut değildir. Ayrıca her ne kadar süreç içerisinde siber güvenliğin sağlanması adına mevcut kanunlarda düzenlemeler yapılmış olsa da siber uzayı yasal olarak düzenleyen tek bir kanun hala bulunmamaktadır.

Tüm bunlara ek olarak tüm bu çalışmalarda bahsi geçen eylemlerin gerçekleştirilebilmesi ve hedeflere ulaşılabilmesi belirli bir finans kaynağını gerektirmektedir. Özellikle teknolojinin geldiği nokta göz önünde bulundurulduğunda günümüz şartlarına uyum sağlayacak teknolojilerin edinimi, Ar-Ge çalışmaları, eğitim programları, yeni kurum ve kuruluşların oluşturulması ve mevcut olan sistemlerin daha güvenli bir hale dönüştürülebilmesi adına ihtiyaç duyulan hizmet ve teknoloji alımı bir bütçe gerektirmektedir. Bu bağlamda yapılan çalışmalarda belirtilen hedefler için ayrılan herhangi bir bütçe bilgisi söz konusu değildir. Tüm bu eylem planlarında belirtilen hedeflere ulaşılması adına yapılan ya da yapılması düşünülen projeler için mutlak surette bir bütçenin tahsis edilmesi gereklidir. Dolayısıyla bu çalışmalarda bahsi geçen hedeflere ulaşılması adına bir bütçe çalışmasının yapılmamış olması büyük bir eksiklik olarak değerlendirilmektedir.

DÖRDÜNCÜ BÖLÜM
TÜRKİYE'NİN SİBER GÜVENLİK ALANINDA YAPTIĞI ULUSLARARASI İŞ BİRLİKLERİ, ÇALIŞMALAR VE ANLAŞMALAR

1. TÜRKİYE'NİN SİBER GÜVENLİK ALANINDA YAPTIĞI ULUSLARARASI ÇALIŞMALAR ve İŞ BİRLİKLERİ

Türkiye, ulusal siber güvenliğin sağlanmasında yaptığı yasal düzenlemeler, kurumlar bazında oluşturduğu siber güvenlik birimleri ve USGS ve Eylem Planlarının yanında uluslararası düzeyde de siber güvenlik konusunda adımlar atmaktadır. Bu bağlamda özellikle üyesi olduğu NATO bünyesinde Müşterek Siber Savunma Mükemmeliyet Merkezi (CCDCoE) çatısı altında gerçekleştirilen çalışmalara destek vermekte ve aynı zamanda düzenlenen siber güvenlik tatbikatlarına katılım sağlamaktadır.

Türkiye Bilimsel ve Teknolojik Araştırma Kurumu (TÜBİTAK) ülkemizde siber güvenlik alanında uluslararası anlamda aktif çalışmalar yürüten en önemli kuruluşlar arasında yer almaktadır. Bu bağlamda TÜBİTAK bünyesinde kurulan Bilişim ve Bilgi Güvenliği İleri Teknolojiler Araştırma Merkezi (BİLGEM) çatısı altında oluşturulmuş Siber Güvenlik Enstitüsü uluslararası nitelikte organizasyonlar düzenlemektedir. Bilgem kuruluşundan bu yana siber güvenlik tatbikatları düzenlemekte ve NATO Müşterek Siber Savunma Mükemmeliyet Merkezi, NATO çalışma grupları, NATO Zararlı Yazılım Bilgi Paylaşımı Platformu (Malware Information Sharing Platform, MISP) gibi oluşumlarla iş birliği içerisinde çalışmalar yürütmektedir.

Siber olaylara müdahale ekiplerinin küresel anlamda bir forumu olan Forum of Incident Response and Security Teams (FIRST), hükümetler, ticari ve eğitim kurumlarından çeşitli siber güvenlik müdahale ekiplerini bir araya getiren bir kuruluştur. FIRST, siber olayların önlenmesinde iş birliğini ve koordinasyonu teşvik etmeyi, olaylara hızlı bir şekilde tepki göstermeyi teşvik etmeyi ve üyeler arasında ve toplum içerisinde siber güvenlikle ilgili bilgi paylaşımını desteklemeyi amaçlamaktadır (FIRST, 2023). Türkiye bu kuruluş içerisinde Ulusal Siber Olaylara

Müdahale Merkezi (USOM), Turkcell Siber Savunma Merkezi (Turkcell CDC), Türk Hava Yolları Siber Olaylara Müdahale Ekibi (TurkishAirlines CERT) ve Yapı Kredi Bankası Siber Olaylara Müdahale Ekibi (YKB-CERT) olarak dört ayrı kuruluşla temsil edilmektedir (FIRST Members, 2023)[21].

Maddi Ceza Hukuku kapsamında hazırlanan ve 2001 yılında Budapeşte'de imzalanarak 2004 yılında yürürlüğe giren Avrupa Siber Suçlar Sözleşmesi (ASS) ya da diğer adıyla Sanal Ortamda İşlenen Suçlar Sözleşmesi, Türkiye'nin siber uzayda güvenliğin sağlanması adına imzaladığı en önemli uluslararası sözleşmedir. Budapeşte Anlaşması olarak da bilinen bu sözleşme siber uzayda güvenliğin sağlanması adına hazırlanan ilk uluslararası sözleşme olması bakımından oldukça önemlidir. Türkiye bu sözleşmeyi 2010 yılında imzalamıştır. TBMM'nin 2012 yılında sözleşmeyi uygun bulmasının ardından 2014 yılında yürürlüğe girmiştir. Sözleşme kapsamında TCK'da bu sözleşmenin hükümlerine uygun olarak düzenlemelere gidilmiştir. Budapeşte Sözleşmesi, Türkiye'de siber alanda işlenen suçların yasal zeminde yer bulması, uluslararası anlamda siber güvenlik konusunda uyum sağlanması ve maddi anlamda cezaların belirlenmesi adına oldukça önemli bir anlaşma olarak karşımıza çıkmaktadır.

1.1. NATO Bünyesinde Siber Güvenlik Çalışmaları ve Türkiye'nin Katkısı

Dünyanın en güçlü askeri ittifakı olan NATO, siber uzayın güvenliği konusunu ilk defa 2002 yılında Prag Zirvesinde siyasi ajandasına almıştır. 2007 yılında birlik üyesi olan ülkelerden Estonya'ya Rusya tarafından yapıldığı iddia edilen siber saldırılar sonrasında (Cutts, 2009: 69) 2008 yılında siber savunma politikasını kabul etmiştir. 2016 yılında gerçekleşen Varşova Zirvesinde ise siber uzay NATO'nun kara, hava ve denizden sonra dördüncü muharebe alanı olarak birlik üyesi ülkeler tarafından kabul edilmiştir (NATO/Varşova Zirvesi, 2016). Ayrıca NATO'nun kurucu anlaşmasına göre üye ülkelerden birisinin ulusal güvenliğine yapılan bir saldırı sonucu ittifak üyesi ülkelerin saldırıya uğrayan ülkenin yanında yer alacağını bildiren 5. maddenin bir siber saldırı sonucunda devreye sokulabileceği sonucuna da varılmıştır (Schmitt ve Vihul, 2017). NATO, bünyesinde siber savunma ile alakalı olarak ittifaka üye ülkelerin olası bir siber saldırı karşısında bu saldırılara karşı koyabilmek adına

[21] Daha fazla bilgi için bkz. https://www.first.org/members/map#country%3ATR

sahip oldukları yeterliliklerini test edebilme ve eksikliklerin görülebilmesi adına siber güvenlik tatbikatları gerçekleştirmektedir.

2008 yılında NATO'nun siber uzayda güvenliğin sağlanması ve siber savunma kapasitesinin artırılması amacıyla kurulan NATO Müşterek Siber Savunma Mükemmeliyet Merkezi (CCDCoE) 9 ittifak üyesi ülkenin destek verdiği ve Türkiye'nin sponsor ülke olarak iştirak ettiği önemli bir oluşumdur (NATO CCD CoE, 2023). Bu bağlamda özellikle TÜBİTAK bünyesinde kurulan SGE Merkezle yakın ilişkiler içerisinde Ulusal Gönüllü Katılımcı statüsünde daimî temsilci bulundurmaktadır. Genelkurmay Başkanlığı'nın Merkezle olan ilişkilerinde iletişim noktası olarak görev yapan SGE, ayrıca Merkez bünyesinde düzenlenen siber savunma tatbikatları ve diğer çalışmalara da katkı sağlamaktadır. SGE, ayrıca NATO bünyesinde oluşturulan çalışma gruplarına ve panellere de aktif katılım sağlamaktadır. 2010 yılından bu yana NATO bünyesinde kurulan Cyber Coalition tarafından düzenlenen uluslararası siber savunma tatbikatlarına da katılım sağlayan Türkiye, yine NATO bünyesinde oluşturulmuş olan Bilgi Sistemleri ve Teknolojileri İş Paneli (NATO Information Systems & Technology Business Panel) üst çalışma grubunda SGE tarafından temsil edilmektedir (TÜBİTAK SGE, 2022).

Tüm bunlara ek olarak Türkiye, siber uzayda oldukça büyük tehlike arz eden zararlı yazılımlarla mücadele amacıyla NATO bünyesinde kurulmuş olan Zararlı Yazılım Bilgi Paylaşımı Platformu (Malware Information Sharing Platform, MISP) tarafından düzenlenen ve mevcut zararlı yazılımların belirlenmesi, konuyla ilgili çalışmaların izlenmesi ve bu konuda ihtiyaç duyulan önlemlerin alınması adına TÜBİTAK SGE temsilciliğinde aktif olarak katkı sağlamaktadır (TÜBİTAK SGE, 2022).

1.2. Siber Olaylara Müdahale Ekipleri Küresel Forumu/Forum Of Incident Response And Security Teams (FIRST) ve Türkiye

FIRST, küresel çapta gerçekleşen siber olaylara müdahale edilmesi ve cevap verilmesi durumlarında dünyaca tanınmış bir örgüttür. FIRST'e üye olan siber olaylara müdahale ekiplerinin siber olaylar karşısında reaktif ve proaktif olarak daha etkili bir şekilde yanıt vermesini amaçlamaktadır. Dünyanın her bölgesinden siber olaylara müdahale ekiplerini bir araya getiren FIRST, siber uzayda oluşan tehditlerin önüne

geçilmesi amacıyla iş birliği ve koordinasyonu teşvik etmeyi, siber olaylara hızlı ve etkili bir şekilde karşılık vermeyi ve organizasyona üye kuruluşlar arasında bilgi paylaşımını desteklemeyi amaçlamaktadır. 105 farklı ülkeden 679 siber olaylara müdahale ekibini bünyesinde barındıran FIRST, 1990 yılında kurulmuş ve sürekli genişleyerek küresel siber olaylara müdahale forumu olarak eğitim, sektör raporları ve farklı projelerle siber güvenlik alanında hizmet vermektedir (FIRST, 2023).

Türkiye daha önce de belirtildiği üzere bu kuruluş içerisinde Ulusal Siber Olaylara Müdahale Merkezi (USOM), Turkcell Siber Savunma Merkezi (Turkcell CDC), Türk Hava Yolları Siber Olaylara Müdahale Ekibi (TurkishAirlines CERT) ve Yapı Kredi Bankası Siber Olaylara Müdahale Ekibi (YKB-CERT) olarak dört ayrı kuruluşla temsil edilmektedir (FIRST Members, 2023). Kuruluş içerisinde Türkiye adına devlet seviyesinde sadece USOM bulunmaktadır. Bunun haricindeki üye kuruluşlar özel nitelikte ve oldukça büyük firmalar olarak göze çarpmaktadır. Bu bağlamda siber güvenlik alanında küresel boyutta bir organizasyonda Türkiye'den dört ayrı ekibin bulunması oldukça önemlidir. Ayrıca Türkiye'nin siber saldırılara müdahale ekiplerinin koordinasyonu ve sorumluluğunu yürüten USOM'un bu organizasyonun bir parçası olması ise uluslararası bağlamda siber güvenlik alanında ortaya çıkan gelişmelerin takip edilmesi, bilgi paylaşımı ve yeni iş birliklerinin geliştirilmesi adına olumlu bir gelişme olarak değerlendirilmektedir.

1.3. Avrupa Siber Suçlar Sözleşmesi ve Türkiye

Avrupa Konseyi Bakanlar Komitesi'nin 2001 tarihinde onayı ile yine aynı yıl Budapeşte'de devletlerin imzasına açılan Avrupa Siber Suçlar Sözleşmesi 2004 tarihinde yürürlüğe girmiştir. Avrupa Konseyi üyesi ülkelerin haricinde konsey üyesi olmayan 21 ülke tarafından imzalanan sözleşme, Türkiye tarafından 2010 yılında imzalanmış ve 2014 yılında yürürlüğe girmiştir. Sözleşme Türkçe'ye resmi olarak "Sanal Ortamda İşlenen Suçlar Sözleşmesi" olarak çevrilerek yürürlüğe koyulmuştur.

Sözleşmenin hazırlanma amacı siber uzayda ortaya çıkan suçlarla mücadele anlamında taraf devletlerin yasal altyapılarının uyumlu hale getirilmesi, bu suçlarla mücadelede soruşturma ve kovuşturma aşamasında taraf ülkelerin ulusal hukuk mevzuatına temel oluşturulması ve özellikle siber suçlarla mücadelede yasal zeminde uluslararası iş birliğinin sağlanması olarak belirtilmiştir. Budapeşte sözleşmesi olarak

da bilinen sözleşme, 2003 yılında eklenen 1 numaralı siber uzayda Yabancı Düşmanlığı ve Irkçılık Propagandası başlıklı ek protokol ve 2022 yılında eklenen 2 numaralı Gelişmiş İş Birliği ve Elektronik Kanıtların İfşasına İlişkin ek protokolle birlikte toplamda 48 madde ve 4 bölümden oluşmaktadır (EC, 2023). Anlaşmanın ilk bölümünde bilgisayar sistemi, bilgisayar verisi, hizmet sağlayıcı ve trafik verisi terimlerinin tanımı yapılmış ve sonrasında ulusal düzeyde alınacak tedbirler kapsamında Maddi Ceza Hukuku başlığı altında bilgisayar verilerinin ve sistemlerinin gizliliğine, bütünlüğüne ve erişebilirliğine yönelik suçlar sıralanmıştır. Yine aynı bölümde bilgisayarla bağlantılı suçlar ve telif hakkı ve bununla bağlantılı hakların ihlaline ilişkin suçlar tanımlanmıştır (Budapest Convention, 2004).

Anlaşmanın üçüncü bölümünde ise uluslararası iş birliği kapsamında izlenecek genel ilkeler;

> "*Taraflar, bilgisayar sistemleri ve verileri ile ilgili cezai suçlara ilişkin soruşturma ve kovuşturmalar için, veya cezai suçlara ilişkin olarak elektronik ortamda delil toplanması amacıyla, işbu bolümün hükümleri uyarınca ve ceza hukukuna dair konulardaki uluslararası işbirliğine ilişkin ilgili uluslararası belgelerin, yeknesak veya karşılıklı mevzuat ile iç hukuku temel alarak üzerinde anlaşmaya vardıkları düzenlemelerin uygulanması suretiyle, birbirleriyle mümkün olan en geniş biçimde işbirliği yapacaklardır.*" (Budapest Convention, 2004: Md. 23)

şeklinde belirtilmiştir. Türkiye sözleşme kapsamında, hukuk sisteminde maddi ceza hukukunun temelini oluşturan TCK'da sözleşmede belirtilen esaslar temelinde düzenlemeler yapmıştır. Bu bağlamda sistemi engelleme, bozma verileri yok etme veya değiştirme suçlarını ele alan TCK'nın 244'üncü maddesi Budapeşte Sözleşmesi'nin 4'üncü maddesinde öngörülen "verilere müdahale" ve 5'inci maddesinde öngörülen "sisteme müdahale" düzenlemelerine uyum sağlamaktır (BTK, 2017). Banka veya kredi kartlarının kötüye kullanılması suçlarını düzenleyen TCK'nın 245'inci maddesinde yapılan düzenlemeler ise Budapeşte Sözleşmesi'nin siber suçlar kısmında belirtilen *"Bilgisayarla bağlantılı sahtecilik"* (Md.7) ve *"Bilgisayarla bağlantılı dolandırıcılık"* (Md.8) suçlarıyla uyum sağlayan bir düzenleme olarak karşımıza çıkmaktadır.

TCK'nın 226'ncı maddesinde ele alınan müstehcenlik suçu her ne kadar bu suçun bilişim teknolojileri kullanılarak ya da bu teknolojiler aracılığıyla işlenmesi

durumunu açıkça ele almış olmasa da ilgili maddede müstehcen görüntü, yazı veya sözleri içeren ürünlerin satışı, kiralanması, dağıtımı ya da basın yayın yoluyla yayınlanması veya bu duruma aracılık edilmesi durumu suç olarak belirlenmiş ve suçun işlenme şekline bağlı olarak altı aydan beş yıla kadar hapis cezası öngörülmüştür. Bu bağlamda yapılan bu düzenleme Budapeşte Sözleşmesi'nin 9'uncu maddesinde düzenlenen "*Çocuk Pornografisiyle Bağlantılı Suçlar*" kapsamında sözleşmeye uyum sağlamaktadır. İlgili maddede müstehcen görüntülerin ya da materyallerin çocukların girebileceği ya da görebileceği yerlerde sergilenmesi, okunması, okutulması ve bu tür materyallerin çocuklara servis edilmesi durumu ele alınarak cezai müeyyideye bağlanmıştır.

2. TÜRKİYE'DE SİBER UZAYIN GÜVENLİĞİNİN SAĞLANMASI ADINA OLUŞTURULAN KURUMSAL YAPILANMALAR

Türkiye 1990'lı yılların başında TCK'da yaptığı düzenlemelerle başladığı siber uzayda güvenliğin sağlanması yolundaki düzenlemelere 2000'li yıllar itibari ile kurumsal bazda oluşturmaya başladığı yeni yapılanmalar ile devam etmiştir. Bu bağlamda siber uzayda bilginin ve sistemlerin güvenliğinin sağlanması, siber suçlarla mücadele, kritik altyapıların bilişim sistemlerinin güvenliği, kurumların bilgi sistemlerinin güvenliği, ulusal güvenlik bağlamında istihbari çalışmalar yürütülmesi, siber uzayda güvenliğin sağlanması adına ihtiyaç duyulan yetişmiş personel ihtiyacının karşılanması amacıyla eğitim faaliyetlerinin gerçekleştirilmesi ve siber güvenlik alanında teknoloji geliştirilmesi adına çalışmalar yapılması adına kurumsal yapılanmalara gidilmiştir. Özellikle e-devlet uygulamalarının geniş çaplı bir şekilde kullanılmaya başlanması, internet kullanımının akıllı telefonlar ve bilgisayar kullanımının artmasına bağlı olarak artması ve gerek kamu gerekse özel sektörün her alanında gerçekleştirilen hizmetlerinin bilişim sistemleriyle kullanımının artması sebebiyle yapılan yasal düzenlemelere ek olarak siber uzayın güvenliğinin sağlanması adına görev yapan kuruluşların ihtiyacı da ortaya çıkmıştır. Mevcut kurumların kendi bünyelerinde oluşturduğu alt birimlere ek olarak Ulusal Siber Güvenlik Merkezi (USOM) gibi münferit kurumlar da oluşturulmuştur. Bu kısımda Türkiye'nin siber

uzayda güvenliğinin sağlanması adına çalışan ve görev yapan kurum ve kuruluşlar incelenecektir.

2.1. Düzenleyici Kurum ve Kurullar

2.1.1. Ulaştırma ve Altyapı Bakanlığı (UAB)

Önceki adı Ulaştırma, Denizcilik ve Haberleşme Bakanlığı (UDHB) olan UAB'nin adı, Cumhurbaşkanlığı Hükümet Sistemi'ne geçildikten sonra 10/07/2018 tarihli ve 30474 sayılı Resmî Gazetede yayımlanan 1 No'lu Cumhurbaşkanlığı Teşkilatı Hakkında Cumhurbaşkanlığı Kararnamesi ile "Ulaştırma ve Altyapı Bakanlığı" olarak değiştirilmiştir. 2012 yılında yayımlanan 2012/3842 sayılı "Ulusal Siber Güvenlik Çalışmalarının Yürütülmesi, Yönetilmesi ve Koordinasyonuna İlişkin Bakanlar Kurulu (BK) Kararı" ile Türkiye'de siber güvenliğin sağlanmasında kurumsal bazda koordinasyonun sağlanması görevi ile siber güvenliğin sağlanmasında ihtiyaç duyulan politikaların belirlenmesi, altyapının geliştirilmesi ve çözüm önerileri sunulması görevi 2011 yılında yayınlanan 655 Sayılı UDHB'nin Teşkilat ve Görevleri Hakkında Kanun Hükmünde Kararname'nin (KHK) ilgili maddeleriyle[22] de bağlantılı olarak UDHB'na verilmiştir.

UAB'nın ulusal siber güvenliğin sağlanması adına görev ve yetkileri 2012/3842 sayılı Bakanlar Kurulu Kararı'nın 5'inci maddesinde sıralanmıştır. Verilen karar kapsamında bakanlığın ulusal siber güvenliğin sağlanmasındaki görev ve yetkileri şu şekildedir:

- Ulusal siber güvenliğin sağlanması için politika, strateji ve eylem planlarını hazırlamak,
- Kamu kurum ve kuruluşlarına ait bilgi ve verilerin güvenliği ile mahremiyetinin güvence altına alınmasını sağlamaya yönelik usul ve esasları hazırlamak,
- Ulusal siber güvenliğin sağlanmasında kamu kurum ve kuruluşlarında teknik alt yapının oluşturulmasını takip etmek, uygulamaların etkinliğinin doğrulanmasını ve test edilmesini sağlamak,

[22] 655 Sayılı UDHB'nin Teşkilat ve Görevleri Hakkında Kanun Hükmünde Kararname'nin bu konudaki ilgili maddeleri daha önce belirtildiği üzere madde 29/7 ve madde 30/1'de düzenlenen uzmanlık gerektiren çalışma gruplarının oluşturulması hakkındaki maddelerdir.

- Ulusal bilgi teknolojileri ve iletişim alt yapısı ve sistemleri ile veri tabanlarının güvenliğini sağlamaya, kritik altyapıları belirleyerek bunlara yönelik siber tehdit ve saldırı izleme, müdahale ve önleme sistemlerini oluşturmaya, ilgili merkezleri kurmaya, kurdurmaya, bu sistemlerin denetimi, işletimi ve sürekli güçlendirilmesine yönelik çalışmaları yapmak,
- Ulusal siber güvenliğin sağlanmasında her türlü milli çözümlerin ve siber saldırılara müdahale araçlarının geliştirilmesi ve üretilmesini teşvik etmek, kullanımını sağlamak,
- Ulusal siber güvenlik açısından kritik kurum ve konumlar için gerekli ve yeterli sayıda uzman personelin temini, eğitimi ve gelişimini planlamak, koordine etmek ve yürütmek,
- Bu karar çerçevesinde düğer ülkeler ve uluslararası kuruluşlarla iş birliği 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,
- Siber Güvenlik Kurulu'nun sekretarya hizmetlerini yürütmek. (2012/3842 sayılı BKK, 2012: Md. 5)

UAB, ilgili Bakanlar Kurulu Kararının 5'inci maddesinin üçüncü fıkrasına göre belirtilen görevlerini Bilgi ve İletişim Teknolojileri Başkanlığı (BTK) aracılığıyla yürütmektedir. Ayrıca yine bu karar kapsamında diğer kurum ve kuruluşlarla da iş birliği yaparak bu görevleri yerine getirmektedir.

UAB ulusal siber güvenliğin sağlanması noktasında kendisine verilen görev ve yetkiler kapsamında bugüne kadar 2013-2014 Ulusal Siber Güvenlik Stratejisi ve Eylem Planı, 2016-2019 Ulusal siber Güvenlik Stratejisi ve Eylem Planı ve son olarak 2020-2023 Ulusal Siber Güvenlik Stratejisi ve Eylem Planı çalışmalarını hazırlayarak yayımlamıştır. Bunlara ek olarak Sektörel ve Kurumsal Siber Olaylara Müdahale Ekibi Kurulum ve Yönetim Rehberleri ile Kurumlar için Siber Güvenlik Önlemlerini Ölçme Testi Dokümanı hazırlamıştır.

UAB kendisine verilen görev ve yetkiler kapsamında ulusal siber güvenliğin sağlanması adına diğer kurum ve kuruluşlarla da ortak çalışmalar yapmaktadır. Bu bağlamda TÜBİTAK tarafından hazırlanan "Kritik Bilgi Sistemi Altyapıları için Asgari Güvenlik Önlemleri Dokümanı" ve "Kamu Kurumlarının Uyması Gereken Asgari Bilgi Güvenliği Kriterleri" çalışmaları bu kapsamda değerlendirilebilir.

2.1.2. Bilgi Teknolojileri ve İletişim Kurumu (BTK)

İlk olarak 27.01.2000 tarihli 4502 sayılı Kanunla "Telekomünikasyon Kurumu" adıyla kurulan kurum, 5809 sayılı Elektronik Haberleşme Kanunu ile yapılan yeni düzenlemede adı "Bilgi Teknolojileri ve İletişim Kurumu (BTK)" olarak değiştirilmiştir. Türkiye'de internet hizmeti veren yer ve hizmet sağlayıcıların kontrol, denetim ve gerekli izinlerinin alınması noktasında tek yetkili olan kuruluş, siber güvenlik bağlamında özellikle daha önce detaylarıyla incelenen 5809 sayılı Elektronik Haberleşme Kanunu'nda yapılan düzenlemelerle bu alanda faaliyetler yürütmektedir. UAB'nin siber güvenlik alanında yaptığı çalışmalarda baş rolü oynayan BTK "güvenli internet" sloganıyla hizmetlerini yürütmektedir. Türkiye'de sektörel bazda düzenleyici bir kurum olarak görev yapan BTK, siber güvenliğin sağlanmasında 5651 sayılı "*İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun*", 5809 sayılı "*Elektronik Haberleşme Kanunu*" ve 5070 sayılı "*Elektronik İmza Kanunu*" gibi kanunlarda yapılan yasal düzenlemelerle geniş görev ve yetkiler verilen bir kuruluştur.

BTK kuruluşundan bu yana özellikle 2009 yılında hazırladığı "*Siber Güvenliğin Sağlanması: Türkiye'deki Mevcut Durum ve Alınması Gereken Tedbirler*" başlıklı raporla birlikte siber güvenliğin sağlanmasında önemli çalışmalar yürütmektedir. Özellikle 5651 sayılı Kanun'da düzenlenen internet ortamında yapılan ve aynı kanunda içeriği suç unsuru teşkil eden yayınlarla ilgili içeriğin kaldırılması ve/veya erişimin engellenmesi kararının verilmesi ve uygulanmasında sorumlu olan BTK, özellikle sosyal medya platformlarının ülkemizdeki hizmetlerinin düzenlenmesi noktasında görevlendirilmiştir. Yine 5651 sayılı Kanun çerçevesinde internet ortamında çocukların korunması, gerçek olmayan bilginin sosyal medya platformlarında yayılması ve toplumsal olarak kamuoyunun yanlış yönlendirilmesinin engellenmesi noktasında sorumlulukları bulunan kurum, 5809 sayılı Kanun'la

elektronik haberleşme sektöründe belirtilen ilkelerin uygulanması ve gözetilmesinde UAB ile birlikte yetkilendirilmiştir. Siber Güvenliğin sağlanması noktasında 5809 sayılı Kanun kapsamında kamu kurum ve kuruluşları ile gerçek ve tüzel kişilere karşı yapılacak siber saldırılara karşı korunmanın sağlanması ve caydırıcı önlemlerin alınması adına görevlendirilen BTK, aynı zamanda 5070 sayılı Kanun gereği artık oldukça yaygın bir şekilde kullanılan elektronik imzaların oluşturulmasında gerekli olan yetkilendirmeyi veren tek kuruluştur.

USGS ve Eylem planları kapsamında da siber güvenliğin sağlanmasında görev ve yetkileri bulunan kuruluş çatısı altında siber uzayda ortaya çıkan tehditlerin azaltılması, potansiyel siber saldırıların ve olayların ortaya çıkartabileceği etkilerin azaltılması ve kamu kurum ve kuruluşlarının siber güvenliği ile ilgili koordinasyonun sağlanması adına 2013-2014 USGS ve Eylem Planı kapsamında 2013 yılında Ulusal Siber Olaylara Müdahale Merkezi (USOM) kurulmuştur. Bu kapsamda aynı zamanda kurumsal ve sektörel Siber Olaylara Müdahale Ekipleri (SOME) oluşturulmuş ve USOM koordinasyonunda gerek kurumsal siber güvenliğin sağlanması gerekse de ülke ekonomisi ve güvenliği bağlamında kritik önem taşıyan sektörlerin siber uzayda güvenliğinin sağlanması adına görev yapmaktadır. Ayrıca kurum koordinasyonunda UAB, TÜBİTAK ve Telekomünikasyon İletişim Başkanlığı iş birliğinde siber güvenlik tatbikatları düzenlenmektedir.

2.1.3. Siber Güvenlik Kurulu

2012/3842 sayılı "*Ulusal Siber Güvenlik Çalışmalarının Yürütülmesi, Yönetilmesi ve Koordinasyonuna İlişkin Bakanlar Kurulu Kararı*" ile oluşturulan Siber Güvenlik Kurulunun görev ve yetkileri 5809 sayılı Elektronik Haberleşme Kanunu'nda 2014 yılında yapılan düzenleme ile belirlenerek Kurula ulusal siber güvenliğin sağlanmasında politika ve stratejilerin belirlenmesinde görev ve yetkiler vermiştir. 3842 sayılı Bakanlar Kurulu Kararının 4'üncü maddesine göre;

> "*Siber güvenlikle ilgili olarak alınacak önlemleri belirlemek, hazırlanan plan, program, rapor, usul, esas ve standartları onaylamak ve bunların uygulanmasını ve koordinasyonunu sağlamak amacıyla; Ulaştırma, Denizcilik ve Haberleşme Bakanının başkanlığında Dışişleri, İçişleri, Milli Savunma, Ulaştırma, Denizcilik ve Haberleşme bakanlıkları müsteşarları, Kamu Düzeni ve Güvenliği Müsteşarı, Milli İstihbarat Teşkilatı Müsteşarı, Genelkurmay Başkanlığı Muhabere Elektronik ve Bilgi Sistemleri Başkanı, Bilgi Teknolojileri ve İletişim Kurumu*

Başkanı, Telekomünikasyon İletişim Başkanı ile Ulaştırma, Denizcilik ve Haberleşme Bakanınca belirlenecek bakanlık ve kamu kurumlarının üst düzey yöneticilerinden oluşan Siber Güvenlik Kurumu kurulmuştur." (2012/3842 sayılı BK Kararı, 2012: Md. 4).

5809 sayılı Elektronik Haberleşme Kanunu Ek Madde 1'e göre Kurulun görevleri Siber güvenlik ile ilgili politika, strateji ve eylem planlarını onaylamak ve ülke çapında etkin şekilde uygulanmasında yönelik kararları almak, kritik altyapıların belirlenmesine ilişkin teklifleri karara bağlamak, siber güvenlikle ilgili hükümlerin tamamından veya bir kısmından istisna tutulacak kurum ve kuruluşları belirlemek ve kanunlarla verilen görevleri yerine getirmek olarak belirlenmiştir (5809 sayılı Kanun, Ek Madde1/2). 2018 tarihinde 703 sayılı KHK ile daha önce Ek Madde 1'de Siber Güvenlik Kurulunu oluşturacak kamu kurum ve kuruluşları ile üyelerinin temsil düzeyinin Bakanlar Kurulu tarafından belirleneceğini belirten 1'inci fıkrası ile Siber Güvenlik Kurulunun çalışma usul ve esaslarının Başbakanlık yönetmeliğiyle belirleneceğini belirten 3'üncü fıkrası yürürlükten kaldırılmıştır. Aynı KHK ile eklenen Ek Madde 2'de ise "*Mevzuatta Siber Güvenlik Kuruluna yapılmış olan atıflar, Cumhurbaşkanınca belirlenen kurul veya mercie yapılmış sayılır*." hükmü eklenmiştir (703 sayılı KHK, Md. 205). Buradan anlaşılan durum ise daha önce 3842 sayılı BKK ile kurularak Kurulu oluşturan kurum ve kuruluş yetkililerinin yerini Cumhurbaşkanınca belirlenecek kurul veya merciinin oluşturacağıdır. Fakat burada dikkat çeken husus ise BTK'nın internet sitesinde vermiş olduğu bilgiye göre Siber Güvenlik Kurulu en son toplantısını 2013 yılında gerçekleştirmiştir (BTK, 2017). 2018 yılında yapılan değişiklikten bugüne kadar ise Cumhurbaşkanı'nın belirlemiş olduğu bir Siber Güvenlik Kurulu ile ilgili herhangi bir bilgi mevcut değildir. Dolayısıyla bu durum, Kurulun varlığı ve çalışmaları hakkında soru işareti oluşturmaktadır.

2.2. Siber Suçlarla Mücadele Eden Kurumlar

2.2.1. Emniyet Genel Müdürlüğü (EGM) Siber Suçlarla Mücadele Daire Başkanlığı (SSMDB)

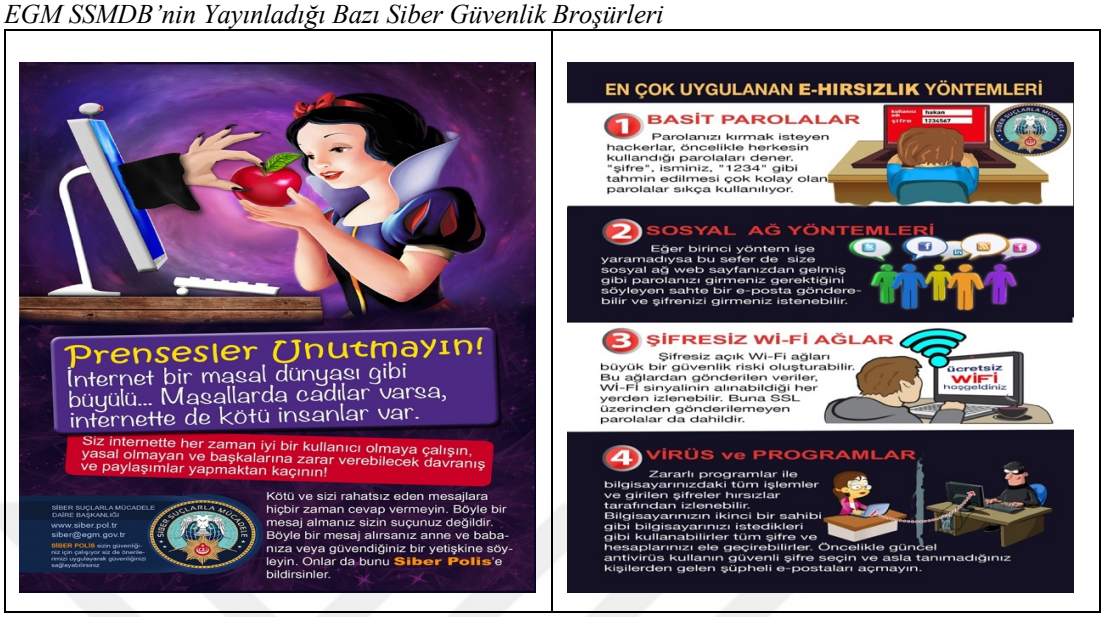
Daha önce EGM çatısı altında siber uzayda işlenen suçlarla mücadele amacıyla 2011/2025 sayılı "Emniyet Genel Müdürlüğünün Merkez Teşkilatında 1 Adet Daire Başkanlığı ve 9 Adet Şube Müdürlüğü Kurulması Hakkında Bakanlar Kurulu Kararı" ile kurulan "Bilişim Suçlarıyla Mücadele Daire Başkanlığı", 2013 yılında İçişleri Bakanlığı'nın olur kararı ile adı "Siber Suçlarla Mücadele Daire Başkanlığı

(SSMDB)" olarak değiştirilmiştir. Siber uzayda işlenen suçlarla mücadele etmek, siber suçlarla alakalı olarak toplumsal farkındalık yaratmak, siber suçlarla mücadelede uluslararası iş birlikleri yapmak, ulusal siber güvenliğe yönelik tehditleri tespit ederek analizler gerçekleştirmek, bu alanda ihtiyaç duyulan yetişmiş personel ihtiyacını gidermek için çalışmalarda bulunmak ve siber suçlarla mücadele kapasitesini artırmak amacıyla hizmet veren SSMDB, özellikle son dönemde artan toplum mühendisliği ve oltalama yöntemleriyle gerçekleştirilen dolandırıcılık suçlarıyla alakalı olarak toplumsal bilgilendirme çalışmaları yürütmekte ve sosyal medya platformlarında TCK kapsamında suç olarak belirlenmiş aktivitelerin takibini yaparak bu suçların önlenmesinde görev almaktadır (EGM, 2023).

Siber uzayda suçla mücadele noktasında uluslararası standartlarda Dijital Delillere ilk Müdahale ve İmaj Eğitimi, Mobil Cihaz İnceleme Eğitimi, Siber Suçlar Araştırma Eğitimi, Siber Suçlar Soruşturma Eğitimi ve Temel Adli Bilişim Eğitimi faaliyetlerini yürüten EGM SSMDB, birçok farklı ülkenin polis teşkilatlarına siber suçlarla mücadele bağlamında bu eğitimleri vermektedir (EGM, SSMDB Uluslararası Eğitim Kataloğu, 2021).

Bireylerin siber uzayda güvenli bir internet kullanımı sağlaması adına bilgilendirme çalışmaları yapan EGM SSMDB çocukların internet ortamında güvenliğinin sağlanması ve siber dolandırıcılıkla mücadele gibi alanlarda toplumsal bilgilendirme çalışmaları yaparak hazırladığı broşürlerle siber güvenlik farkındalığı oluşturmaya çalışmaktadır. Özellikle sosyal medya platformlarının kullanımının milyonlara ulaşması ve alanda artan suç oranlarıyla mücadele kapsamında hesap güvenliği, sahte hesapların tespiti ve sosyal medya üzerinden suç içeriği taşıyan içeriklerin takibi, yayından kaldırılması ve suçun tespiti konularında çalışmalar düzenleyen EGM SSMDB bu konuda ayrıca toplumsal bilgilendirme çalışmaları da yürütmektedir.

Şekil 1.
EGM SSMDB'nin Yayınladığı Bazı Siber Güvenlik Broşürleri



Kaynak: EGM SSMDB, 2023

Başkanlık aynı zamanda 2018 yılında Uluslararası Siber Suçları Çalıştayı'nı düzenlemiştir. Tüm bunlara ek olarak güncel siber dolandırıcılık faaliyetleri hakkında da sürekli bilgi paylaşımı yapılmaktadır (EGM SSMDB, 2022).

2.2.2. Jandarma Genel Komutanlığı (JGK) Siber Suçlarla Mücadele Daire Başkanlığı

İçişleri Bakanlığına bağlı olarak emniyet ve asayişin sağlanması ile kamu düzeninin korunması amacıyla silahlı genel kolluk kuvveti olarak görev yapan JGK, sorumluluk bölgesi dahilinde siber ortamda meydana gelen suçlarla mücadele bağlamında daha önce "Siber Suçlarla Mücadele Şube Müdürlüğü" adı altında görev yapan birimini 2019 yılında daire başkanlığı seviyesine çıkartarak "Siber Suçlarla Mücadele Daire Başkanlığı (SSMDB)" adıyla görev yapmaktadır. SSMDB, bağlı bulunduğu JGK sorumluluk bölgelerinde ortaya çıkan olaylarda ele geçirilen ve adli makamlar tarafından gönderilen dijital materyallerin incelenerek raporlanması, siber güvenlik alanında ihtiyaç duyulan yetişmiş personel ihtiyacının karşılanması, siber suçlarla mücadele, bilişim teknolojileri kullanılarak veya aracılığıyla işlenen suçların soruşturulması ve bu amaçla operasyonlar düzenlenmesi ve koordine edilmesi, meydana gelen olaylarda suçun ortaya çıkartılması amacıyla bilişim sistemlerinde

arama, dijital kopya, inceleme, verileri kurtarma ve raporlama faaliyetleri yürütmektedir (JGK SSMDB, 2022).

JGK SSMDB aynı zamanda EGM SSMDB'ye benzer bir şekilde siber suçlarla mücadele ve bu suçların soruşturulması görevlerine ek olarak siber suçlarla mücadele bağlamında toplumsal bilgilendirme faaliyetleri de yürütmektedir. Bu bağlamda afiş, broşür, sunum, bilgilendirme videoları ve bilgi notları hazırlayan JGK SSMDB, bireylerin mevcut siber tehditlere maruz kalmasını önlemek amacıyla siber uzayda oldukça yaygın olan yasa dışı bahis, güvenli internet kullanımı, banka ve ödeme dolandırıcılığı, kiralık araç dolandırıcılığı, otel dolandırıcılığı, oltalama yöntemiyle dolandırıcılık ve siber zorbalık hakkında toplumun her kesiminde siber güvenlik farkındalığı oluşturmaya çalışmaktadır[23](JGK SSMDB, 2022).

2.3. Ulusal Siber Güvenliğin Sağlanmasında Görevli Kurumlar

2.3.1. Türk Silahlı Kuvvetleri (TSK) Siber Savunma Komutanlığı

Bilindiği üzere ulusal güvenliğin sağlanmasında başat rolü oynayan TSK, kara, hava ve deniz alanlarında Türkiye'nin milli güvenliğini garanti altına alma görevinin yanında siber uzayın özellikle NATO nezdinde yeni bir muharebe alanı olarak kabul edilmesiyle beraber bu alanda da ulusal güvenliğin temin edilmesi ihtiyacının farkında olarak 2012 yılında "TSK Siber Savunma Merkezi Başkanlığı" adıyla siber uzayda güvenliğin sağlanması çalışmalarına başlamıştır. 2013-2014 USGS ve Eylem Planının yayınlamasından hemen sonra ise Başkanlık, komutanlık seviyesine dönüştürülerek 30 Ağustos 2013'te "TSK Siber Savunma Komutanlığı" adıyla görevine devam etmektedir. Siber uzayda milli teknoloji ve ürün geliştirilmesi noktasında TÜBİTAK, ASELSAN ve STM gibi kuruluşlarla ortaklaşa yaptığı çalışmalarla Türkiye'nin siber uzayda savunma kapasitesinin artırılması, TSK'nın kullandığı sistemlere gerçekleştirilebilecek potansiyel saldırıların tespiti ve önlenmesi ve bu alanda TSK'nın savunma kabiliyetinin artırılması adına çalışmalar yapan Siber Savunma Komutanlığı bünyesinde ayrıca "Siber Savunma Harekât Merkezi" bulunmaktadır. Merkez 7 gün 24 saat esasına göre görev yapmaktadır (AA, 2016).

[23] JGK SSMDB tarafından hazırlanan siber suçlarla mücadele afiş, broşür, sunum, video ve bilgi notlarına ulaşmak için bkz. https://www.jandarma.gov.tr/siber

Siber Savunma Komutanlığı ayrıca NATO ile iş birliği kapsamında Müşterek Siber Savunma Mükemmeliyet Merkezi'nin yapmış olduğu çalışmalara TÜBİTAK SGE ile koordineli olarak aktif katılım ve katkı sağlamaktadır. Bu bağlamda özellikle daha önce bahsi geçen siber güvenlik tatbikatlarına aktif katılım sağlayan TSK Siber Savunma Komutanlığı, son olarak 17-21 Nisan 2023 tarihleri arasında 38 ülkenin katılımıyla gerçekleştirilen LockShields Tatbikatına katılım sağlamıştır (MSB, 2023).

2.3.2. Millî İstihbarat Teşkilâtı (MİT)

Türkiye'nin ulusal güvenliğinin sağlanmasında hayati rol oynayan MİT, siber uzayın her mecrada kullanılmaya başlanması ve teknolojinin geldiği noktanın farkında olarak icra ettiği istihbarat faaliyetlerini siber uzayda da sürdürmektedir. Bünyesinde bulundurduğu başkanlık seviyesindeki birimlerden "Elektronik Teknik İstihbarat Başkanlığı" ve "Sinyal İstihbaratı Başkanlığı", siber uzayda ulusal güvenliğin sağlanması adına kritik önem taşıyan bilgilerin edinilmesi alanında faaliyet gösteren birimlerdir.

Her türlü bilgi ve belgenin dijital ortamlarda saklanarak işlendiği, bireyler, kurum ve kuruluşlar arasında haberleşmenin dijital ortamlarda gerçekleştiği günümüzde, siber uzayın getirdiği imkanlar sayesinde bilgiye ulaşım oldukça kolay bir hale gelmiştir. Yapılan siber saldırılarla kritik bilgilerin ele geçirilmesi, sosyal medya platformları aracılığıyla yayılan bilginin bir açık kaynak istihbaratı oluşturması, ulusal güvenliği tehdit eden faaliyetlerin planlanmasında bilişim teknolojilerinin kullanımının artması, siber terör faaliyetlerinin artması, tüm kamu kurum ve kuruluşlarının verdiği hizmetleri bilişim teknolojileri kullanarak dijital ortamlarda ulaşılabilir hale getirmesi ve özellikle kritik altyapıları kontrol eden bilişim teknolojileri sistemlerinin siber uzayın önemli bir parçasını oluşturması, bu alanda ortaya çıkabilecek tehditleri de artırmıştır. Bu bağlamda MİT, siber uzayda ortaya çıkabilecek tehditlerin önlenmesi, karşı konulması ve karşılık verilmesinin yanında espiyonaj faaliyetlerinin sürdürülmesi ve bilgi edinimi noktasında siber uzayı aktif bir şekilde kullanmakta ve ulusal siber güvenliğin sağlanmasına katkıda bulunmaktadır.

Cumhurbaşkanlığı'na bağlı olan MİT, 2937 sayılı "*Devlet İstihbarat Hizmetleri ve Millî İstihbarat Teşkilâtı Kanunu"* kapsamında kendisine tevdi edilen görev ve sorumlulukları yerine getirmektedir. 2014 yılında 6532 sayılı Kanun ile 2937

sayılı Kanunda yapılan düzenlemelerle MİT'e ulusal siber güvenliğin sağlanması adına da görev yüklenmiştir. Buna göre "*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.*" (2937 sayılı Kanun, 1983, Md. 4-i) görevleri yüklenen MİT, gelişen teknoloji ile milli güvenliğe karşı ortaya çıkan tehditlerin de niteliğinin değiştiğinin farkında olarak siber tehditlere karşı faaliyetler yürütmektedir. Bu bağlamda özellikle daha önce Genelkurmay Başkanlığı bünyesinde hizmet veren "Genelkurmay Elektronik Sistemler (GES) Komutanlığı'nın" 2012 yılında MİT bünyesine katılmasıyla Teşkilatın siber kapasitesi artırılmış ve siber istihbarat çalışmalarında önemli bir avantaj sağlamıştır (MİT, 2022).

Teşkilatın yayınladığı 2022 Faaliyet Raporunda istihbarat çalışmalarında teknolojinin önemi vurgulanmış ve bu bağlamda konvansiyonel anlamdaki istihbarat yaklaşımının ötesinde teknolojinin MİT için ana faaliyet alanlarından birisi olduğu vurgulanmıştır. Bu kapsamda büyük veri analizi, yapay zekâ uygulamaları, görüntü istihbaratı, sinyal istihbaratı, uydu istihbaratı ve siber istihbarat alanlarında Teşkilatın kapasitesini artırdığı ve bu alanlarda yürütülen yeni teknoloji edinimi çalışmaları ve gerçekleştirilen yatırımlar sayesinde MİT'in istihbarat faaliyetlerinin gerçekleştirilmesi için ihtiyaç duyduğu teknolojiyi kendi imkanlarıyla karşılayacak düzeye geldiği belirtilmiştir (MİT Başkanlığı 2022 Faaliyet Raporu, 2023).

2.3.3. Ulusal Siber Olaylara Müdahale Merkezi (USOM) ve Siber Olaylara Müdahale Ekipleri (SOME)

2012/3842 sayılı "*Ulusal Siber Güvenlik Çalışmalarının Yürütülmesi, Yönetilmesi ve Koordinasyonuna İlişkin Bakanlar Kurulu Kararı*" ve 2013-2014 USGS ve Eylem Planı çerçevesinde Türkiye'nin ulusal siber güvenliğinin sağlanması amacıyla ortaya çıkabilecek potansiyel siber tehditlerin belirlenmesi, meydana gelen siber saldırıların etkilerinin en aza indirilmesi ve sonrasında saldırının gerçekleştirildiği sistemin en kısa sürede mümkün olan en iyi şekilde eski haline döndürülebilmesi amacıyla BTK bünyesinde 2013 tarihinde "Ulusal Siber Olaylara Müdahale Merkezi (USOM)" kurulmuştur. Buna ek olarak yine 2013-2014 USGS ve

Eylem Planı kapsamında kamu kurum ve kuruluşlarının siber uzayda güvenliğinin sağlanması adına USOM rehberliğinde "Siber Olaylara Müdahale Ekipleri (SOME)" kurulmuştur. Bu ekipler aynı zamanda "Kurumsal" ve "Sektörel" olarak ikiye ayrılmış ve özellikle kritik altyapı sektörlerinin siber uzayda güvenliğinin sağlanması adına USOM ile iş birliği çerçevesinde sorumluluğu altında kuruldukları kurum veya kuruluşun siber güvenliğini sağlamakla yükümlü olarak görev yapmaktadırlar (USOM, 2023).

USOM, Türkiye'nin kurumsal ve sektörel bağlamda siber güvenliğinin sağlanması, tehditlerin belirlenmesi ve bu tehditlerle ilgili önlem alınması, meydana gelen siber saldırıların önlenmesi ve zararın en aza indirilmesi adına bir siber güvenlik koordinasyon merkezi olarak görev yapmaktadır. 7 gün 24 saat çalışma esasına göre hizmet veren USOM, aynı zamanda siber güvenlik konusunda farkındalık çalışmaları da yürütmektedir. Bilişim sistemlerinde ortaya çıkan güvenlik açıklıkları ve zararlı yazılımlarla ilgili olarak kurumsal ve sektörel SOME'lere bilgilendirme yapan USOM, büyük veri, yapay zekâ ve zararlı yazılım analizi konuları ile ilgili Ar-Ge çalışmaları da yürütmektedir. USOM aynı zamanda SOME ile iletişim ve koordinasyonun sağlanması amacıyla bir iletişim platformu da oluşturmuştur (USOM, 2023).

2013-2014 USGS ve Eylem Planı kapsamında 28818 sayılı "Siber Olaylara Müdahale Ekiplerinin Kuruluş, Görev ve Çalışmalarına Dair Usul ve Esaslar Hakkında Tebliğ" ile UAB'nin hazırlamış olduğu sektörel ve kurumsal "SOME Kurulum ve Yönetim Rehberi" çerçevesinde enerji, elektronik haberleşme, finans, su yönetimi, kritik kamu hizmetleri ve ulaştırma sektörlerinde SOME'ler kurulmuş ve bu sektörlerin siber güvenliğinden sorumlu birimler olarak USOM koordinasyonunda çalışmalarına başlamışlardır. Sektörel SOME, kritik sektörü düzenleyici ve denetleyici kurumlar çatısı altında kritik altyapı sektörü alanında hizmet vermektedir. Kurumsal SOME ise kamu kurum ve kuruluşları ile kritik altyapı sektörlerindeki özel kurumlarda kurulmuş ve bu kuruluşların siber ortamlarının güvenliği konusunda hizmet vermeye başlamışlardır. Çatısı altında kuruldukları kurum ve kuruluşların siber uzayda güvenliğinin sağlanması görevlerine ek olarak, bu kurum ve kuruluşlarda siber güvenlik ile alakalı olarak farkındalık çalışmaları yürüten SOME, bağlı bulunduğu kurum ve kuruluşların personellerine siber güvenlikle ilgili bilgilendirme çalışmaları

yürütmekle de yükümlüdür (UAB, Kurumsal/Sektörel SOME Kurulum ve Yönetim Rehberi, 2014).

2.4. Ulusal Siber Güvenliğin Sağlanmasında Teknoloji ve Ürün Geliştiren Kuruluşlar

2.4.1. Türkiye Bilimsel ve Teknolojik Araştırma Kurumu (TÜBİTAK)

Türkiye'de bilim ve teknolojinin geliştirilmesi adına akademik ve endüstriyel araştırma ve çalışmaları destekleyen, araştırma ve teknoloji geliştirme amacıyla AR-Ge enstitüleri aracılığıyla hizmet veren ve bu anlamda çalışmalar yürüten TÜBİTAK, ulusal siber güvenliğin sağlanması noktasında bünyesinde bulunan "Bilişim ve Bilgi Güvenliği İleri Teknolojiler Araştırma Merkezi (BİLGEM)" çatısı altında kurulmuş olan "Siber Güvenlik Enstitüsü (SGE)" ve "Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü (UEKAE)" aracılığıyla yaptığı çalışmalar ve verdiği hizmetler ile ulusal siber güvenliğin sağlanmasında önemli rol oynamaktadır.

SGE, Türkiye'de siber uzayın güvenliğinin sağlanması adına kapasitenin artırılması amacıyla ilk olarak 1990'lı yılların sonunda "Bilişim Sistemleri Güvenliği Birimi" adı ile UEKAE bünyesi altında çalışmalarına başlamıştır. Bu birim, 2012 yılından günümüze ise ayrı bir enstitü olarak çalışmalarına devam etmektedir. Siber güvenlik alanında Ar-Ge faaliyetleri yürüten SGE, silahlı kuvvetler ile kamu kurum ve kuruluşlarına ve özel sektöre siber güvenliğin sağlanması adına projeler üretmektedir. SGE, siber güvenlik alanında danışmanlık hizmetleri kapsamında kamu kurum ve kuruluşları ile özel sektöre güvenli yazılım geliştirme kapsamında eğitimler, yazılım geliştirirken yapılan yanlışlar sonucu ortaya çıkan açıklıkların tespit edilmesi, risk analizi, tehdit modelleme, yeni ve güvenli yazılım geliştirme yöntemleri ile bu alanda çalıştaylar ve konferanslar düzenleme konularıyla ilgili hizmet vermektedir. Bu anlamda yine danışmanlık hizmetleri kapsamında kamu kurum ve kuruluşları ile özel sektör şirketlerine sızma testi ve güvenlik denetlemeleri, askeri ve kamu kurumları ile özel sektör kuruluşları için bilgi güvenliği risk analizi ve zararlı yazılım ve zafiyet analizi altyapısı oluşturma hizmetleri vermektedir. Ayrıca SGE'nin "Bilişim ve Otomasyon Teknolojileri Sızma Testi ve Güvenlik Denetimi Platformu (BOT-SEGEN)" geliştirmek adına çalışmaları halen devam etmektedir. Bu çalışmayla ortak bir nokta üzerinden sızma testleri ve güvenlik denetimlerinin bir otomasyona

bağlanarak uzmanlık gerektirmeden düşük maliyetlerle hızlı ve etkili bir şekilde gerçekleştirilmesi amaçlanmaktadır (BİLGEM SGE, 2023).

SGE bu alanda güvenliğin sağlanması adına silahlı kuvvetler, kamu kurum ve kuruluşları ile özel sektör kuruluşları için geliştirdiği ürünler ile de ulusal siber güvenliğin sağlanmasına katkıda bulunmaktadır. "Siber Tehditleri Algılama Merkezi" projesi kapsamında geliştirmiş olduğu "Siber Tehditleri Algılama Merkezi Sistemi" ve bu konuda verdiği eğitimler, kritik altyapı sistemlerine gerçekleştirilecek olan siber saldırıların algılanması, algılanan tehditlerin engellenmesi amacıyla geliştirilen "Siber Ortam Tuzak Sistemi" ve bu sistemle ilgili olarak verdiği eğitimler, kurumsal verilerin korunmasını sağlamak ve yetkisiz kişiler aracılığıyla bu verilerin kurum dışına sızdırılmasını önlemek amacıyla geliştirilen "Veri Kaçağı Önleme Sistemi", siber güvenliğin sağlanmasında ihtiyaç duyulan yetişmiş personel ihtiyacının sağlanması adına oluşturulmuş "Sanal Siber Güvenlik Laboratuvarı ve Tatbikat Altyapısı" ve siber uzayda işlenen suçların soruşturma ve kovuşturma aşamasında delillerin toplanması, muhafaza edilmesi ve korunması adına geliştirilen "Dijital Adli Analiz Laboratuvarı Kurulumu ve Eğitimi" hizmetleri ile "Adli Analiz Altyapısı (A3)" SGE'nin siber güvenlik alanında verdiği ve ürettiği başlıca hizmet ve ürünlerdir. Ayrıca yine SGE'nin geliştirdiği ve verilerin korunması, casus yazılımların tespiti ve izinsiz veri paylaşımının önüne geçilmesini sağlayan "ORION Veri Güvenlik Platformu" SGE'nin ulusal siber güvenliğin sağlanmasında yapmış olduğu en önemli çalışmalardan birisidir (BİLGEM SGE, 2023).

TÜBİTAK BİLGEM çatısı altında kurulmuş olan "Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü (UEKAE)" ulusal siber güvenliğin sağlanmasında kritik araştırmalar yapan ve bu konuda çözüm üreten teknolojiler geliştirerek özellikle stratejik kamu kurumlarının ihtiyaç duyduğu bilgi güvenliği ve güvenli haberleşme teknolojileri adına geliştirdiği teknoloji ve ürünler ile ön plana çıkmaktadır. Kriptoloji ve bilgi güvenliği alanlarında oldukça önemli bir bilgi birikimine sahip olan UEKAE bu konularda Türkiye'nin en geniş kütüphanesine sahiptir (BİLGEM UEKAE, 2023).

UAKEA, stratejik kamu kurumları için güvenli haberleşme çözümleri, kripto anahtar yönetim sistemleri, akıllı kart ve kimlik doğrulama sistemleri ve elektronik istihbarat çözümleri gibi projeler geliştirerek siber uzayda güvenliğin sağlanmasına

katkıda bulunmaktadır. Bu bağlamda geliştirilen Emniyetli IP Terminal Cihazı (MİLSEC-3), Taktik IP Kripto Cihazı (IPKC-T), Taktik Ağ Güvenlik Cihazı (AGC-T) Gigabit IP Kripto Cihazı (IPKC-G2) ve Gigabit Ağ Güvenlik Cihazı (AGC-G) gibi ürünler güvensiz ağlar üzerinden haberleşme ve yerel ağlar arasındaki bilgi ve veri akışını kriptolayarak güvenli bir hale getirmek için geliştirilmiştir. Ek olarak geliştirilen Mesaj İletişim Sistemi (MİS), Güvenli Mesajlaşma Sistemi (GMS) ve Güvenli Mesajlaşma İstemcisi gibi ürünler de güvenli haberleşmenin sağlanması adına geliştirilen teknolojilerdir. Özellikle stratejik kamu kurumlarının gizlilik derecesi yüksek verilerinin korunması amacıyla geliştirilen bu cihazlar kritik bilgilerin siber uzayda yetkisiz kişiler tarafından ele geçirilmesini önleme amacı taşımaktadır. UEKAE ayrıca veri güvenliği noktasında geliştirdiği Kriptolu USB Bellek Cihazı (SIR-S), Kriptolu Sabit Disk Cihazı ve Hassas Veri Taşıma Cihazı (HVTC) gibi ürünlerle de veri güvenliğinin sağlanmasına katkıda bulunmaktadır. UAKAE siber uzayda haberleşme ve veri güvenliğinin sağlanması amacıyla gerçekleştirdiği devam eden ve tamamlanmış birçok projeye sahiptir (BİLGEM UEKAE, 2023).

2.4.2. Askeri Savunma Elektronik Sanayii (ASELSAN) A.Ş.

Türkiye'nin savunma sanayisinde en büyük ve en güçlü teknoloji firması olan ASELSAN, 1975 yılında TSK'nın haberleşme noktasında ihtiyaçlarını karşılamak adına kurulmuş ve Türk Silahlı Kuvvetlerini Güçlendirme Vakfı'na (TSKGV) bağlı bir anonim şirkettir. Özellikle savunma elektroniği alanında faaliyet gösteren kuruluş TSK ile yurt içinde ve dışında kurum ve kuruluşların ihtiyaç duyduğu haberleşme ve bilgi teknolojileri, radar ve elektronik harp, insansız sistemler, kara, deniz ve silah sistemleri, hava savunma ve füze sistemleri gibi teknolojiler üzerinde çalışmalar yürüten, teknoloji ve ürün geliştiren güçlü bir kuruluştur. Siber uzayda savunma ihtiyacı gerçeğinin ortaya çıkması ile bu alanda da çalışmalar yürütmeye başlayan ASELSAN, kripto ve bilgi güvenliği sistemleri, bilgi teknolojileri sistemleri, haberleşme ve bilgisayar sistemlerinde ağ güvenliği ürünleri, güvenli veri paylaşım sistemleri ve kriptolama çözümleri gibi alanlarda ihtiyaç duyulan teknolojilerin geliştirilmesi ile üretilmesi konusunda önemli hizmetler vermektedir (ASELSAN, 2023).

Kripto ve bilgi güvenliği sistemleri konusunda teknoloji geliştiren ASELSAN, kritik güvenlik hizmeti veren kamu kurum ve kuruluşları için geliştirdiği ürünlerle haberleşme alanında verilerin güvenli bir şekilde aktarımının sağlanması, güvenli haberleşmenin gerçekleştirilmesi ve hassas bilgilerin kriptolanarak dijital ortamlarda transferinin sağlanmasına yönelik ortaya koyduğu ürünlerle güvensiz olarak nitelenen ağlarda güvenli bir şekilde bu işlemlerin gerçekleştirilebilmesini sağlamaktadır. Yine bu alanda güvenli veri paylaşım sistemleri, çevrimdışı kriptolama çözümleri ve anahtar yönetim ve güvenlik yönetim sistemleri üzerine ortaya koymuş olduğu "Siber Zırh" programı ve "Güvenli Yönetim Merkezi" gibi yazılım ve ürünlerle ulusal siber güvenliğin sağlanmasına katkıda bulunmaktadır. Yine aynı şekilde bilgi teknolojilerinin güvenliğinin sağlanması amacıyla ağ cihazları ve çözümleri geliştiren ASELSAN, aynı zamanda komuta, kontrol, haberleşme ve bilgisayar sistemleri konusunda yerli teknolojiler üzerine de çalışmaktadır. Bu bağlamda üretilen Yeni nesil Intel Core i7 işlemcili, yüksek performanslı askeri el bilgisayarı ve milli işlemci adıyla öne çıkan "ÇAKIL" savunma sistemlerinde ihtiyaç duyulan komuta ve kontrol sistemlerinde ülkenin kendi imkanlarını kullanarak çözümler üretmesi konusunda ulusal siber güvenliğe katkı sağlamaktadır. TÜBİTAK BİLGEM ile yapılan ortak çalışma sonucunda ortaya çıkan "Milli İşlemci ÇAKIL", savunma sektöründe ihtiyaç duyulan atış kontrol, insansız hava aracı, güdüm ve oto pilot, uçuş kontrol, işaret işleme ve görev yönetimi alanlarında ihtiyaç duyulan işlemci ihtiyacında dışa bağımlılığın azaltılması adına üretilmiş tek çekirdekli bir işlemcidir[24] (ASELSAN, 2023).

Ulusal siber güvenliğin sağlanmasında silahlı kuvvetlerin kullanmış olduğu sistemlerin siber uzaydaki güvenliği gerçekleştirilen operasyonların başarıya ulaşmasında, stratejik askeri bilgilerin güvenliğinin sağlanmasında ve ayrıca ortaya çıkabilecek potansiyel bir çatışma durumunda bu sistemlerin doğru ve etkili çalışabilmesi adına hayati önem taşımaktadır. Bu bağlamda ASELSAN'ın siber güvenliğin sağlanması noktasında geliştirdiği teknoloji ve ürünler ile yaptığı çalışmalar milli güvenliğin tam olarak sağlanabilmesi adına hayati önem taşımaktadır.

[24] ASELSAN'ın siber güvenliğn sağlanması amacıyla geliştirdiği teknoloji ve ürünler hakkında daha fazla bilgi için bkz. https://www.aselsan.com/tr/savunma/kategori/10/siber-teknolojiler?content=bilgi-teknolojileri-sistemleri

2.4.3. HAVELSAN A.Ş.

1982 yılında kurulan HAVELSAN, ASELSAN gibi TSKGV'ye bağlı bir kuruluş olarak hizmet vermektedir. Türkiye'nin en büyük teknoloji kuruluşlarından birisi olan HAVELSAN, TSK, kamu kurum ve kuruluşları ile özel sektör kuruluşlarının savunma ihtiyaçlarının giderilmesinde teknoloji ve ürün geliştiren bir kuruluştur. Kara, deniz ve hava alanlarında savunma sistemleri ve ürünleri geliştiren HAVELSAN, komuta kontrol ve savunma teknolojileri, simülasyon çözümleri ile bilgi ve iletişim teknolojileri alanlarında ürün ve teknoloji geliştiren bir kuruluştur (HAVELSAN, 2023). HAVELSAN, günümüz teknolojisinin geldiği noktada TSK, kamu kurum ve kuruluşları ile özel sektör kuruluşlarının siber uzayda güvenli bir şekilde haberleşmesinin sağlanmasına yardımcı olacak çözümler üretmektedir. Ayrıca verilerin güvenli bir şekilde depolanması, anlık mesajlaşma ve görüntülü konuşma ile kamu kurum ve kuruluşlarının iş süreçlerinin bilişim sistemleri aracılığıyla gerçekleştirilebilmesini sağlayacak çözümler üreten HAVELSAN, kara, hava ve deniz alanlarının savunmasında kullanılan cihaz ve araçların yönetimini sağlayan yazılımlar da geliştirerek, bu alanda güvenli bir operasyonel kapasite oluşturulması ile ulusal siber güvenliğe katkıda bulunmaktadır.

HAVELSAN, bilişim sektöründe geliştirmiş olduğu ürünler ile siber uzayda güvenli doküman ve bilgi paylaşımı, anlık mesajlaşma, dosya depolama ve paylaşım sağlanması bağlamında günümüzde çoğunlukla siber uzayın beraberinde getirdiği teknolojiler aracılığıyla sağlanan bu işlemlerin daha güvenli bir şekilde gerçekleştirilmesini amaçlamaktadır. Bu kapsamda geliştirilen kamu kurumları, askeri kurumlar ve özel sektör için iş süreçlerinin tek bir sistem altında güvenli bir şekilde kontrolünü sağlayan "KOVAN", kağıda dayalı tüm işlemlerin dijital ortama taşınarak güvenli bir iş süreci sağlanmasını amaçlayan "EVRAKA", yerli bir görüntülü konuşma sistemi olan "DİYALOG", güvenli dosya depolama ve paylaşım platformu olan "HAVELSAN Drive" ve mobil cihazlarda güvenli anlık mesajlaşma uygulaması olan "İLETİ" programlarını geliştirerek hizmete sunmuştur[25] (HAVELSAN, 2023).

[25] HAVELSAN'ın siber güvenliik bağlamında geliştirdiği bilişim teknolojileri ürünleri hakkında daha fazla bilgi için bkz. https://www.havelsan.com.tr/sektorler/bilgi-ve-iletisim

2.4.4. Savunma Teknoloji Mühendislik (STM)

Türkiye'nin en büyük savunma sanayii kuruluşlarından birisi olan STM, 1991 yılında Savunma Sanayi İcra Komitesi (SSİK) kararıyla kurulmuştur. STM, Savunma Sanayii Başkanlığı ve TSK'ya yüksek teknoloji gerektiren birçok farklı alanda proje yönetimi, sistem mühendisliği, teknoloji transferi ve danışmanlık gibi hizmetler sağlamaktadır. Türkiye'nin savunma sanayisinde birçok farklı projede görev yapan STM, komuta kontrol sistemleri, siber güvenlik, danışmanlık, radar sistemleri, uydu sistemleri, mini İHA sistemleri ve sertifikasyon gibi alanlarda faaliyet göstermektedir. Özellikle TSK'nın ihtiyaç duyduğu komuta kontrol sistemlerinin geliştirilmesinde önemli rol oynayan STM, Türkiye'de ulusal siber güvenliğin sağlanmasında teknoloji geliştiren en önemli kuruluşlardan bir tanesidir (STM, 2022a).

Türkiye'de siber güvenlik alanında geniş çalışmalar yapan STM, gerçekleştirdiği siber güvenlik projeleri, siber güvenlik farkındalık çalışmaları, eğitimler, siber güvenlik danışmanlık hizmetleri, siber güvenlik test ve analiz hizmetleri, zararlı yazılım analizi, sızma testi faaliyetleri, kaynak kod güvenlik analizi, Ar-Ge projeleri, periyodik olarak hazırlanan siber tehdit durum raporları ve veri merkezi kurulum ve danışmanlık hizmetleriyle ulusal siber güvenliğin sağlanmasına katkıda bulunmaktadır. Bünyesinde 2016 yılında kurulan siber güvenlik merkezi "STM Siber Füzyon Merkezi", siber güvenlik alanında kamu kurum ve kuruluşlarıyla beraber özel sektör kuruluşlarına siber operasyon merkezi danışmanlığı, risk yönetimi, siber olaylara müdahale, siber tehdit istihbaratı, zararlı yazılım ve sistem analizi alanlarında hizmet vermektedir. STM, siber güvenlik alanında kurumlar için kesintisiz siber güvenlik hizmeti veren "STMBugShield", siber tehdit istihbarat verilerini STM raporlarıyla birleştirerek tehdit analizi raporları oluşturarak muhtemel siber saldırıların gerçekleşmeden önüne geçmeyi amaçlayan "CyThreat" ve sağlık sektöründe bilişim sistemlerini siber tehditler konusunda koruma amacıyla geliştirilmiş olan "IoT Medic" ürünleri ile kurum ve kuruluşların siber uzayda güvenliğinin sağlanması adına katkı sağlamaktadır. Ayrıca periyodik olarak hazırlanan Siber Tehdit Durum Raporlarına ek olarak 2015 yılından bu yana düzenlenen "STM Capture The Flag" yarışması ile siber güvenlik alanında farkındalık yaratmak ve teknoloji geliştirmek adına çalışmalar yürütmektedir. NATO Müşterek Siber Savunma Mükemmeliyet Merkezi (CCD CoE) ve NATO İletişim ve Bilgi Ajansı (NCI) ile iş birliği yapan STM, bunun yanında

Avrupa Güvenlik Organizasyonu (European Organisation for Security/EOS), Avrupa Siber Güvenlik Organizasyonu (European Cyber Security Organisation/ECS) ve Avrupa Siber Güvenlik Koruma İttifakı (European Cyber Security Protection Alliance/CYSPA) kuruluşlarına da üyedir[26] (STM, 2022b).

[26] STM'nin siber güvenliik bağlamında geliştirdiği ürün ve hizmetler hakkında daha fazla bilgi için bkz. https://www.stm.com.tr/tr/cozumlerimiz/siber-guvenlik-ve-bilisim#siber-guvenlik

SONUÇ

İnsanlığın bilgisayar ve internet teknolojisi ile tanıştığı ilk günlerden bu yana bilgi ve iletişim teknolojileri tahmin edilemeyen boyutlarda gelişerek deyim yerinde ise evrim niteliğinde bir değişikliğe uğramıştır. İlk kullanılmaya başlandığı zamanlarda dönemin şartları itibari ile karmaşık matematiksel işlem ve analizler yapabilen bilgisayarlar, bugünün bilgisayar teknolojisi ile kıyaslandığında ise oldukça basit işlemler yapabilme kapasitesine sahipti. İlk ortaya çıktıklarında binaların odalarına sığmayacak büyüklükte ve ancak iş makineleriyle kaldırılabilecek ağırlıkta olan bilgisayarlar, akıllı telefon teknolojisinin geldiği noktayla artık herkesin her an yanında taşıyabildiği bir teknolojiye dönüşmüştür. İnternet teknolojisinin yaygınlaşmasıyla birlikte ise bilgisayar teknolojisinin yapabileceği iş ve işlem kapasitesi en basit market alışverişinden toplumsal ilişkilere kadar tüm hayatı dijital bir dönüşüm içerisine sokmuştur. Artık en basit mutfak aletlerinden devasa büyüklükteki sanayi üretim tesislerine kadar birçok teknolojik cihazın internet bağlantısı sayesinde birbirine bağlanarak sürekli veri alışverişi yapabildiği günümüz dünyası tam anlamıyla dijital bir yaşamın sürdürüldüğü bir yer haline gelmiştir.

Üretim ve tüketimin, kamu hizmetlerinin, insan ilişkilerinin, bankacılık hizmetlerinin ve hatta toplumların dijitalleştiği bu yeni dönem, insanlara kısa bir zaman öncesinde tüm bu teknolojilerin oldukça kısıtlı kullanımının olduğu ve bu teknolojilere ulaşımın oldukça maliyetli olduğu dönemleri çok çabuk bir şekilde unutturmuştur. Artık akıllı telefonlar ve bilgisayarlar gündelik hayatın doğal bir parçası haline dönüşmüş ve insanoğlu bu değişime oldukça kısa bir sürede uyum sağlamıştır. İnsanların yanlarından bir an olsun ayırmadıkları cep telefonları artık günlük hayatın vazgeçilmez bir parçası haline gelen bilgi ve iletişim teknolojilerinin her an her yerde kullanımını mümkün kılmaktadır. Bilginin dijital ortamlarda saklanarak işlendiği dijital çağda yeni değerler de ortaya çıkmıştır. Kişisel verilerin gizliliği, sosyal medya platformlarında oluşturulan profillerin nasıl göründüğü, kişilerin bu platformlarda kaç kişi tarafından takip edildiği veya paylaştıkları bir

fotoğrafın kimler tarafından beğenildiği konuları dijital hayatın yeni değerleri olarak karşımıza çıkmaktadır.

İnsanların dijitalleşen hayatı yaşadıkları mekanları da etkilemiş ve bu bağlamda artık mekanlar da dijitalleşmeye başlamıştır. Akıllı ev, akıllı buzdolabı, akıllı çamaşır makinası, akıllı televizyon gibi kavramların hayatımıza girdiği günümüzde artık kentler de akıllı hale gelmeye başlamıştır. Bilgi ve iletişim teknolojilerinin kent yönetimlerinde aktif olarak kullanılmaya başlanması, dünya nüfusunun çok büyük bir kısmını barındıran kentlerin de teknolojiyle iç içe girmesine izin vermiştir. Toplu taşıma, elektrik, su ve doğalgaz dağıtımı, belediye hizmetleri veya sosyal aktivitelerin kontrolü özellikle büyük metropollerde bilgi ve iletişim teknolojilerinin getirdiği yeniliklerle çok daha kolay bir şekilde yönetilebilir hale gelmeye başlamıştır. Binlerce sensör yardımıyla trafik yoğunluğu, hava kirliliği, insan trafiği, enerji kullanımı ve kentlerde yaşayan insanların günlük hayattaki alışkanlıkları takip edilerek matematiksel veriler oluşturulmaya başlanmıştır. Elde edilen bu verilerin analiz edilmesiyle ortaya çıkan sonuçlar kapsamında kent yönetimini daha verimli bir hale getirmeye çalışan belediyeler, akıllı kentler denilen bu yeni mekanlarda daha iyi bir yönetim anlayışı içerisinde kentleri yönetmeyi hedeflemektedirler.

Kentlerin yönetiminde bilgi ve iletişim teknolojilerinin bu kadar yoğun olarak kullanılması ise beraberinde yeni tehditleri de ortaya çıkartmıştır. Siber uzayın bir parçası olan bu teknolojilere yapılacak siber saldırılar, kent yönetimini verimli hale getirmeye çalışırken büyük felaketlere de yol açabilecek fırsatları da doğurmaktadır. Büyük oranla bilgi ve iletişim teknolojileri aracılığıyla yönetilen akıllı kentlerin bu sistemlerine yapılacak planlı bir siber saldırı kent trafiğini alt üst edebilme, enerji dağıtımını kesintiye uğratma ya da toplu taşıma sistemlerinin felç olabilmesi olasılıklarını barındırmaktadır. Kentlerin akıllı hale getirilmesinin yanında yöneticiler bu yeni akıllı sistemlerin güvenliğini de düşünerek siber güvenlik yatırım ve projelerine de yatırım yapmalıdırlar. Ortaya çıkabilecek potansiyel bir siber saldırının önlenmesi, zararın en aza indirilmesi ve en kısa sürede saldırıya uğrayan sistemlerin eski haline döndürülmesi adına yedi gün yirmi dört saat çalışan ve bilgi ve iletişim sistemlerinin güvenliğini sağlayan ekiplerin olması bu anlamda hayati önem taşımaktadır. Artık birçok kent yönetiminde bu sistemlerin güvenliğini sağlayan

ekipler çalışıyor olsa da her gün artan siber tehditler daha çok yetişmiş personel ihtiyacını ortaya çıkartmaktadır. Dolayısıyla kent yönetimleri mekanları dijitalleştirirken aynı zamanda bu mekanların güvenliğini sağlayacak personellerin yetiştirilmesi amacıyla eğitim yatırımları da yapmalıdır.

Mekanların dijitalleşmesi ve kablosuz ağların kullanım alanının yaygınlaşması her an birbiriyle bağlantılı bir şekilde çalışan ve hayatı yönlendiren teknolojilerin yeni bir alan oluşturmasına yol açmıştır. Siber uzay ya da siber alan olarak adlandırılan ve tamamen insan eliyle üretilmiş bu yeni alan artık birçok ülke ve uluslararası kuruluş tarafından varlığı kabul edilmiş yeni bir mücadele alanı haline dönüşmüştür. NATO'nun kara, hava ve denizden sonra dördüncü, ABD'nin ise kara, hava, deniz ve uzaydan sonra beşinci muharebe alanı olarak kabul ettiği bu yeni alan ülkelerin bu alanda operasyonel kapasitelerini geliştirmek amacıyla teknoloji üretmeye başlamalarına neden olmuştur. Bu bağlamda NATO kendi bünyesinde Müşterek Siber Savunma Mükemmeliyet Merkezi'ni oluşturarak ittifak üyesi ülkeler arasında siber uzayda güvenliğin sağlanması ve savunma kapasitelerinin geliştirilmesi adına önemli çalışmalar yürütmektedir. Ek olarak ülkelerin silahlı kuvvetler çatısı altında oluşturdukları siber savunma komutanlıkları, siber olaylara müdahale ekipleri ve siber savunma merkezleri bu yeni alanın güvenlikleştirilmesi adına yapılan önemli çalışmalardır. Realist teori kapsamında ortaya atılan güvenlikleştirme kavramının siber uzayın gerçek dünyaya yansıması şeklinde değerlendirilebilecek bu adımlar, bu alanın güvenliğinin sağlanmasının ne kadar önemli olduğunun da bir göstergesidir.

Siber uzay, bu alanı oluşturan teknolojilerin her türlü bileşenini içeren bir alandır. Bilgisayarlar, bilgisayarları oluşturan her türlü fiziksel donanım, internet, internet bağlantısını sağlayan fiber optik kablolar, kablosuz internet ağları ve yazılımlar siber uzayın bir parçası olarak değerlendirilmelidir. Dolayısıyla siber uzayda ortaya çıkan tehditler sadece internet vasıtası ile gerçekleştirilecek siber saldırılar olarak algılanmamalıdır. Siber uzayı oluşturan fiziksel altyapılara yapılacak bir saldırı da aynı zamanda bir siber tehdit olarak algılanmalı ve bu altyapıların güvenliğinin sağlanması adına da önlemler alınmalıdır. Siber uzayın güvenliğinin tam olarak sağlanması ancak hem fiziksel hem de donanımsal olarak siber uzayın bileşenlerinin bir bütün şeklinde güvenliğinin sağlanması ile gerçekleştirilebilecektir.

Siber uzay, coğrafi olarak sınırları bulunmayan, zamandan ve mekândan bağımsız bir alandır. Dolayısıyla yeterli teknolojik imkanların sağlandığı her mekân siber uzayda iş ve işlem yapabilme kabiliyeti sağlamaktadır. Dünyanın herhangi bir yerinde herhangi bir zamanda bir başka ülkenin siber uzayını oluşturan sistemlere saldırı gerçekleştirilebilir. Saldırıyı gerçekleştiren kişi, kurum, kuruluş ya da devletin kendisi de olabilir. Sınırları olmayan bu yeni alanının güvenliğinin sağlanması bu anlamda uluslararası bir iş birliğini gerekli kılmaktadır. Oldukça karmaşık ve sınırsız olan bu alanın güvenliğinin sağlanması adına yapılan uluslararası anlaşmalar oldukça kısıtlı ve yetersizdir. Siber uzayın uluslararası anlamda kontrolünü sağlayan bir anlaşma ya da kurallar bütününden bahsetmek mümkün değildir. Dolayısıyla devletler kendi kontrol alanlarında yaptıkları yasal düzenlemeler ve oluşturdukları kurumlar aracılığı ile bu alanın güvenliğini sağlamaya çalışmaktadır. Avrupa Siber Suçlar Sözleşmesi ise bu alanın güvenliğinin sağlanması adına yapılmış ilk ve belki de uluslararası niteliğe sahip tek anlaşma olarak değerlendirilebilir. Siber uzayda işlenen suçlarla mücadelede taraf ülkelerin mevzuatında uyumluluğun sağlanması adına hazırlanmış bu anlaşma, bu alanda gerçekleşecek suçlarla uluslararası anlamda mücadele edilmesi anlamında oldukça önemlidir. Siber güvenliğin sağlanmasında uluslararası anlaşmaların ve iş birliğinin eksikliği bu alanın tam anlamıyla güvenli bir yer olmasını engelleyen en önemli unsur olarak değerlendirilmektedir.

Siber uzayda ortaya çıkan tehditler ülkelerin bilgi ve iletişim sistemlerinin yanında kritik altyapılar olan enerji, finans, savunma ve üretim sektörlerini de büyük tehlike altına sokmaktadır. Ek olarak her geçen gün çeşitlenen siber tehditler ülkelerin siber uzayın güvenliğini sağlamaları adına yaptığı çalışmaları sürekli güncellemesini gerekli kılmaktadır. Artık konvansiyonel anlamda gerçekleşen saldırıların birçoğu siber uzayın beraberinde getirdiği teknoloji aracılığıyla çok daha kolay, masrafsız ve oldukça düşük risklerle gerçekleştirilebilecek boyuta gelmiştir. Ayrıca siber uzayda gerçekleşen başarılı bir saldırının etkileri geleneksel anlamda yapılan saldırılardan çok daha etkili olabilecek kapasiteye sahiptir. Bir ülkenin su dağıtım şebekelerini kontrol eden sistemlere yapılacak bir siber saldırı, bu sistemlerin düzensiz çalışarak içme suyunun kirlenmesine ve milyonlarca kişinin etkilenmesine neden olabilir. Ya da yoğun bir hava trafiği olan bir hava alanının kule kontrol sistemlerinin ele geçirilmesi oldukça büyük bir felakete yol açabilir. Tüm bu olasılıklar dahilinde ülkeler siber

güvenlik anlamında bütün ihtimalleri göz önünde bulundurarak gerekli çalışmaları yapmalıdırlar.

Siber uzayla birlikte suçun ve saldırının büyük bir değişime uğradığını söylemek mümkündür. Özellikle artık uluslararası bir sorun olarak değerlendirilen terörün de siber uzayda kendisine yer bulması, ülkelerin siber teröre karşı önlem almasını gerektiren bir durum haline gelmiştir. Terörist oluşumlar siber uzayın getirdiği kolaylıklardan mümkün olduğunca faydalanarak eylemlerinin kapasitelerini geliştirme çabası içerisine girmişlerdir. Örgüt kapasitesinin geliştirilmesi adına yeni sempatizan ve destekçilerin bulunması, bu anlamda propaganda çalışmalarının yapılması, örgüt üyeleri arasında iletişimin gerçekleştirilmesi ya da yapılacak olan eylemlerin planlanması siber uzayın getirdikleri sayesinde artık çok daha kolay bir şekilde gerçekleştirilebilmektedir. Örneğin Google Earth uygulaması ile herkesin erişebileceği uydu görüntüleri terörist oluşumlar için büyük bir nimet niteliği taşımaktadır. Ya da internet ile bilgiye erişimin oldukça kolay olduğu günümüzde basit bir arama sonucu elde edilecek tarifle herhangi bir yapı marketten alınabilecek ürünler kullanarak etkili bir patlayıcı yapmak oldukça basit bir hale gelmiştir. Tüm bunların yanında siber uzayda gerçekleştirilecek tüm bu eylemler çok daha az masraflı, daha az tehlikeli ve yakalanma riski oldukça düşüktür. Ülkeler siber terörizmle mücadelede özellikle yasal düzenlemelerini daha güçlü hale getirerek bu alanda gerçekleşen faaliyetlerin takibini oldukça dikkatli bir şekilde yapmalıdır. Yasal düzenlemeler ise bu anlamda oldukça gereklidir. Özellikle kişilerin siber uzaydaki hareketlerinin takip edilebilmesi ve bunu gerçekleştirirken temel hak ve özgürlüklerin ihlal edilmeden yapılabilmesi adına yasal düzenlemeler hayati önem taşımaktadır.

Siber uzay, güvenlik bağlamında birçok kavramında dönüşüme uğramasına neden olmuştur. Bu kavramların başında ise Soğuk Savaş döneminde ülkelerin ulusal güvenliklerini sağlamak adına girdiği silahlanma yarışının bir sonucu olarak ortaya çıkan "caydırıcılık" kavramı gelmektedir. Soğuk Savaş dönemi boyunca ülkelerin özellikle nükleer silah edinimi sonucunda ortaya çıkan nükleer caydırıcılık olgusu, siber tehditlerin artması ve ülkelerin siber uzayın güvenliğini sağlamak adına giriştiği teknoloji edinimi yarışı sonrasında siber caydırıcılık kavramının ortaya çıkmasına neden olmuştur. Nükleer caydırıcılığın yerini siber caydırıcılığın almaya başladığı tartışmaları önem kazanmaya başlamıştır. Artık ülkelerin önemli savunma sistemleri

de dahil olmak üzere finans, enerji, iletişim, ulaşım ve üretim sektörlerinin çok büyük bir kısmının kontrolü bilgi ve iletişim teknolojileri aracılığı ile gerçekleşmektedir. Dolayısıyla bu teknolojilere yapılacak bir siber saldırı tüm bu sistemlerin işlevsiz bir hale gelmesine neden olabilir. Bu kapsamda siber caydırıcılığın nükleer caydırıcılığın yerini aldığını söylemek tam olarak mümkün olmasa da nükleer caydırıcılık kadar önemli bir konu haline geldiğini söylemek yanlış olmayacaktır. Dolayısıyla ülkeler siber uzayda caydırıcılığa sahip olmak adına savunma ve saldırı kapasitelerini güçlendirmeye devam edeceklerdir.

Siber uzayın dönüşüme uğrattığı bir diğer kavram ise bu çalışmanın da ana konusunu oluşturan "güvenlik" kavramı olmuştur. Güvenlik, tarih boyunca dönemin şartlarına bağlı olarak farklı şekillerde algılanmıştır. İlk olarak yırtıcı hayvanlar ve çetin hava şartlarından korunma anlamında insan oğlunun hayatına giren güvenlik kavramı, insanların toplu olarak bir arada yaşamaya başlaması ile dışarıdan gelecek olan tehditlerden korunma olarak algılanmaya başlamıştır. Toplumlar ve devletlerin ortaya çıkmasıyla birlikte başlayan savaşlar neticesinde bu savaşlardan korunma anlamına dönüşen güvenlik kavramı, dünya savaşları döneminde ulusal güvenlik, soğuk savaş döneminde ise nükleer saldırılardan korunma anlamında caydırıcılığın kazanılması şeklinde algılanmıştır. Terör saldırılarının 1990'lı yıllarda artması ve 2001'de gerçekleşen 11 Eylül saldırılarıyla birlikte terörle mücadele olarak algılanan güvenlik kavramı, günümüzde bilgi ve iletişim teknolojilerinin kullanımının artmasıyla birlikte siber uzayda güvenliğin sağlanması olarak da algılanmaya başlanmıştır. Kişisel verilerin korunması, veri güvenliği, kritik altyapıları kontrol eden sistemlerin güvenliği, internetten yapılan alışverişlerde güvenli ödemelerin yapılabilmesi veya bilgi güvenliği şeklinde algılanmaya başlanan kavram, siber güvenlik olgusunu oldukça önemli bir hale getirmiştir.

Siber uzayın beraberinde getirdiği siber güvenlik olgusu teorik çalışmalarda da kendisine yer bulmuştur. Sınırları olmayan bu alanın güvenliği konusu özellikle uluslararası ilişkiler teorileriyle açıklanmaya çalışılan bir kavramdır. İdealizm, liberalizm, realizm ve neo-realizm temelinde çalışılan birçok konuyla bağlı bir şekilde açıklanabilecek ve teorik bir çerçeveye oturtulabilecek siber güvenlik kavramı, özellikle idealizm ve kolektif güvenlik düşünceleri ile uluslararası iş birliğinin sağlanması gereken bir konudur. Liberalizm temelinde gelişen özgür düşünce ve

serbest piyasa olgusu ise siber uzayın temel yapısıyla örtüşen bir nitelik göstermektedir. Realizm ve neo-realizm düşüncelerinde kendisine yer bulan güvenlik olgusu ise özellikle devletlerin siber savunma ve saldırı kapasitelerini geliştirme yarışında sadece kendi kaynaklarına güvenmeleri, bu yarışın bir güvenlik ikilemi oluşturması nedeniyle devletlerin siber uzayda kendilerini güvenli olarak hissetmemesi ve aynı zamanda yapılan yasal düzenlemeler ve oluşturulan kurumlarla bu alanın güvenlikleştirilme çabaları bağlamında siber güvenliğin doğasıyla örtüşmektedir.

Siber uzayın karmaşık ve kontrolsüz yapısı, beraberinde getirdiği dijitalleşme kavramı ve bu durumun hayatın her alanına dokunmasıyla birlikte toplumların da dijitalleşmesi durumu ise bu yeni alanın kontrolü ve yönetiminin egemen bir otorite tarafından gerçekleştirilmesi gerektiği tartışmalarını ortaya çıkartmıştır. Bu bağlamda toplum sözleşmesi teorilerinin ortaya koyduğu doğa durumu ve egemen güç kavramı, siber uzayın yasal ve yönetsel olarak düzenlenmesi olgusunu açıklar niteliktedir. Bu noktada gerçek hayatı düzenleyen yasal düzenlemelerin siber uzayı da düzenleyebileceğini savunan düşüncelerle bu alanın gerçek hayattan tamamen farklı olduğunu savunan ve gerçek hayattan farklı olan yasal düzenlemelerin ancak bu alanı yönetebileceğini savunan düşünceler birbiriyle çatışmaktadır. Toplum sözleşmesi düşüncesinin insanın doğa durumunun anarşi içerisinde olduğu yaklaşımı siber uzayın kontrolsüz ve özgür yapısını açıklar niteliktedir. Fakat toplum sözleşmesi düşünceleri kapsamında insanların bu durumdan çıkarak sahip oldukları hakların bir kısmını veya tamamını bir üst otoriteye devretmesi durumu siber uzay için hala oldukça erken ve zor bir durum olarak değerlendirilebilir. İnsanların özgürce fikri ve düşüncelerini paylaşabildiği bu karmaşık düzen içerisinde bir üst otorite tarafından kısıtlanma düşüncesi kolay kabul edilebilir bir düşünce olarak değerlendirilmemektedir. Fakat günden güne tehditlerin arttığı, suç oranlarının yükseldiği ve çeşitlendiği bu yeni alanın güvenliğinin sağlanması için gereken egemen yapının gerekliliği de ortadadır.

Türkiye siber uzayın güvenliğinin sağlanmasının gerekliliğini her ne kadar erken fark eden ve bu anlamda yasal düzenlemeler yapan ve oluşturduğu kurum ve kuruluşlarla önemli çalışmalara imza atan bir ülke olsa da sürekli değişen ve gelişen bu yeni alanın güvenliğini sağlamada oldukça önemli yapısal eksikliklere sahiptir. İlk olarak 1990'lı yılların başında TCK'da yaptığı değişikliklerle bu alanın yasal olarak

düzenlenmesi adına adım atan Türkiye, 2000'li yıllar itibari ile bu yasal düzenlemelere hız kazandırmış ve oluşturmuş olduğu kurumsal yapılanmalarla siber güvenliğin öneminin farkında olarak önlemler almaya başlamıştır.

Türkiye'de siber uzayı düzenleyen tek bir kanunun bulunmaması zaten oldukça karmaşık bir yapıya sahip olan bu alanın düzenlenmesini daha da karmaşık hale getirmektedir. Siber uzayda gerçekleşen suçlarla mücadelede yapılan düzenlemeler suçla mücadelede yasal bir zemin oluşturmuş olsa da birçok konuda eksiklik hala varlığını sürdürmektedir. Özellikle TCK'nın Bilişim Alanında Suçlar başlığı altında düzenlenen suç unsurları, siber uzayda işlenen suçları tamamen kapsayıcı bir nitelikte değildir. Budapeşte Sözleşmesi kapsamında TCK'da yapılan düzenlemeler siber uzayda suçla mücadele anlamında olumlu bir gelişme olarak değerlendirilmektedir. Lakin daha önce detaylarıyla incelenen ve bilişim teknolojileri kullanarak veya aracılığıyla işlenen suçlar olarak değerlendirilebilecek eylemlerin ayrı bir bölümde tanımının yapılmaması, işlenen suçların bu teknolojiler aracılığıyla işlenmesi halinde uygulanacak olan cezai müeyyidelerin büyük oranda belirlenmemiş olması ve diğer birçok kanunla bağlantılı olarak işlenen bu suçların değerlendirilmesi siber suçlarla mücadeleyi zorlaştırmaktadır. Siber uzayı düzenleyen tek bir kanunun bulunmaması durumu, suçun işlenmesinin ardından başlayan soruşturma ve kovuşturma süreçlerini uzatmaktadır. Artık gerçek hayatta işlenen suçların büyük çoğunluğunun siber uzayda işlenebilir hale gelmesi ya da siber uzayın beraberinde getirdiği teknolojiler aracılığıyla işlenebilmesi, siber uzayda güvenliğin sağlanması adına bir siber suçlar ceza kanunu düzenlemesine gidilmesini gerekli kılmaktadır.

İnternet ortamında işlenen suçlarla mücadele noktasında çıkartılan 5651 sayılı "İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun" oldukça önemli bir düzenlemedir. Lakin 2020 ve 2022 yıllarında bu Kanun'da yapılan değişiklikler beraberinde büyük tartışmaları da getirmiştir. Kamuoyunda "Sosyal Medya Düzenlemesi" ve "Sansür Yasası" olarak anılan bu düzenlemeler Türkiye'nin basın ve ifade özgürlüğü konularında uluslararası bağlamda prestijini düşürmüştür. Kullanıcı sayıları milyonları aşan sosyal medya platformlarının ulusal güvenliğin sağlanması adına yasal düzenlemelere tabii olması bir gerekliliktir. Lakin yapılan bu yasal düzenlemelerin temel hak ve özgürlükler kapsamında tartışmalara yer vermeyecek

şekilde gerçekleştirilmesi gerekmektedir. Özellikle erişimin engellenmesi ve bazı içeriklerin yayından kaldırılması kararlarının verilmesinde adil yargılama ve şeffaflık prensipleri göz önünde bulundurularak yeni düzenlemelere gidilmesinin gerektiği değerlendirilmektedir.

Türkiye'de siber uzayın güvenliğinin sağlanması amacıyla 5809 sayılı Elektronik Haberleşme Kanunu, 5070 sayılı Elektronik İmza Kanunu ve 6698 sayılı Kişisel Verilerin Korunması Kanunu ile Ulusal Siber Güvenlik Çalışmalarının Yürütülmesi, Yönetilmesi ve Koordinasyonuna İlişkin Bakanlar Kurulu Kararı, Kamu Kurum ve Kuruluşlarının KamuNet'e Dahil Edilmesi Hakkında Genelge ve Bilgi ve İletişim Güvenliği Tedbirleri Hakkında Cumhurbaşkanlığı Genelgesi bu alanın güvenliğinin sağlanması adına yapılan önemli düzenlemeler ve verilen önemli kararlardır. Lakin Türkiye'nin 1980'li yıllardan bu yana mücadele ettiği terör sorununu yasal zeminde düzenleyen Terörle Mücadele Kanunu'nda siber terörizmle ilgili olarak herhangi bir düzenlemenin yapılmamış olması oldukça büyük bir eksiklik olarak değerlendirilmektedir. Bahsi geçen tüm yasal düzenlemeleri içeren tek bir kanunun oluşturulması siber uzayın güvenliğinin sağlanmasında güçlü bir yasal zemine sahip olmak adına oldukça önemlidir.

İlk defa 2013-2014 yıllarını kapsayacak şekilde hazırlanan Ulusal Siber Güvenlik Stratejisi ve Eylem Planları çalışmaları ise Türkiye'nin siber güvenlik noktasında izleyeceği yol ve yöntemlerin belirlenmesi adına oldukça önemlidir. Fakat ilk defa hazırlanmasının ardından 2016-2019 ve sonrasında 2020-2023 dönemlerini kapsayacak şekilde hazırlanan bu çalışmalar genellikle birbirinin tekrarı şeklinde hazırlanmış ve yapılan ufak değişikliklerle kamuoyuna sunulmuştur. Özellikle bir önceki dönemde belirlenen stratejik eylemlerin ne aşamada gerçekleştirildiği ve hangi hedeflere ulaşıldığını açıklayan herhangi bir çalışmanın olmaması ise belirlenen stratejik eylemlerin ve planlamaların gerçekleşip gerçekleşmediği hususunda soru işaretleri oluşturmaktadır. Ayrıca her çalışmada üzerinde durulan şeffaflık ve hesap verilebilirlik ilkeleriyle de çelişen bu durum yapılan çalışmalarda belirlenen hedeflerin sadece kâğıt üzerinde kaldığı düşüncesini ortaya çıkartmaktadır. Tüm bunlara ek olarak saniyelerin bile önemli olduğu siber uzayın güvenliği konusunda hazırlanan bu çalışmaların dörder yıllık süreler için hazırlanması ve bu süreler içerisinde herhangi bir güncellemeye tabi tutulmaması ise oldukça büyük bir eksikliktir. En son 2020-2023

yıllarını kapsayacak şekilde hazırlanan Ulusal Siber Güvenlik Stratejisi ve Eylem Planı çalışması sonrasında bu satırların yazıldığı 2023 yılının son döneminde hala yeni bir çalışma yayımlanmamıştır.

Türkiye'nin uluslararası boyutta siber güvenliğin sağlanması adına yaptığı iş birlikleri ve çalışmalar ise oldukça yetersizdir. Üyesi olduğu NATO bünyesinde yapılan siber savunma tatbikatlarına katılım sağlayan Türkiye, aynı zamanda uluslararası bazı kuruluşlara da üyelikleri vardır. Fakat siber uzayın sınırları olmayan küresel yapısı bağlamında değerlendirildiğinde bu iş birliği çalışmaları oldukça yetersizdir. Türkiye, ulusal güvenliğini tam olarak sağlayabilmek adına siber uzayın güvenliğini güvence altına alacak uluslararası iş birliği çalışmalarına önem göstermelidir. Özellikle kendi öncülüğünde uluslararası bir siber güvenlik yapılanması Türkiye'nin bu alanda değer kazanmasını ve yatırım almasını sağlayacak bir girişim olacaktır. Yapılan tüm çalışmalara ek olarak uluslararası iş birliği çalışmaları bu anlamda oldukça önemlidir. Unutulmamalıdır ki siber güvenliğin sağlanmasında yapılan çalışmalar uluslararası bir nitelik taşımadığı sürece anlamsız olacaktır. Dolayısıyla Türkiye'nin de taraf olduğu Avrupa Siber Suçlar Sözleşmesi bu anlamda oldukça önemli bir yerde durmaktadır.

Türkiye'de siber uzayın güvenliğinin sağlanması adına oluşturulan kurumsal yapılanmalar ise olumlu olarak değerlendirilmekle beraber bu alanın düzenlenmesi adına tek bir kanunun bulunmadığı gibi tek bir kurumun da bulunmaması durumu büyük bir eksiklik olarak değerlendirilmektedir. Siber uzayın güvenliği konusunda koordinasyonu sağlama görevi Ulaştırma ve Altyapı Bakanlığı ile Bakanlığa bağlı olan Bilgi Teknolojileri ve İletişim Kurumu'na verilmiştir. Fakat 2019 yılında kurulan Cumhurbaşkanlığı Dijital Dönüşüm Ofisi de siber güvenliğin sağlanmasında koordinasyon görevini üstlenmektedir. Özellikle e-Devlet hizmetlerinin geliştirilmesi ve güvenliğinin sağlanmasında koordinasyon görevini üstlenen CDDO, siber uzayda güvenliğin sağlanması adına görev ve sorumluluklar anlamında karmaşıklık ortaya çıkartmaktadır. Ayrıca sürekli değişen kurum adları, oluşturulan yeni kurumlar ve beraberinde gelen yeni görev ve sorumluluklar bu alanın yönetsel bağlamda düzenlenmesini daha da karmaşık bir hale sokmaktadır. Siber uzayın güvenliğinin sağlanmasında düzenleyici kurumlar, siber suçlarla mücadele eden kurumlar, ulusal siber güvenliğin sağlanması adına çalışan kurumlar ve siber güvenlik adına teknoloji

geliştiren kurumlar tek bir çatı altında toplanarak koordinasyon ve iletişim halinde çalışmalıdırlar.

Ulusal siber güvenliğin sağlanmasında teknoloji ve ürün geliştiren kurumlar ise Türkiye'nin siber uzayda milli teknolojiler geliştirerek dışa bağımlılığın azaltılmasında kritik öneme sahip kuruluşlardır. Bu kuruluşların bugüne kadar yaptığı çalışmalar incelendiğinde her ne kadar oldukça önemli çalışmalara imza attıkları görülse de ortaya çıkarttıkları ürünler ve verdikleri hizmetler kapsamında değerlendirildiğinde hala yetersiz oldukları sonucuna ulaşılmaktadır. Özellikle geliştirilen ürünlerin kamu kurum ve kuruluşlarında ne seviyede kullanıldığı ile ilgili olarak herhangi bir çalışma mevcut değildir. Ayrıca ortaya koyulan ürünler hala dünya teknolojisini yakalamakta oldukça geridedir. ASELSAN'ın ürettiği tek çekirdekli milli işlemci ÇAKIL bu noktada önemli bir örneği teşkil etmektedir. Artık yeni nesil akıllı telefonların bile 32 çekirdek işlemci kapasitesiyle üretilebildiği günümüzde tek çekirdekli bir işlemci mevcut teknolojik gelişmeleri yakalamaktan oldukça uzak bir yerde durmaktadır.

Dünyanın önde gelen siber güvenlik firmalarından birisi olan Kaspersky'nin 2023 verilerine göre Türkiye dünyada en çok siber saldırılara uğrayan ülkeler listesinde 27'nci sıradadır (Kaspersky, 2023b). Dolayısıyla Türkiye'nin oldukça yüksek bir siber tehdit riski altında olduğu söylenebilir. Uluslararası Telekomünikasyon Birliği tarafından hazırlanan Küresel Siber Güvenlik İndeksi çalışmasında ise Türkiye 11'inci sıradadır (ITU, 2020). Bu bağlamda değerlendirildiğinde Türkiye siber güvenliğin sağlanmasında oldukça iyi bir yede durmaktadır. Lakin incelendiği üzere bahsedilen eksikliklerin bir an önce giderilmesi bu alanda güvenliğin tam olarak sağlanması adına hayati önem taşımaktadır.

Türkiye siber uzayda güvenliğin sağlanması adına mevcut olan karmaşık durumu düzeltmelidir. Yapılması gereken şey ise siber uzayı düzenleyen tüm yasal düzenlemeleri kapsayan tek bir kanunun oluşturulması gerektiğidir. Burada dikkat edilmesi gerek konu ise özellikle temel hak ve özgürlükler bağlamında bireylerin ifade ve düşünce özgürlüklerini garanti altına alacak yasal düzenlemelerle siber güvenliğin hukuki bir temele oturtulması gerekliliğidir. Ek olarak, yapılacak olan yasal

düzenlemelerde dikkat edilmesi gereken bir diğer önemli husus ise şeffaflık ve hesap verilebilirlik ilkeleri olmalıdır.

Türkiye'de siber güvenliğin sağlanması adına çalışan mevcut kurum ve kuruluşlar tek bir çatı altından yönetilmelidir. Oluşturulacak olan çatı kuruluşun görev ve sorumlulukları hazırlanacak olan kapsayıcı yasal düzenlemede açık bir şekilde belirlenerek denetime tabi tutulmalıdır. Hazırlanan Ulusal Siber Güvenlik Stratejisi ve Eylem Planı çalışmaları kapsamında Türkiye'nin siber güvenlik alanında yapılan çalışmaları oluşturulacak olan çatı kurum koordinasyonunda gerçekleştirilmelidir.

Siber güvenliğin sağlanmasında ihtiyaç duyulan yetişmiş nitelikli insan gücü ihtiyacı ise bu alanın güvenliğinin sağlanmasında hayati öneme sahiptir. Sadece yüksek öğrenim seviyesinde açılacak olan siber güvenlik meslek yüksek okulları ya da dört senelik lisans programları değil aynı zamanda orta öğrenim seviyesinde teknik liselerde siber güvenlik programları oluşturularak yetişmiş insan ihtiyacının karşılanmasına önem verilmelidir.

Türkiye ayrıca siber güvenliğin sağlanmasında ihtiyaç duyulan bütçenin ayrılmasına da önem göstermelidir. Ulusal güvenliğin tam anlamıyla sağlanmasının siber uzayın güvenliğinin sağlanmasından geçtiğinin farkında olarak bu alana yapılacak olan yatırımlar artırılmalıdır. Ayrıca siber güvenlik alanında çalışan özel sektör kuruluşlarına verilen maddi desteğin de önemi oldukça büyüktür. Projeler desteklenmeli ve yeni projeler üretilmesi adına Ar-Ge çalışmalarına önem verilmelidir.

Türkiye'de siber güvenliğin sağlanmasında teknoloji üreten firmaların ortaya koyduğu çalışmalar ve ürünler desteklenerek kullanım alanları artırılmalıdır. Özellikle kamu kurum ve kuruluşlarında kullanılan bilgi ve iletişim teknolojilerinin güvenliğinin sağlanması amacıyla ortaya koyulan yerli teknolojilerin kullanım oranları artırılmalı ve teşvik edilmelidir.

Son olarak Türkiye'nin siber güvenlik alanında nerede olduğunun saptanması adına her yıl detaylı bir rapor hazırlanarak eksiklikler belirlenmeli ve hazırlanacak olan eylem planları ile bu eksikliklerin giderilmesi adına çalışmalar yapılmalıdır. Her an değişen ve gelişen siber uzayın güvenliğinin sağlanması ancak güncel teknolojilerin

takibi ve bu teknolojilerle uyumlu şekilde çalışacak yerli teknolojilerin geliştirilmesiyle mümkün olacaktır.

KAYNAKÇA

2937 sayılı Devlet İstihbarat Hizmetleri ve Millî İstihbarat Teşkilatı Kanunu (1983). https://www.mevzuat.gov.tr/MevzuatMetin/1.5.2937.pdf (Erişim Tarihi: 07 Haziran 2023)

3713 Sayılı Terörle Mücadele Kanunu (1991). https://www.mevzuat.gov.tr/mevzuatmetin/1.5.3713.pdf (Erişim Tarihi: 12 Temmuz 2023)

5070 Sayılı Elektronik İmza Kanunu (2004). https://www.mevzuat.gov.tr/mevzuatmetin/1.5.5070.pdf (Erişim Tarihi: 12 Temmuz 2023)

5237 Sayılı Türk Ceza Kanunu (2004). https://www.mevzuat.gov.tr/MevzuatMetin/1.5.5237.pdf (Erişim Tarihi: 12 Temmuz 2023)

5271 Sayılı Ceza Muhakemesi Kanunu (2004). https://www.mevzuat.gov.tr/mevzuatmetin/1.5.5271.pdf (Erişim Tarihi: 12 Temmuz 2023)

5651 Kanun (2004). https://www.mevzuat.gov.tr/mevzuatmetin/1.5.5651.pdf (Erişim Tarihi: 5 Mayıs 2023)

AA (2016). *"Türk ordusunun yeni "kuvveti"* siber savunma". https://www.aa.com.tr/tr/turkiye/turk-ordusunun-yeni-kuvveti-siber-savunma/584061 (Erişim Tarihi: 17 Haziran 2023)

AA (2021). *"Ankara TEM ekiplerince PKK'nın hacker gruplarına yönelik operasyon*

düzenlendi. https://www.aa.com.tr/tr/gundem/ankara-tem-ekiplerince-pkknin-hacker-gruplarina-yonelik-operasyon-duzenlendi/2440645 (Erişim Tarihi: 1 Mayıs 2023).

AA (2023). *"Banka bilgileri hırsızlığı 2022'de ikiye katlandı."* https://www.aa.com.tr/tr/sirkethaberleri/bilisim/banka-bilgileri-hirsizligi-2022de-ikiye-katlandi/677005 (Erişim Tarih: 07 Haziran 2023)

Ablon, L., Libicki, M. C., & Golay, A. A. (2014). *Markets for Cybercrime Tools and Stolen Data: Hackers' Bazaar.* RAND Corporation.

AK (2023). *Smart cities*. https://commission.europa.eu/eu-regional-and-urban-development/topics/cities-and-urban-development/city-initiatives/smart-cities_en (Erişim Tarihi: 2 Temmuz 2023)

Al Jazeera Turk (2015). "*Suriye Elektronik Ordusu'ndan Türkiye'ye saldırı*." http://www.aljazeera.com.tr/haber/suriye-elektronik-ordusundan-turkiyeye-saldiri (Erişim Tarihi: 1 Haziran 2023)

Al-Rebholz, A. (2017). Kent kuramları: klasikler ve çağdaşlar. M. Talas ve E. Yiğit (Eds.), *Kent Sosyolojis*i (ss. 135-164*)*, İstanbul: Lisans Yayıncılık.

Anayasa Mahkemesi (2014). *30270 Sayılı Karar*. https://kararlarbilgibankasi.anayasa.gov.tr/BB/2014/5552 (Erişim Tarihi: 23 Haziran 2023)

Andress, J. & Winterfeld, S. (2014). *Cyber warfare: techniques, tactics, and tools for security practition*, Elsevier, Amsterdam.

ASELSAN *(2022). Siber Teknolojiler.* https://www.aselsan.com/tr/savunma/kategori/10/siber-teknolojiler?content=bilgi-teknolojileri-sistemleri (Erişim Tarihi: 25 Haziran 2023)

AVAST (2022). *What is Cybercrime and How Can You Prevent It?*. https://www.avast.com/c-cybercrime (Erişim Tarihi: 16 Temmuz 2023)

Avrupa Birliği Başkanlığı (2002). *E-Türkiye Girişimi Eylem Planı.* https://www.ab.gov.tr/p.php?e=22224 (Erişim Tarihi: 15 Mayıs 2023)

Awan, I. (2014). Debating The Term Cyber-Terrorism: Issues and Problems. *Internet Journal of Criminology.*

Badie, B., Berg-Schlosser, D., & Morlino, L. (2011). *International Encyclopedia of Political Science*. https://doi.org/10.4135/9781412994163

Bal, İ. (2006). *Alaca Karanlıkta Terör ile Mücadele ve Komplo Teorileri*, USAK Yayınları.

Baldwin, D. A. (1997). The concept of security. *Review of International Studies*, *23*(1), 5-26. https://doi.org/10.1017/S0260210597000053

Barker, E. (1960). *Social contract: Essays by Locke, Hume, and Rousseau*. Oxford University Press.

Barlow, J. P. (2016). *A Declaration of the Independence of Cyberspace*. Electronic Frontier Foundation. https://www.eff.org/cyberspace-independence (Erişim Tarihi: 1 Temmuz 2023)

Baumgold, D. (2005). Hobbes's and Locke's Contract Theories: Political not Metaphysical. *Critical Review of International Social and Political Philosophy*, *8*(3), 289-308. https://doi.org/10.1080/13698230500187169

Baylis, J. (2008). Uluslararası İlişkilerde Güvenlik Kavramı. *Uluslararası İlişkiler*, 5(18): 69-85.

Bayraktar, G. (2014). Harbin Beşinci Boyutunun Yeni Gereksinimi: Siber İstihbarat. *Güvenlik Stratejileri Dergisi*, *10*(20), 119-148.

BBC News (2026). *"How France's TV5 was almost destroyed by "Russian hackers*".

https://www.bbc.com/news/technology-37590375 (Erişim Tarihi: 17 Haziran 2023)

BBC News Türkçe (2022). *"Dezenformasyonla Mücadele": CHP'li Burak Erbay, yasa teklifini Meclis kürsüsünde çekiçle telefonunu kırarak protesto etti*. https://www.bbc.com/turkce/articles/cedv8w25ey3o (Erişim Tarihi: 23 Mayıs 2023)

Bertram, C. (2013). *Routledge Philosophy GuideBook to Rousseau and the Social Contract*. Taylor and Francis.

BİLGEM SGE (2021). *NATO CCDCoE Daimi Temsilciliği* https://sge.bilgem.tubitak.gov.tr/tr/nato-ccdcoe-daimi-temsilciligi (Erişim Tarihi: 11 Mayıs 2023)

BİLGEM SGE (2022). *Siber Dünyanın En Büyük On Gücü Arasındayız.* https://sge.bilgem.tubitak.gov.tr/tr/haber/siber-dunyanin-en-buyuk-gucu-arasindayiz (Erişim Tarihi: 23 Haziran 2023)

BİLGEM UEKAE (2021). *Kripto Anahtar Yönetim Sistemleri.* https://uekae.bilgem.tubitak.gov.tr/tr/urunler/kripto-anahtar-yonetim-sistemleri (Erişim Tarihi: 23 Haziran 2023)

Bilgin, G. (2019). *Akıllı Şehir Nedir?* https://www.akillisehirler.gov.tr/akilli-sehir-nedir/ (Erişim Tarihi: 2 Temmuz 2023)

Blackburn, S. (2008). *The Oxford dictionary of philosophy* (Rev. 2nd ed.). Oxford University Press.

Booth, K. (2007). *Theory of World Security*. University Press. https://doi.org/10.1017/CBO9780511840210

Bostan, A. & Şengül, G. (2018). Siber Güvenlik Farkındalığı Oluşturma. (Sarıoğlu, Ş.,

& Alkan, M. Ed.). *Siber Güvenlik ve Savunma: Farkındalık ve Caydırıcılık*. Havelsan, 145-165

Boulos, S. (2017). Cyberspace: Risks and Benefits for Society, Security and Development, Ramírez, J. M., & García-Segura, L. A. (Eds.). *The Talinn Manual and Jus as bellu: Some Critical Notes*, 231-242, Springer International Publishing. https://doi.org/10.1007/978-3-319-54975-0

Brauch, H. G. (2008). *Güvenliğin Yeniden Kavramsallaştırılması: Barış, Güvenlik, Kalkınma ve Çevre Kavramsal Dörtlüsü* . Uluslararası İlişkiler Dergisi , Özel Sayı: Güvenlik , 1-47. https://dergipark.org.tr/tr/pub/uidergisi/issue/39260/462351 (Erişim Tarihi: 25 Nisan 2023)

Britannica (2023). *Cybercrime*. https://www.britannica.com/topic/cybercrime (Erişim Tarihi: 16 Temmuz 2023)

BTK (2009). *Siber Güvenliğin Sağlanması: Türkiye'deki Mevcut Durum ve Alınması Gereken Tedbirler*. https://www.btk.gov.tr/uploads/undefined/sg.pdf (Erişim Tarihi: 7 Mayıs 2023)

BTK (2017). *Elektronik Sertifika Hizmet Sağlayıcıları.* https://www.btk.gov.tr/elektronik-sertifika-hizmet-saglayicilari (Erişim Tarihi: 13 Haziran 2023)

BTK (2017). *Siber Güvenlik Kurulu.* https://www.btk.gov.tr/siber-guvenlik-kurulu (Erişim Tarihi: 25 Haziran 2023)

Burgess, E. W. (1925). The growth of the city an introduction to a research project. R.E. Park, E.W. Burgess and R.D. McKenzie (Eds.), *The City-Suggestions for Investigation of Human Behavior in the Urban Environment* (pp. 47-62), The University of Chicago Press.

Buzan, B. (1984). Peace, Power, and Security: Contending Concepts in the Study of International Relations. *Journal of Peace Research*, 21(2), 109–125. https://doi.org/10.1177/002234338402100203

Buzan, B. (1987). *An introduction to strategic studies: Military technology and international relations*. St. Martin's Press.

Buzan, B. (1991). *People, States and Fear: An Agenda for International Security Studies in the Post-Cold War Era*. ECPR Press.

Buzan, B., & Hansen, L. (2009). *The Evolution of International Security Studies*. University Press. https://doi.org/10.1017/CBO9780511817762

Buzan, B., & Wæver, O. (2009). Macrosecuritisation and Security Constellations: Reconsidering Scale in Securitisation Theory. *Review of International Studies*, *35*(2), 253-276. https://www.jstor.org/stable/20542789 (Erişim Tarihi: 5 Nisan 2023)

Carr, E. H. (1964). *The twenty years' crisis, 1919-1939; an introduction to the study of international relations* (1st Harper torchbook ed.). Harper and Row.

Carr, E.H. (2001). *The Twenty Years' Crisis: An Introduction to the Study of International Relations*, New York: Palgrave.

Carter, & Yanes, N. A. (2012). *The iconic Obama, 2007-2009: essays on media representations of the candidate and new president.* McFarland and Company.

Castels, S.& Miller, M. J. (1998). *The Age of Migration*, McMillian Press Ltd.

CBDDO (2022). *Bilgi ve İletişim Güvenliği Rehberi*. https://cbddo.gov.tr/sss/bilgi-iletisim-guvenligi-rehberi/ (Erişim Tarihi: 3 Temmuz 2023)

CBDDO (2023). *Projeler.* https://cbddo.gov.tr/projeler/#3168 (Erişim Tarihi: 27 Haziran 2023)

CCDCoE (2023). *About us.* https://ccdcoe.org/about-us/ (Erişim Tarihi: 3 Mayıs 2023)

CCRS (2017*). Cyber Terrorism Insurance Futures, Cyber Terrorism: Assessment of the Threat to Insurance*. https://www.jbs.cam.ac.uk/wp-content/uploads/2020/08/pool-re-cyber-terrorism.pdf (Erişim Tarihi: 2 Nisan 2023)

CFR (2023). *Tracking State-Sponsored Cyberattacks Around the World*. https://www.cfr.org/cyber-operations (Erişim Tarihi: 14 Mart 2023)

Chen, J.Q. & Dinerman, A. (2018). Cyber Security: Power and Technology, Lehto, M., & Neittaanmäki, P. (Eds.). *Cyber Capabilites in Modern Warfare*. Springer International Publishing. https://doi.org/10.1007/978-3-319-75307-2

CISA (2022). *Critical Infrastructure Security and Resilience.* https://www.cisa.gov/infrastructure-security (Erişim Tarihi: 11 Ekim 2022)

CISCO (2023). *What Is a Cyberattack? - Most Common Types* https://www.cisco.com/c/en/us/products/security/common-cyberattacks.html (Erişim Tarihi: 8 Temmuz 2023)

CNN International (2013). *"Iran says it built copy of captured U.S. drone".* https://edition.cnn.com/2014/05/12/world/meast/iran-u-s-drone-copy/index.html (Erişim Tarihi: 18 Ocak 2023)

Council of Europe Budapest Convention (2004). *The Budapest Convention (ETS No. 185) and its Protocols*. https://www.coe.int/en/web/cybercrime/the-budapest-convention (Erişim Tarihi: 20 Haziran 2023)

Cutts, A. (2009). Warfare and the continuum of cyber risks: A policy perspective. In Czosseck, C., & Geers, K. (Eds.). *The virtual battlefield: Perspectives on cyber warfare* (66-77). IOS Press.

ÇŞB (2019). *Ulusal Akıllı Şehirler Stratejisi ve Eylem Planı.*

https://www.akillisehirler.gov.tr/wp-content/uploads/EylemPlani.pdf (Erişim Tarihi: 13 Temmuz 2023)

CISA (2022). *Federal Information Security Modernization Act.* https://www.cisa.gov/topics/cyber-threats-and-advisories/federal-information-security-modernization-act (Erişim Tarihi: 23 Mayıs 2023)

DataReportal (2022). *Digital 2022: Global Overview Report.* https://datareportal.com/reports/digital-2022-global-overview-report (Erişim Tarihi: 15 Temmuz 2023)

Deibert, R. (2016). *Cyber-Security*. Routledge Handbooks Online. ttps://doi.org/10.4324/9781315753393.ch16

Deibert, R. J., & Rohozinski, R. (2010). Risking Security: Policies and Paradoxes of Cyberspace Security. *International Political Sociology*, *4*(1), 15-32. https://doi.org/10.1111/j.1749-5687.2009.00088.x

Denning, D. (1999). *Activism, hacktivism, and cyberterrorism: the Internet as a tool for influencing foreign policy.* Nautilus Institute for Security and Sustainability. https://nautilus.org/global-problem-solving/activism-hacktivism-and-cyberterrorism-the-internet-as-a-tool-for-influencing-foreign-policy-2/ (Erişim Tarihi: 1 Haziran 2023)

DOD (2015). *The DoD Cyber Strategy.* https://archive.defense.gov/home/features/2015/0415_cyberstrategy/final_2015_dod_cyber_strategy_for_web.pdf (Erişim Tarihi: 29 Haziran 2022)

DOD (2017). *Dictionary of Military and Associated Terms.* https://apps.dtic.mil/sti/pdfs/AD1029823.pdf (Erişim Tarihi: 11 Temmuz 2023)

Dolu,O., Büker, H.& Uludağ, Ş. (2012). *Türk Ceza Adalet Sisteminin Caydırıcılık*

Kapasitesine İlişkin Eleştirel Bir Değerlendirme, Ankara Üniversitesi Hukuk Fakültesi Dergisi, 61(1), 69-106. https://doi.org/10.1501/Hukfak_0000001651

Donnelly, J. (2000). *Realism and international relations*. University Press.

Douzet, F. (2018). *Cyber-Security Challenges* (C. 1). Oxford University Press. https://doi.org/10.1093/oso/9780198790501.003.0031

Douzet, F. (2018). The Handbook of European Defence Policies and Armed Forces. Meijer, H. & Wyss, M. (Eds.), *Cyber-Security Challenges,* Oxford University Press. https://doi.org/10.1093/oso/9780198790501.003.0031

Dowding, K. (2011). Idealism in International Relations. İçinde *Encyclopedia of Power*. SAGE Publications, Inc. https://doi.org/10.4135/9781412994088.n183

DPT (2002). *e-Devlet'e Geçiş Sürecinde KamuNet Çalışmaları.* http://www.bilgitoplumu.gov.tr/wp-content/uploads/2014/04/e-Devlete_Gecis_Surecinde_KAMU-NET_Calismalari.pdf (Erişim Tarihi: 12 Temmuz 2023)

DPT (2004). *e-Dönüşüm Türkiye Projesi Kısa Dönem Eylem Planı 2003-2004*. http://www.bilgitoplumu.gov.tr/Documents/1/Yayinlar/040900_KDEPKitapcik.pdf (Erişim Tarihi: 12 Temmuz 2023)

DPT (2007). *e-Dönüşüm Türkiye Projesi: 2003-2007 Arası Gelişmeler.* http://bilgitoplumu.gov.tr/Documents/1/Icra_Kurulu/071025_IK22.ToplantisiE-DonusumTurkiyeProjesi.pdf (Erişim Tarihi: 12 Temmuz 2023)

Dünya Bankası (2023). *Urban Development, Overview*. https://www.worldbank.org/en/topic/urbandevelopment/overview (Erişim Tarihi: 2 Temmuz 2023)

e-Devlet Kapısı (2023). *E-Devlet İstatistikleri*. https://www.turkiye.gov.tr/edevlet-istatistikleri (Erişim Tarihi: 3 Haziran 2023)

EC (2022). *The EU general data protection regulation (GDPR).* https://www.consilium.europa.eu/en/policies/data-protection/data-protection-regulation/ (Erişim Tarihi: 1 Haziran 2023)

EGM (2019). *Siber Suç Nedir?*. https://www.egm.gov.tr/siber/sibersucnedir (Erişim Tarihi: 16 Temmuz 2023)

EGM (2022). *SSMDB Uluslararası Eğitim Kataloğu*. https://www.pa.edu.tr/egitim-katalogu.html (Erişim Tarihi: 7 Temmuz 2023)

Ermiş, U. (2015). *Siber Caydırıcılık Kavramının Nükleer Caydırıcılık Olgusu ile Karşılaştırmalı Analizi*. Uludağ Üniversitesi Sosyal Bilimler Enstitüsü, (Yayınlanmamış Yüksek Lisans Tezi).

ESB (2021). "*Hakkımızda" Erişim Sağlayıcıları Birliği*. https://www.esb.org.tr/hakkimizda/ (Erişim Tarihi: 10 Haziran 2023)

Eşitli, E.A. (2013). Suçların ve Cezaların Kanuniliği İlkesi. *TBB Dergisi.* http://tbbdergisi.barobirlik.org.tr/m2013-104-1249 (Erişim Tarihi: 12 Temmuz 2023)

FBI (2011). *Cyber Terror*. https://leb.fbi.gov/articles/featured-articles/cyber-terror (Erişim Tarihi: 5 Nisan 2023)

FBI (2016). *Russian Interference In 2016 U.S. Elections*. https://www.fbi.gov/wanted/cyber/russian-interference-in-2016-u-s-elections (Erişim Tarihi: 25 Mayıs 2023)

FIRST (2023a). "*Improving Security Together*. Forum of Incident Response and Security Teams." https://www.first.org/ (Erişim Tarihi: 20 Haziran 2023)

FIRST (2023b). *"Members around the world*." Forum of Incident Response and Security Teams. https://www.first.org/members/map (Erişim Tarihi: 20 Haziran 2023)

Finklea, K. & Theohary, C.A. (2015). Cybercrime: Conceptual Issues for Congress and U.S. Law Enforcement, *Congressional Research Servise*. https://sgp.fas.org/crs/misc/R42547.pdf (Erişim Tarihi: 2 Nisan 2023)

Gibson, W. (1994). *Neuromancer* (1st Ace hardcover ed.). Ace Books.

Gilpin, R. G. (1996). No one loves a political realist. *Security Studies*, *5*(3), 3-26. https://doi.org/10.1080/09636419608429275

Glaser, C. L. (1997). The Security Dilemma Revisited. *World Politics*, *50*(1), 171-201. https://doi.org/10.1017/S0043887100014763

Goldsmith, J. L. (1998). Against Cyberanarchy. *The University of Chicago Law Review*, *65*(4), 1199-1250. https://doi.org/10.2307/1600262

Gonzalez, M. D. (2015). International Perspectives of Cyber Warfare. *International Journal of Cyber Warfare and Terrorism*, *5*(4), 59-68. https://doi.org/10.4018/IJCWT.2015100103

Graves, K. (2010). *CEH Certified Ethical Hacker Study Guide: Certified Ethical Hacker Study Guide*. John Wiley & Sons, Incorporated.

Green, J. A. (2015). *Cyber Warfare: A multidisciplinary analysis* (1st ed.). Routledge. https://doi.org/10.4324/9781315761565

Güntay, V. (2016). *Uluslararası İlişkiler Temelinde Siber Güvenlik: Mikro Siber İttifak Teorisi (Micro-Cat)*, Karadeniz Üniversitesi Sosyal Bilimler Enstitüsü (Yayınlanmamış Doktora Dezi).

Güntay, V. (2017). Uluslararasi Sistem Ve Güvenlik Açisindan Değişen Savaş Kurgusu; Siber Savaş Örneği. *Güvenlik Bilimleri Dergisi*, *6*(2), 81-108. https://doi.org/10.28956/gbd.354150

Güntay, V. (2019). 21. Yüzyıl Paradoksu Olarak Siber Uzay ve Uluslararası Hukuk. *Novus Orbis: Siyaset Bilimi ve Uluslararası İlişkiler Dergisi*, *1*(2), 87-109.

Hadnagy, C. (2018). *Social engineering: The science of human hacking* (Second edition.). Wiley.

Hartz, E., & Nielsen, C. F. (2015). From conditions of equality to demands of justice: Equal freedom, motivation and justification in Hobbes, Rousseau and Rawls. *Critical Review of International Social and Political Philosophy*, *18*(1), 7-25. https://doi.org/10.1080/13698230.2014.995498

Harvey, D. (1985). *The urbanization of capital.* Oxford: Basil Blackwell.

Harvey, D. (2006). *Sosyal adalet ve şehir.* (Çev. M. Moralı). İstanbul: Metis Yayınları.

Harvey, D. (2012). *Rebel cities-from the right to the city to the urban revolution*. London: Verso.

Hathaway, M.E. & Klimburg, A. (2012). Preliminary Considerations: On National Cyber Security. *National Cyber Security Framework Manual*. https://www.belfercenter.org/sites/default/files/files/publication/hathaway-klimburg-nato-manual-ch-1.pdf (Erişim Tarihi: 12 Temmuz 2023)

HAVELSAN (2023). *Bilgi ve İletişim Teknolojileri*. https://www.havelsan.com.tr/sektorler/bilgi-ve-iletisim (Erişim Tarihi: 25 Haziran 2023)

HAVELSAN (2023). *Şirket Profili.* https://www.havelsan.com.tr/kurumsal/hakkimizda/sirket-profili (Erişim Tarihi: 25 Haziran 2023)

Healy, J. & Jordan, K.T. (2014). *Nato's Cyber Capabilities: Yesterday, Today, and Tomorrow*, Atlantic Council. https://www.atlanticcouncil.org/wp-content/uploads/2014/08/NATOs_Cyber_Capabilities.pdf (Erişim Tarihi: 15 Ocak 2015)

Henry, K. (2011). *Liberalism and the culture of security the nineteenth-century*

rhetoric of reform. University of Alabama Press.

Herz, J. H. (1950). Idealist Internationalism and the Security Dilemma. *World Politics*, *2*(2), 157-180. https://doi.org/10.2307/2009187

Herz, J. H. (1951). *Political realism and political idealism, a study in theories and realities.* University of Chicago Press.

Hobbes, T. (2017). *Leviathan*. Electronic Book.

Horowitz, S.J. (2006). *As Boundries Fade: The Social Contract in Cyberspace*. Temple University. http://dx.doi.org/10.34944/dspace/423

Housley, W. (2022). *The SAGE handbook of digital society*. Sage Publishing.

Huot, J.L, Thalmann, J.P. and Valbelle, D. (2000). *Kentlerin doğuşu*. (Çev. Ali Bektaş Girgin), Ankara: İmge Kitabevi.

IBM (2023). *"What is a phishing attack?"*https://www.ibm.com/topics/phishing (Erişim Tarihi: 8 Temmuz 2023)

IEP (2022). *Global Terrorism Index 2022: Measuring the impact of terrorism*. https://www.economicsandpeace.org/wp-content/uploads/2022/03/GTI-2022-web-09062022.pdf (Erişim Tarihi: 16 Ocak 2023)

IMF (2022). *World Economic Outlook: GDP, current prices*. gönderen https://www.imf.org/external/datamapper/NGDPD@WEO (Erişim Tarihi: 20 Mart 2023)

InfoSec, (2012). *Cyberterrorism Defined (as distinct from "Cybercrime") - InfoSec Resources.* http://resources.infosecinstitute.com/cyberterrorism-distinct- (Erişim Tarihi: 18 Mart 2022)

ITU (2020). *Global Cybersecurity Index*. https://www.itu.int:443/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx (Erişim Tarihi: 14 Temmuz 2023)

Jervis, R. (1978). Cooperation under the Security Dilemma. *World Politics, 30(2), 167-214. https://doi.org/10.2307/2009958*

JGK SSMDB (2022). *Siber Suçlarla Mücadele*. https://www.jandarma.gov.tr/siber (Erişim Tarihi: 24 Haziran 2023)

Johnson, D. R., & Post, D. (1996). Law and Borders: The Rise of Law in Cyberspace. *Stanford Law Review*, *48*(5), 1367-1402. https://doi.org/10.2307/1229390

Johnson, S. (2022). *The Hold Me Tight Workbook: A Couple's Guide for a Lifetime of Love* (Workbook edition). Little, Brown Spark.

Junio, T. J. (2013). How Probable is Cyber War? Bringing IR Theory Back In to the Cyber Conflict Debate. *Journal of Strategic Studies*, *36*(1), 125-133. https://doi.org/10.1080/01402390.2012.739561

Kalkınma Bakanlığı (2015). *2015-2018 Bilgi Toplumu Stratejisi ve Eylem Planı.* http://www.sp.gov.tr/tr/temelbelge/s/109/Bilgi+Toplumu+Stratejisi+ve+Eylem+Plani+_2015-2018 (Erişim Tarihi: 11 Mayıs 2023)

Kalkman, J. P., & Wieskamp, L. (2019). Cyber Intelligence Networks: A Typology. *The International Journal of Intelligence, Security, and Public Affairs*, *21*(1), 4-24. https://doi.org/10.1080/23800992.2019.1598092

Kant, I. (1798). *Essays and treatises on moral, political, and various philosophical subjects. By Emanuel Kant, ... From the German by the translator of the principles of critical philosophy* (C. 1). printed for the translator; and sold by William Richardson.

Kaspersky (2022a). "*What is Social Engineering?"* https://usa.kaspersky.com/resource-center/definitions/what-is-social-engineering (Erişim Tarihi: 1 Temmuz 2023)

Kaspersky (2022b). *What is Spoofing – Definition and Explanation*.

https://usa.kaspersky.com/resource-center/definitions/spoofing (Erişim Tarihi: 24 Nisan 2023)

Kaspersky (2023a). *What is cybercrime? How to protect yourself from cybercrime.* https://www.kaspersky.com/resource-center/threats/what-is-cybercrime (Erişim Tarihi: 1 Mart 2023)

Kaspersky (2023b). *MAP/Kaspersky Cyberthreat real-time map*. https://cybermap.kaspersky.com (Erişim Tarihi: 14 Temmuz 2023)

Keleş, R. (2012). *Kentleşme politikası*. Ankara: İmge Kitabevi.

KGM (2023). *Türkiye'de Kullanılan İlk Bilgisayar.* https://www.kgm.gov.tr/Sayfalar/KGM/SiteTr/Galeri/IlkBilgisayar.aspx (Erişim Tarihi: 5 Haziran 2023)

Kim, J. Y. (2015). The Evolution of Security in Human History. *Journal of Military and Strategic Studies,* 17(1), 1-23.

Kneuer, M., & Milner, H. V. (2019). *Political Science and Digitalization – Global Perspectives* (1. bs). Verlag Barbara Budrich. https://doi.org/10.2307/j.ctvm7bc05

Kostopoulos, G. K. (2018). *Cyberspace and cybersecurity* (Second edition). CRC Press, Taylor & Francis Group.

Kremer, J.-F., & Müller, B. (2014). *Cyberspace and International Relations*. Springer Berlin Heidelberg. https://doi.org/10.1007/978-3-642-37481-4

László, K. (2018). National Cyber Security as the Cornerstone of National Security. *Revista Academiei Forţelor Terestre*, *23*(2), 113-120. https://doi.org/10.2478/raft-2018-0013

Lehto, M. (2018). Cyber Security: Power and Technology, Lehto, M., & Neittaanmäki,

P. (Eds.), *The Modern Strategies in the Cyber Warfare*, Springer International Publishing. https://doi.org/10.1007/978-3-319-75307-2

Lehto, M., & Neittaanmäki, P. (2018). *Cyber Security: Power and Technology* (C. 93). Springer International Publishing. https://doi.org/10.1007/978-3-319-75307-2

Liaropoulos, A. (2020). A Social Contract for Cyberspace. *Journal of Information Warfare*, *19*(2), 1-11.

Libicki, M. (2012). Cyberspace is Not a Warfighting Domain, *I/S: A Journal of Law and Policy*, 8/2, 321–36.

Libicki, M. C. (2007). *Conquest in cyberspace: National security and information warfare*. Cambridge University Press. https://doi.org/10.1017/CBO9780511804250

Libicki, M. C. (2009). *Cyberdeterrence and cyberwar*. The Rand Corporation.

Locke, J. (1988). *Two treatises of government* (Student edition.). Cambridge University Press.

Locke, J., & Shapiro, I. (2003). *Two Treatises of Government and A Letter Concerning Toleration*. Yale University Press.

Long, D. & Wilson, P. & Wilson, P.C. (1995). *Thinkers of The Twenty Years' Crisis: Inter-war Idealism Reassessed.* Oxford University Press.

Machiavelli, N. (2021). *The Prince*. Open Road Integrated Media, Inc.

Matan, A. (2004). Equality and community: State of nature and social contract in Hobbes' and Rawls' theory. *Politička Misao*, *41*(4), 42-58.

Mazarr, M. J. (2018). Understanding Deterrence. *Rand Corporation Perspective*. https://www.rand.org/content/dam/rand/pubs/perspectives/PE200/PE295/RAND_PE295.pdf (Erişim Tarihi: 16 Temmuz 2023)

McAfee (2023). *What is Malware?*. https://www.mcafee.com/enus/antivirus/malware.html#:~:text=Malware%20is%20software%20that%20is,for%20malicious%20files%20or%20programs. (Erişim Tarihi: 21 Temmuz 2023)

McGlinchey, S., Walters, R., & Scheinpflug, C. (2017). *International Relations Theory*. E-International Relations.

Mearsheimer, J. J. (1994). The False Promise of International Institutions. *International Security*, *19*(3), 5–49. https://doi.org/10.2307/2539078

Mearsheimer, J. J. (2013). International Relations Theories : Discipline And Diversity. Dunne, M. Kurki, & S. Smith (Eds.), *Structural Realism*, Oxford University Press.

Milli İstihbarat Teşkilatı (2023). *2022 MİT Faaliyet Raporu.* https://www.mit.gov.tr/MitFaaliyetRaporu/index.html (Erişim Tarihi: 1 Haziran 2023)

Milli İstihbarat Teşkilatı (2023). *Teknik ve Siber İstihbarat.* https://www.mit.gov.tr/2937.html (Erişim Tarihi: 23 Haziran 2023)

Mishra, N. (2020). The Trade: (Cyber)Security Dilemma and Its Impact on Global Cybersecurity Governance. *Journal of World Trade*, *54*(4). https://kluwerlawonline.com/api/Product/CitationPDFURL?file=Journals\TRAD\TRAD2020025.pdf (Erişim Tarihi: 5 Haziran 2023)

Morgenthau, H. J. (1967). *Politics among nations; the struggle for power and peace* (4th ed.). Knopf.

Morris, C.W. (1999). *The Social Contract Theorists : Critical Essays on Hobbes, Locke, and Rousseau.* Lanham, Md: Rowman and Littlefield.

MSB (2023). *Kilitli Kalkan- 2023 (Locked Shields-2023) Tatbikatı.*

https://www.hvkk.tsk.tr/News/Article/hvkk/1685 (Erişim Tarihi: 5 Temmuz 2023)

Muravchik, J. (1992). Conservatives for Clinton. *The New Republic*, 2(22).

National Geographic (2020). *Smart Cities.* https://education.nationalgeographic.org/resource/smart-cities/ (Erişim Tarihi: 15 Haziran 2023)

NATO (2023). *Cyber defence*. https://www.nato.int/cps/en/natohq/topics_78170.htm (Erişim Tarihi: 11 Mayıs 2023)

Nikitakos, N. & Mavropoulos, P. (2014). Cyberspace as a State's Element of Power. Carayannis, E., Campbell, D., Efthymiopoulos, M. (Eds.), *Cyber-Development, Cyber-Democracy and Cyber-Defense.* Springer, New York, NY. https://doi.org/10.1007/978-1-4939-1028-1_10

Norton (2021). *"Hacktivism: An overview plus high-profile groups and examples*." https://us.norton.com/blog/emerging-threats/hacktivism (Erişim Tarihi: 22 Mart 2023)

NPR (2019). *"Edward Snowden Speaks Out: "I Haven't and I Won't" Cooperate With Russia."*. https://www.npr.org/2019/09/19/761918152/exiled-nsa-contractor-edward-snowden-i-haven-t-and-i-won-t-cooperate-with-russia (Erişim Tarihi: 3 Haziran 2023)

NTV Haber (2000). *Türkiye'de bilişimin öyküsü-1*. http://arsiv.ntv.com.tr/news/28088.asp (Erişim Tarihi: 5 Haziran 2023)

Nye, J. S. (2005). *Power in the global information age: From realism to globalization*. Routledge.

Nye, J. S. (2007). *Understanding international conflicts: An introduction to theory and history* (6. ed). Pearson Longman.

Nye, J. S. (2010). Cyber Power. *Belfer Center for Science and International Affairs.* *https://apps.dtic.mil/sti/pdfs/ADA522626.pdf* (Erişim Tarihi: 23 Nisan 2023)

Nye, J. S. (2011a). Nuclear Lessons for Cyber Security? *Strategic Studies Quarterly*, *5*(4), 18-38.

Nye, J. S. (2011b). *The future of power* (1. ed). PublicAffairs.

Nye, J. S. (2014). *The regime complex for managing global cyber activities*. The Centre for International Governance Innovation and the Royal Institute for InternationalAffairs. https://www.cigionline.org/sites/default/files/gcig_paper_no1.pdf (Erişim Tarihi: 15 Nisan 2023)

On Birinci Kalkınma Planı (2019). https://www.sbb.gov.tr/wp-content/uploads/2022/07/On_Birinci_Kalkinma_Plani-2019-2023.pdf (Erişim Tarihi: 11 Mayıs 2023)

Orhan, U. (2021). Cezaları Ağırlaştırmak Caydırıcılığı Artırır mı? (Does Aggravating Penalties Increase Deterrence?). *Türkiye Barolar Birliği Dergisi*, 34(56), 65-85. http://tbbdergisi.barobirlik.org.tr/m2021-156-1997 (Erişim Tarihi: 3 Ocak 2023)

Oymak, H. (2020). 7253 Sayılı "İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanunda Değişiklik Yapılmasına Dair Kanun'un Getirdikleri. *Yeni Medya*, *2020*(9), 129-141. https://dergipark.org.tr/tr/download/article-file/1473782 (Erişim Tarihi: 5 Nisan 2023)

Oymak, H. (2022). Kamuoyunda Dezenformasyon Yasası Olarak Bilinen, 7418 Sayılı "Basın Kanunu İle Bazı Kanunlarda Değişiklik Yapılmasına Dair Kanun'' un Getirdikleri. *Yeni Medya*, *2022*(13), 504-514.

https://dergipark.org.tr/tr/download/article-file/2860682 (Erişim Tarihi: 5 Nisan 2023)

Pınarcıoğlu, N. Ş., Kanbak, A. ve Şiriner, M. (2010). Kent kuramları. Ö. Uğurlu, N. Pınarcıoğlu, A. Kanbak ve M. Şiriner (Eds.). *Türkiye Perspektifinden Kent Sosyolojisi Çalışmaları* (ss. 71-102*),* İstanbul: Örgün Yayınları.

Prasad, R., & Rohokale, V. (2020). *Cyber Security: The Lifeline of Information and Communication Technology*. Springer International Publishing. https://doi.org/10.1007/978-3-030-31703-4

Rattray, G. & Healey, J. (2010). *Categorizing and understanding offensive cyber capabilities and their use*. Proceedings of a workshop on deterring cyber-attacks: informing strategies and developing options for U.S. Policy. The National Academies. 77–97. https://nap.nationalacademies.org/read/12997/chapter/8 (Erişim Tarihi: 6 Şubat 2023)

Resmi Gazete (1991). *3756 sayılı 765 sayılı Türk Ceza Kanunu'nun Bazı Maddelerinin Değiştirilmesine Dair Kanun.* https://www.resmigazete.gov.tr/arsiv/20901.pdf (Erişim Tarihi: 2 Şubat 2023)

Resmi Gazete (2006). *2006/10316 sayılı e-Devlet Kapısının Kurulması, İşletilmesi ve Yönetilmesine İlişkin Bakanlar Kurulu Kararı.* https://www.resmigazete.gov.tr/eskiler/2006/04/20060420-3.htm (Erişim Tarihi: 10 Mayıs 2023)

Resmî Gazete (2006). *2006/22 sayılı E-Devlet Kapısının Kurulması, İşletilmesi ve*

Yönetilmesi Hakkında Başbakanlık Genelgesi. https://www.resmigazete.gov.tr/eskiler/2006/08/20060810-6.htm (Erişim Tarihi: 10 Mayıs 2023)

Resmi Gazete (2007). *e-Dönüşüm Türkiye Projesi Kurumsal Yapılanması, Başbakanlık Genelgesi.* https://www.resmigazete.gov.tr/eskiler/2007/04/2007040314.htm (Erişim Tarihi: 10 Mayıs 2023)

Resmi Gazete (2008*). 5809 sayılı Elektronik Haberleşme Kanunu*. https://www.resmigazete.gov.tr/eskiler/2008/11/20081110M1-3.htm (Erişim Tarihi: 12 Mayıs 2023)

Resmi Gazete (2011). *655 sayılı Ulaştırma, Denizcilik ve Haberleşme Bakanlığının Teşkilat ve Görevleri Hakkında Kanun Hükmünde Kararname.* https://www.resmigazete.gov.tr/eskiler/2011/11/20111101M1-1.htm (Erişim Tarihi: 3 Mart 2022)

Resmi Gazete (2012). *2012/3842 sayılı Ulusal Siber Güvenlik Çalışmalarının Yürütülmesi, Yönetilmesi ve Koordinasyonuna İlişkin Bakanlar Kurulu Kararı.* https://www.resmigazete.gov.tr/eskiler/2012/10/20121020-18-1.pdf (Erişim Tarihi: 6 Mayıs 2023)

Resmi Gazete (2013). *2818 sayılı Siber Olaylara Müdahale Ekiplerinin Kuruluş, Görev ve Çalışmalarına Dair Usul ve Esaslar Hakkında Tebliğ.* https://www.resmigazete.gov.tr/eskiler/2013/11/20131111-6.htm (Erişim Tarihi: 2 Şubat 2023)

Resmi Gazete (2016*). 6698 Sayılı Kişisel Verilerin Korunması Kanunu.* https://www.resmigazete.gov.tr/eskiler/2016/04/20160407-8.pdf (Erişim Tarihi: 1 Haziran 2023)

Resmi Gazete (2017). *KamuNet Ağına Bağlanma ve KamuNet Ağının Denetimine İlişkin Usul ve Esaslar Hakkında Tebliğ.* https://www.resmigazete.gov.tr/eskiler/2017/06/20170621-15.htm (Erişim Tarihi: 13 Temmuz 2023)

Resmi Gazete (2019). *Bilgi ve İletişim Güvenliği Tedbirleri Hakkında Cumhurbaşkanlığı Genelgesi.* https://www.resmigazete.gov.tr/eskiler/2019/07/20190706-10.pdf (Erişim Tarihi: 17 Temmuz 2023)

Resmi Gazete (2022*). 7418 sayılı Basın Kanunu ile Bazı Kanunlarda Değişiklik Yapılmasına Dair Kanun*. https://www.resmigazete.gov.tr/eskiler/2022/10/20221018-1.htm (Erişim Tarihi: 11 Ocak 2023)

Reuters (2022). "*U.S. compels Iran to again release seized U.S. sail drones, U.S. officials say."* https://www.reuters.com/world/iran-says-it-briefly-seizes-unmanned-us-drones-red-sea-2022-09-02/ (Erişim Tarihi: 1 Temmuz 2023)

Riglietti, G. (2017). Defining the threat: what cyber terrorism means today and what it could mean tomorrow. *International Journal of Business & Cyber Security*, 1(2), 15-23.

Roberts, T. (2011). Cyber Intelligence: Setting the Landscape for an Emerging Discipline, *Intelligence and National Security Allian*ce, Vol.9, 1-20

Salahdine, F., & Kaabouch, N. (2019). Social Engineering Attacks: A Survey. *Future Internet*, *11*(4). https://doi.org/10.3390/fi11040089

Samoilenko, S. V. (2022). *Digitalization: Contexts, Roles, and Outcomes*. Routledge. https://doi.org/10.1201/9781003304906

Sanfelice, R.C. (2016). Cyber-Physical Systems: From Theory to Practice. Rawat, D.

B., Rodrigues, J. J. P. C., Stojmenovic, I., Rodrigues, J. J. P. C., & Stojmenovic, I. (Eds). *Analysis and Design of Cyber-Physical Systems: A Hybrid Control Systems Approach*, CRC Pres. https://doi.org/10.1201/b19290

Schaap, A. (2009). Cyber warfare operations: development and use under international law. *Air Force Law Rev*, 64, 121–174.

Scherrer, J. H., & Grund, W. C. (2009). *A Cyberspace Command and Control Model:* Defense Technical Information Center. https://doi.org/10.21236/ADA540457

Schmitt, M. N., Vihul, L., & NATO Cooperative Cyber Defence Centre of Excellence (Ed.). (2017). *Tallinn manual 2.0 on the international law applicable to cyber operations* (First published 2017). Cambridge University Press.

Scholtz, T. (2017). *The History of Private Security. In Private Security Today* (pp. 1-22). Routledge.

Shapiro, J. N. (2013). *The terrorist's Dilemma: Managing violent covert organizations*. Princeton, NJ: Princeton University Press.. https://press.princeton.edu/books/hardcover/9780691157214/the-terrorists-dilemma (Erişim Tarihi: 17 Kasım 2022)

Simmel, G. (2009). *Metropol ve zihinsel hayat: Bireysellik ve Kültür*. İstanbul: Metis Yayınları.

Singer, P. W. & Friedman, A. (2014). *Cybersecurity and cyberwar: What everyone needs to know*. Oxford University Press.

Slayton, R. (2017). What Is the Cyber Offense-Defense Balance?: Conceptions, Causes, and Assessment. *International Security*, *41*(3), 72-109. https://doi.org/10.1162/ISEC_a_00267

Snyder, G. H. (1984). The Security Dilemma in Alliance Politics. *World Politics*, *36*(4), 461-495. https://doi.org/10.2307/2010183

Statista (2023).*" Desktop operating system market share 2013-2023*."
https://www.statista.com/statistics/218089/global-market-share-of-windows-7/ (Erişim Tarihi: 16 Mayıs 2023)

STM (2018). *Siber Tehdit Durum Raporu, Ocak-Mart 2018.*
https://thinktech.stm.com.tr/tr/siber-tehdit-durum-raporu-ocak-mart-2018
(Erişim Tarihi: 27 Eylül 2022)

STM (2019). *Siber Tehdit Durum Raporu, Ekim-Aralık 2019.*
https://thinktech.stm.com.tr/uploads/raporlar/pdf/2312020175942772_stm_siber_tehdit_durum_raporu_ekim_aralik_2019.pdf (Erişim Tarihi: 27 Eylül 2022)

STM. (2022a). *Hakkımızda*. https://www.stm.com.tr/biz-kimiz/hakkimizda (Erişim Tarihi: 25 Haziran 2023)

STM (2022b). *Siber Güvenlik ve Bilişim*. https://www.stm.com.tr/cozumlerimiz/siber-guvenlik-ve-bilisim (Erişim Tarihi: 25 Haziran 2023)

Strateji ve Bütçe Başkanlığı (2021). *2022 Yılı Cumhurbaşkanlığı Yıllık Programı.*
https://www.sbb.gov.tr/wp-content/uploads/2021/10/2022-Yili-Cumhurbaskanligi-Yillik-Programi-26102021.pdf (Erişim Tarihi: 11 Mayıs 2023)

Şenol, M. (2017). Türkiye'de Siber Saldırılara Karşı Caydırıcılık. *Uluslararası Bilgi Güvenliği Mühendisliği Dergisi*, *3*(2).
https://doi.org/10.18640/ubgmd.373193

T.C. 58. Hükümet Acil Eylem Planı (2003).
https://vergiyedaircom.files.wordpress.com/2021/03/t.c.-58.-hukumet-acil-eylem-plani-aep.pdf (Erişim Tarihi: 9 Mayıs 2023)

T.C. Ulaştırma ve Altyapı Bakanlığı. (2012). *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: 5 Ocak 2023)

T.C. Ulaştırma ve Altyapı Bakanlığı. (2016). *2016-2019 Ulusal Siber Güvenlik Stratejisi*. https://www.uab.gov.tr/uploads/pages/siber-guvenlik/2016-2019guvenlik.pdf (Erişim Tarihi: 1 Temmuz 2023)

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

TBMM (2016). *6698 Sayılı Kanun Gerekçesi*. https://www2.tbmm.gov.tr/d24/1/1-1009.pdf (Erişim Tarihi: 13 Temmuz 2023)

Terzi, M. (2018). Bilgi ve İletişim Teknolojilerine Dayali Oluşumlar ile Bu Oluşumların Uluslararası İlişkilere Güvenlik Bağlamındaki Etkisi: Siber Terörizm. *Kara Harp Okulu Bilim Dergisi*, *28*(1), 73-108.

Tezsever, S. (1999). *Milli Güvenliğimiz İçerisinde İstihbarat-Türkiye Cumhuriyeti ve İstihbarat Olgusu*, İ.U. Basımevi.

The Guardian (2007). "*Russia accused of unleashing cyberwar to disable Estonia*". https://www.theguardian.com/world/2007/may/17/topstories3.russia (Erişim Tarihi: 15 Ocak 2023)

The Guardian (2013). "*Edward Snowden: the whistleblower behind the NSA surveillance revelations*". https://www.theguardian.com/world/2013/jun/09/edward-snowden-nsa-whistleblower-surveillance (Erişim Tarihi: 3 Temmuz 2023)

The New York Times (2018). "*Cambridge Analytica and Facebook: The Scandal*

and the Fallout So Far". https://www.nytimes.com/2018/04/04/us/politics/cambridge-analytica-scandal-fallout.html (Erişim Tarihi: 3 Haziran 2023)

The New York Times (2021). *"How the Taliban Turned Social Media into a Tool for Control."* https://www.nytimes.com/2021/08/20/technology/afghanistan-taliban-social-media.html (Erişim Tarihi: 15 Haziran 2023)

Torres-Soriano, M. R., & Toboso-Buezo, M. (2019). Five Terrorist Dystopias. *The International Journal of Intelligence, Security, and Public Affairs*, *21*(1), 49-65. https://doi.org/10.1080/23800992.2019.1598094

TWI Global (2023). *"What is a Smart City? Definition and Examples*." https://www.twi-global.com/technical-knowledge/faqs/what-is-a-smart-city.aspx (Erişim Tarihi: 3 Temmuz 2023)

UAB (2020). *2020-2023 Ulusal Siber Güvenlik Stratejisi ve Eylem Planı.* https://hgm.uab.gov.tr//uploads/pages/siber-guvenlik/ulusal-siber-guvenlik-stratejisi-ep-2020-2023.pdf (Erişim Tarihi: 16 Temmuz 2023)

UAB (2023). *KamuNet.* https://hgm.uab.gov.tr/kamu-net (Erişim Tarihi: 13 Haziran 2023)

USOM (2023). *Ulusal Siber Olaylara Müdahale Merkezi Arge Çalışmaları*. https://www.usom.gov.tr/arge (Erişim Tarihi: 25 Mayıs 2023)

Valeriano, B., & Maness, R. (2012). The fog of cyberwar: Why the threat does not live up to the hype. *Foreign Affairs*. http://www.foreignaffairs.com/articles/138443/brandon-valeriano-and-ryan-maness/the-fog-of-cyberwar (Erişim Tarihi: 10 Mart 2023)

Van Houten, V. (2010). *An overview of the cyber warfare*. Exploitation and

Information Dominance (CWEID) Lab. http://info.publicintelligence.net/cyberwarfarebrief.pdf (Erişim Tarihi: 4 Mart 2023)

Van Long Do, Fillatre, L., Nikiforov, I., & Willett, P. (2017). Security of SCADA systems against cyber-physical attacks. *IEEE Aerospace and Electronic Systems Magazine*, *32*(5), 28-45. https://doi.org/10.1109/MAES.2017.160047

Wall, D. (2007). *Cybercrime: The Transformation of Crime in the Information Age*. Polity. https://books.google.com.tr/books?id=ybntngEACAAJ (Erişim Tarihi: 16 Temmuz 2023)

Waltz, K. N. (1979). *Theory of international politics*. Addison-Wesley Pub. Co.

Warner, M. (2014). *The rise and fall of intelligence: An international security history*. Georgetown University Press.

Weber, A. F. (1899). *The growth of cities in the nineteenth century*. New York: McMillian.

Weimann, G. (2015). *Terrorism in cyberspace: The next generation*. Woodrow Wilson Center Press.

Westberg, G. (2017). Cyberspace, Advanced Sciences and Technologies for Security Applications, Ramírez, M. J. & García-Segura, L.A. (Eds.), *Can Cyber Attack Prevent Wars.* DOI: 10.1007/978-3-319-54975-0_1

Wiener, N. (1948). *Cybernetics; or, Control and communication in the animal and the machine.* JWiley.

Wilner, A. S. (2020). US cyber deterrence: Practice guiding theory. *Journal of Strategic Studies*, *43*(2), 245-280. https://doi.org/10.1080/01402390.2018.1563779

Winterfeld, S., & Andress, J. (2012). *The Basics of Cyber Warfare: Understanding the*

Fundamentals of Cyber Warfare in Theory and Practice. Elsevier Science & Technology Books. http://ebookcentral.proquest.com/lib/gmu/detail.action?docID=1073026 (Erişim Tarihi: 4 Nisan 2023)

Wohlforth. (2020). Realism and great power subversion. *International Relations (London),* 34(4), 459–481. https://doi.org/10.1177/0047117820968858

Wolfers, A. (1952). "National Security" as an Ambiguous Symbol. *Political Science Quarterly*, *67*(4), 481-502. https://doi.org/10.2307/2145138

Wolfsfeld, G., Segev, E., & Sheafer, T. (2013). Social Media and the Arab Spring: Politics Comes First. *The International Journal of Press/Politics*, *18*(2), 115-137. https://doi.org/10.1177/1940161212471716

YÖK (2023). *"YÖK Siber saldırılara karşı uzman yetiştirmek için 4 yeni meslek yüksekokulu açılıyor"*. https://www.yok.gov.tr/Sayfalar/Haberler/2023/siber-saldirilara-karsi-uzman-yetistirmek-icin-4-yeni-myo-aciliyor.aspx (Erişim Tarihi: 19 Haziran 2023)