T.C.
İSTANBUL TİCARET ÜNİVERSİTESİ
LİSANSÜSTÜ EĞİTİM ENSTİTÜSÜ
KAMU HUKUKU ANABİLİM DALI
KAMU HUKUKU TEZLİ YÜKSEK LİSANS PROGRAMI

MİLLETLERARASI HUKUK ÇERÇEVESİNDE DEVLETİN SİBER EGEMENLİĞİ

Yüksek Lisans Tezi

Hakan KONAK

İstanbul, 2025

T.C.
İSTANBUL TİCARET ÜNİVERSİTESİ
LİSANSÜSTÜ EĞİTİM ENSTİTÜSÜ
KAMU HUKUKU ANABİLİM DALI
KAMU HUKUKU TEZLİ YÜKSEK LİSANS PROGRAMI

MİLLETLERARASI HUKUK ÇERÇEVESİNDE DEVLETİN SİBER EGEMENLİĞİ

Yüksek Lisans Tezi

Hakan KONAK

100022423

Danışman: Doç. Dr. Abdülkadir AKIL

İstanbul, 2025

ETİK BEYAN SAYFASI

Hazırlamış olduğum tez özgün bir çalışma olup YÖK ve İstanbul Ticaret Üniversitesi Yönetmeliklerine uygun olarak hazırlanmıştır. Ayrıca, bu çalışmayı yaparken bilimsel etik kurallarına tamamıyla uyduğumu; yararlandığım tüm kaynakları gösterdiğimi ve hiçbir kaynaktan yaptığım ayrıntılı alıntı olmadığını beyan ederim. Bu tezin ihtiva ettiği tüm hususlar şahsi görüşüm olup İstanbul Ticaret Üniversitesi'nin resmi görüşünü yansıtmamaktadır.

Hakan KONAK

TEŞEKKÜR

Bu tezin hazırlanmasında değerli katkılarından dolayı danışmanım Doç. Dr. Abdülkadir AKIL hocama, araştırma sürecinde bana destek olan Prof. Dr. İbrahim SUBAŞI hocama ve Dr. Öğr. Üyesi Özlem YÜCEL hocama içtenlikle teşekkür ederim. Çalışmam boyunca benden bir an olsun yardımlarını esirgemeyen Tayfun GÖZLER hocama ve bana her zaman moral ve motivasyon desteği veren sevgilim Ayşenur'a minnettarım.

İstanbul 2025

Hakan KONAK

MİLLETLERARASI HUKUK ÇERÇEVESİNDE

DEVLETİN SİBER EGEMENLİĞİ

ÖZET

21. yüzyıl, dijitalleşmenin etkisiyle siyaset, güvenlik ve hukuk alanlarında köklü dönüşümlerin yaşandığı bir dönem olarak öne çıkmaktadır. Bu dönüşüm, özellikle geleneksel egemenlik anlayışının sorgulanmasına ve siber uzayın stratejik bir alan haline gelmesine neden olmuştur. Bilgi ve iletişim teknolojilerine olan bağımlılığın artması, siber tehditlerin ulusal ve milletlerarası güvenlik için ciddi riskler doğurmasına yol açmıştır. Siber uzay, günümüzde yalnızca teknik bir faaliyet alanı olmanın ötesine geçmiş; politik, ekonomik ve stratejik karar alma süreçlerini doğrudan etkileyen, çok katmanlı ve disiplinlerarası bir güvenlik alanı haline gelmiştir. Bu bağlamda siber saldırılar, sadece sistemleri hedef almakla kalmayıp, devletlerin siyasal istikrarını ve milletlerarası hukuk düzenini de tehdit etmektedir. Günümüzde devletler, siber güvenliği savunma politikalarının ayrılmaz bir parçası olarak ele almakta ve bu alanda yeni stratejik yaklaşımlar geliştirmektedir. Özellikle Amerika Birleşik Devletleri (ABD), Rusya ve Estonya gibi aktörler siber kapasite inşasında öncü rol üstlenirken, milletlerarası kuruluşlar da bu sürece normatif katkılar sunmaktadır. Bu gelişmeler, siber egemenlik kavramının dijital çağda milletlerarası hukukta yeniden tanımlanması ihtiyacını gündeme getirmiştir.

Anahtar Sözcükler: *Egemenlik, Milletlerarası Hukuk, Siber Uzay, Siber Egemenlik, Siber Güvenlik.*

ABSTRACT

The 21st century stands out as a period of profound transformation in the fields of politics, security, and law due to the impact of digitalization. This transformation has led to the questioning of traditional notions of sovereignty and the emergence of cyberspace as a strategic domain. Increased dependence on information and communication technologies has led to cyber threats posing serious risks to national and international security. Cyberspace is no longer just a technical domain; it is also a multidimensional security agenda that influences political and economic decision-making processes. In this context, cyber attacks not only target systems but also threaten the political stability of states and the international legal order. Today, countries consider cybersecurity an integral part of their defense policies and are developing new strategic approaches in this area. While actors such as the US, Russia, and Estonia are taking the lead in building cyber capacity, international organizations are also contributing to this process by setting norms. These developments have brought to the fore the need to redefine the concept of cyber sovereignty in international law in the digital age.

Keywords: *Sovereignty, international Law, Cyberspace, Cyber Sovereignty, Cyber Security.*

İÇİNDEKİLER

Etik Beyan Sayfası……i
Teşekkür……..ii
Özet……..iii
Abstract……...iv
İçindekiler……..…….....v
Şekiller Listesi……....vii
Kısaltmalar.……..…viii

GİRİŞ……1

BİRİNCİ BÖLÜM: EGEMENLİĞİN ORTAYA ÇIKIŞI VE GELİŞİMİ……5
1.1. Devleti Oluşturan Unsurlar……...13
1.1.1. Beşerî Unsur: Millet……..14
1.1.2. Toprak Unsuru: Ülke……16
1.1.3. Egemenlik Unsuru……18
1.1.3.1. Egemenliğin Tanımı ve Tarihsel Gelişimi……..20
1.1.3.2. Egemenliğin Çeşitleri……25
1.1.3.2.1. Dış Egemenlik……..25
1.1.3.2.2. İç Egemenlik……25
1.2. Egemenliğin Sahibi Konusunda Teoriler……..26
1.2.1. Teokratik Egemenlik Teorisi……26
1.2.2. Demokratik Egemenlik Teorisi……26

İKİNCİ BÖLÜM: DEVLETİN EGEMENLİK HAKLARI VE SINIRLARI…….27
2.1. Devletin Siber Alanla İlgili Hak ve Yükümlülükleri……28
2.1.1. Devletin Hak ve Yükümlülükleri……...32
2.1.1.1. Savunma Hakkı……..…….....32
2.1.1.2. Suçu Önleme Hakkı……...…….....36
2.2. Devletin Milletlerarası Hukukta Hak ve Yükümlülükleri……...……...38
2.2.1. Milletlerarası Hukukta Savunma Hakkı……...…….……..……..39
2.2.2. Suçluyu Cezalandırma Yetkisi……..……..……..43
2.2.3. Geri Verilmesini Talep Hakkı……..…….45

ÜÇÜNCÜ BÖLÜM: MİLLETLERARASI HUKUK ÇERÇEVESİNDE SİBER EGEMENLİK VE İLGİLİ ÇALIŞMALAR……....52

3.1. Siber Egemenlik Kavramının Ortaya Çıkışı ve Tanımı..……..……58

3.1.1. Milletlerarası Hukukta Siber Egemenlik……..…..60

3.1.2. Siber Uzay Kavramı……..63

3.1.2.1. Siber Güvenliğin Tanımı ve Ortaya Çıkışı……...70

3.1.2.2. Siber Saldırı Kavramı……..…79

3.1.2.3. Siber Saldırılar ile İnsan Haklarının İhlali……...85

3.1.2.4. Siber Saldırılar ve Milletlerarası Güvenlik Sorunu…….….93

3.2.Siber Egemenlik ve Milletlerarası Düzenlemeler…….……100

3.2.1. Birleşmiş Milletler, Avrupa Birliği, Kuzey Atlantik Antlaşması Teşkilatı gibi Milletlerarası Kurumların Rolü……..101

3.2.1.1. Birleşmiş Milletler (BM)……...……103

3.2.1.2. Avrupa Birliği (AB)……...……115

3.2.1.3. Kuzey Atlantik Antlaşması Teşkilatı (NATO)……..……122

3.2.2. Türkiye'de Siber Egemenliğe İlişkin Hukuki Düzenlemeler…….…….....131

SONUÇ…….142

KAYNAKÇA……147

ŞEKİLLER LİSTESİ

Şekil 1: Dünyada İnternet Kullanan Nüfusun Oranları (1990 ile 2023 arası) 66
Şekil 2: AB'de Güvenlik Sorunları ile Karşılaşan İnternet Kullanıcısı Yüzdesi (2015) 118

KISALTMALAR

AAET : Avrupa Atom Enerjisi Topluluğu

AB : Avrupa Birliği

ABD : Amerika Birleşik Devletleri

AET : Avrupa Ekonomik Topluluğu

a.g.e. : Adı Geçen Eser

a.g.m. : Adı Geçen Makale

a.g.t. : Adı Geçen Tez

AİHS : Avrupa İnsan Hakları Beyannamesi

AKÇT : Avrupa Kömür ve Çelik Topluluğu

AUÇG : Açık Uçlu Çalışma Grubu

b. : Basım

BİT : Bilişim ve İletişim Teknolojisi

Bkz. : Bakınız

BM : Birleşmiş Milletler

BTK : Bilgi Teknolojileri İletişim Kurumu

C. : Cilt

CIA : Merkezi İstihbarat Teşkilatı

çev. : Çeviren

DDoS : Distributed Denial of Service

der. : Derleyen

DoS : Denial of Service

Dr. : Doktor

ed. : Editör

ENISA : Avrupa Birliği Siber Güvenlik Ajansı

FBI : Federal Soruşturma Bürosu

HUG : Hükümet Uzmanları Grubu

IP : Internet Protocol Address

ITU : Uluslararası Telekomünikasyon Birliği

İHEB : İnsan Hakları Evrensel Beyannamesi

md. : Madde

NATO : Kuzey Atlantik Antlaşması Teşkilatı

NICC : NATO Entegre Siber Savunma Merkezi

NSA : Ulusal Güvenlik Teşkilatı

OECD : Ekonomik Kalkınma ve İş Birliği Örgütü

Prof. : Profesör

RF : Rusya Federasyonu

s. : Sayfa

S. : Sayı

SBE : Sosyal Bilimler Enstitüsü

SSCB : Sovyet Sosyalist Cumhuriyetler Birliği

TCP : Transmission Control Protocol

TİB : Telekomünikasyon İletişim Başkanlığı

TÜBİTAK : Türkiye Bilimsel ve Teknik Araştırma Kurumu

UEKAE : Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü

USOM : Ulusal Siber Olaylara Müdahale Merkezi

vb. : Ve benzeri

vd. : Ve devamı

vs. : Ve saire

GİRİŞ

21. yüzyıl, dijitalleşmenin derin etkileriyle birlikte siyaset, güvenlik ve hukuk alanlarında radikal değişimlerin yaşandığı bir döneme işaret etmektedir. Bu dönüşümün en belirgin sonuçlarından biri, geleneksel egemenlik anlayışının yeniden tartışmaya açılması ve siber uzayın milletlerarası ilişkilerde stratejik bir alan olarak öne çıkmasıdır. Günümüz dünyasında hem bireylerin hem de devletlerin yaşamları bilgi ve iletişim teknolojilerine giderek daha fazla bağımlı hale gelmiş, bu da siber tehditlerin sadece bireysel düzeyde değil, ulusal ve milletlerarası güvenlik açısından da önemli bir risk unsuru haline gelmesine neden olmuştur.

Siber uzay, artık yalnızca teknolojik bir alan olarak değil; aynı zamanda siyasi, ekonomik ve diplomatik ilişkileri doğrudan etkileyen çok boyutlu bir güvenlik sorunu olarak değerlendirilmekte ve bu kapsamda devletlerin stratejik planlamalarında merkezi bir rol üstlenmektedir. Bilgi teknolojilerindeki hızlı gelişim, devletleri ve milletlerarası örgütleri dijital altyapıya bağımlı hale getirmiş, bu durum ise, yeni tehdit türlerinin ve çatışma biçimlerinin ortaya çıkmasına zemin hazırlamıştır. Bu bağlamda siber saldırılar, yalnızca teknik aksaklıklara yol açmakla kalmamakta, aynı zamanda siyasal istikrarı sarsmakta ve milletlerarası hukuk düzenini de tehdit etmektedir.

Siber güvenlik, günümüzde ulusal güvenlik politikalarının ayrılmaz bir parçası haline gelmiştir. Devletler, savunma, caydırıcılık ve milletlerarası iş birliği politikalarını yeniden tanımlama gereği duymakta; bu kapsamda yeni hukuki ve kuramsal yaklaşımlar geliştirilmektedir. ABD, Rusya ve İran gibi küresel aktörlerin yanı sıra, Estonya ve İsrail gibi dijitalleşmede öncü ülkeler de siber güvenlik stratejilerini derinleştirmiştir. Türkiye ise, bölgesel koşulları dikkate alarak kendi siber güvenlik politikalarını şekillendirme sürecindedir. Ayrıca Birleşmiş Milletler (BM), Kuzey Atlantik Antlaşması Teşkilatı (NATO) ve Avrupa Birliği (AB) gibi milletlerarası kuruluşlar da siber güvenlik konusundaki normatif çerçevenin oluşumuna aktif katkılar sunmaktadır.

İnternetin 1990'lı yıllardan itibaren hızla ticarileşmesi ve küresel ölçekte yaygınlaşması, siber uzay kavramını doğurmuş; bu da ulusal güvenlik tehditlerinin dijital düzleme taşınmasına yol açmıştır. Stuxnet solucanı örneğinde olduğu gibi, devlet destekli saldırıların etkisi, siber alanın stratejik önemini daha da artırmıştır. Estonya'ya 2007 yılında gerçekleştirilen Distributed Denial of Service (DDoS) saldırısı, dijital tehditlerin

bir ülkenin kamu hizmetlerini durdurabilecek ölçekte olabileceğini gözler önüne sermiştir. Bu saldırı, aynı zamanda siber güvenliğin milletlerarası ilişkiler açısından kritik bir unsur olduğunu ilk kez bu denli açık biçimde ortaya koymuştur.

Güvenlik kavramı, Soğuk Savaş sonrası dönemde sadece askeri tehditlerle sınırlı kalmamış; iklim krizi, salgın hastalıklar, terör ve siber saldırılar gibi çok katmanlı tehditleri içerecek şekilde yeniden tanımlanmıştır. Özellikle siber saldırılar, yalnızca dijital altyapıyı değil; insan haklarını, egemenlik sınırlarını ve milletlerarası hukuk kurallarını da ihlal eder niteliktedir. Bu bağlamda devletler, siber alan üzerindeki hakimiyetlerini artırma yönünde çaba sarf etmektedir. Siber tehditlerin milletlerarası istikrarı bozabilecek potansiyele sahip olması, devletleri bu alanda daha etkin düzenlemeler yapmaya sevk etmiştir.

Siber güvenliğin sağlanmasında bireyler, en zayıf halka olarak kabul edilmekle birlikte aynı zamanda en kritik aktörler arasında yer almaktadır. Çünkü pek çok siber saldırı bireysel hatalardan veya güvenlik açıklarından kaynaklanmaktadır. Bu nedenle bireylerin siber güvenlik konusunda bilinçlendirilmesi ve eğitilmesi, güvenlik politikalarının başarısı açısından büyük önem arz etmektedir. Etkili bir siber güvenlik stratejisinin yalnızca teknik önlemlerle değil, aynı zamanda sosyal, hukuki ve kültürel boyutlarla da desteklenmesi gerekmektedir. Nitelikli insan kaynağına dayanmayan güvenlik önlemleri sürdürülebilir olmaktan uzaktır.

Siber tehditlerin doğası gereği sınır tanımaz olması, milletlerarası iş birliğini zorunlu kılmaktadır. Bu nedenle, siber suçlarla mücadelede küresel düzeyde norm oluşturma ve ortak standartlar geliştirme ihtiyacı giderek artmaktadır. Farkındalık yaratma, bilgi paylaşımı ve karşılıklı güven esasına dayalı yönetim mekanizmaları, siber güvenliğin kalıcı biçimde sağlanmasına katkı sunmaktadır. Bu doğrultuda geliştirilen tanıma göre, siber güvenlik; tüm dijital varlıkları ve aktörleri kapsayan, çok katmanlı ve entegre çözümlerle desteklenen, teknik önlemler kadar eğitim, hukuk ve yönetim süreçlerini içeren bütüncül bir güvenlik kültürünü ifade etmektedir.

11 Eylül 2001'de yaşanan terör saldırıları, dijital teknolojilerin asimetrik tehdit unsurları tarafından da kullanılabileceğini göstermiştir. Bu olayda saldırganların internet ve iletişim araçlarını etkin biçimde kullanmış olmaları, siber uzayın yalnızca devletler arası rekabetin değil, devlet dışı aktörlerin de faaliyet gösterdiği bir çatışma zemini haline

geldiğini ortaya koymuştur. Bu gelişme, siber güvenlik kavramının klasik güvenlik yaklaşımlarının ötesine geçmesini zorunlu kılmıştır.

Devletler, bu tehditlere karşı politik, teknolojik ve hukuki araçlarla karşılık vermeye çalışmakta; dijital egemenliklerini korumak için yeni stratejiler geliştirmektedir. Bu çerçevede siber egemenlik, klasik egemenlik teorilerinin dijital çağdaki yansıması olarak öne çıkmakta ve milletlerarası hukukta yeni tartışmalara zemin hazırlamaktadır. Teknolojinin baş döndürücü bir hızla gelişmesi, siber egemenlik kavramının ulusal ve milletlerarası düzeyde giderek daha fazla önem kazanmasına neden olmuştur. Konunun güncelliği ve hızla değişen dinamikleri nedeniyle literatürde bu alana ilişkin çalışmalar sınırlı kalmaktadır. Bu bağlamda, gerçekleştirdiğimiz özgün çalışmanın, siber egemenlik konusuna ilgi duyan araştırmacılar için faydalı bir kaynak oluşturması hedeflenmiştir. Siber egemenlik, çok boyutlu ve çeşitli kavramlarla iç içe geçmiş bir alan olduğundan, çalışmamızda ilgili diğer kavramlara da yer verilmiş; böylece konunun daha kapsamlı ve anlaşılır bir şekilde ele alınması amaçlanmıştır. Bu çalışmanın, alana katkı sunmasının yanı sıra, ileride yapılacak araştırmalar için de yol gösterici olacağı düşünülmektedir. Literatürde daha önce yeterince ele alınmamış bazı alt başlıklara odaklanılarak, konuya farklı bir perspektiften yaklaşılmış ve sistematik bir şekilde analiz edilmiştir.

Bu bağlamda çalışmanın temel amacı, devletlerin siber egemenlik anlayışlarını milletlerarası hukuk çerçevesinde değerlendirmek ve bu egemenliğin meşruiyet sınırlarını analiz etmektir. Devletin klasik unsurlarından biri olan egemenlik, dijital çağın gerekleri doğrultusunda yeniden yorumlanmakta; siber uzay yeni bir egemenlik sahası olarak tartışılmaktadır.

Tezin ilk bölümünde; egemenlik kavramının daha iyi anlaşılması adına devletin tarihsel kökeni, unsurları ve egemenlik teorileri ele alınmıştır. Böylece siber egemenlik kavramı daha anlaşılır olacaktır. İkinci bölümde ise, devletlerin siber alandaki hak ve yükümlülükleri hem iç hukuk hem de milletlerarası hukuk perspektifiyle değerlendirilmiştir. Üçüncü ve son bölümde ise, siber egemenlik kavramı detaylı şekilde açıklanarak BM, NATO, AB gibi milletlerarası örgütlerin yaklaşımları, yapmış oldukları hukuki düzenlemeler ve Türkiye'nin yasal düzenlemeleri ışığında somut örneklerle desteklenmiş ve anlatılmaya çalışılmıştır.

Bu çalışma, küresel ölçekte gittikçe büyüyen siber tehditlere karşı devletlerin meşru müdafaa hakkını, dijital çağın gereklilikleriyle egemenlik kavramının nasıl yeniden tanımlandığına dair bir perspektif sunmayı hedeflemektedir. Aynı zamanda, milletlerarası hukukta siber uzay üzerindeki egemenlik hakkının sınırları ve geleceği hakkında teorik ve pratik bir tartışma zemini oluşturmayı amaçlamaktadır. Sonuç olarak bu çalışma, dijitalleşmenin güvenlik paradigmasında yol açtığı dönüşümleri anlamlandırmakta ve siber egemenliğin milletlerarası hukuk bağlamındaki yerini teorik ve pratik bir bakış açısıyla ortaya koymayı amaçlamaktadır. Devletlerin siber alandaki meşru müdafaa hakkının sınırlarını çizmek, gelecekteki hukuki ve politik yaklaşımlar için önemli bir zemin sunmaktadır.

BİRİNCİ BÖLÜM

1. EGEMENLİĞİN ORTAYA ÇIKIŞI VE GELİŞİMİ

İnsan, varoluşunun her evresinde toplum adı verilen sosyal bir yapı içerisinde doğar, gelişir ve yaşamını sonlandırır. İnsanların topluluklar halinde yaşam sürdürdüğü ve bu yapının evrensel bir olgu olduğu bilimsel bir gerçekliktir.[1] Zorlu doğa koşullarına karşı korunma, temel gereksinimlerini karşılama ve hayatta kalabilme adına insanlar, topluluklar halinde yaşama gereği duymuşlardır. Aristoteles'e göre, insanın toplum dışında varlık gösterebilmesi için ya tanrısal bir nitelik taşıması ya da bir canavar olması gerekir. İnsan ihtiyaçlarının sınırsız oluşu, buna karşılık bireysel emek ve üretim kapasitesinin sınırlılığı, insanların bir arada yaşamasını ve karşılıklı bağımlılık ilişkileri kurmasını zorunlu kılmıştır. Birey, yaşamını sürdürebilmek için yalnızca kendi emeğine değil; aynı zamanda fırıncıdan terziye, kasaptan marangoza ve tamirciye kadar birçok farklı meslek grubunun katkısına ihtiyaç duyar. İnsanların bir arada yaşama ihtiyacını doğuran bir diğer unsur ise, savunma gereksinimidir. Bu gereksinim, kolektif güvenlik arayışını beraberinde getirerek devletin doğuşuna zemin hazırlamıştır. Bu bağlamda devlet, yalnızca siyasi bir otorite değil, aynı zamanda insanların birlikte yaşama zorunluluğunun kurumsal bir tezahürüdür.[2] Dolayısıyla, insan yalnızca doğal bir varlık değil; aynı zamanda sosyal bir varlıktır. Toplum içinde yaşayan bireyler, birbirleriyle kurdukları ilişkiler ve karşılıklı etkileşimler yoluyla çeşitli sosyal yapılar oluştururlar. Bu yapılar; aile, eğitim, din, ekonomi gibi kurumsal düzenlemeler şeklinde ortaya çıkar. Aynı zamanda bireylerin ortak yaşamını düzenleyen değerler, normlar ve kurallar da bu toplumsal ortamda şekillenir. Böylece insan, yalnızca doğaya değil, toplumsal bir bağlama da bağımlı olarak varlığını sürdürür ve anlam kazanır.[3] İnsanları bir arada tutan şeyin bir ihtiyaç değil zorunluluk olduğu sonucuna da varmak mümkündür.

Daha önce herhangi bir siyasal yapılanmanın bulunmadığı bir bölgede ilk devletlerin ortaya çıkışını açıklayan faktörler oldukça çeşitlidir. Bu süreçte etkili olan unsurlar, genellikle karmaşık ve çok katmanlı toplumsal organizasyonların gelişmesini

[1] Fatih Bilgili ve Ertan Demirkapı, **Hukukun Temel Kavramları**, 9. b, Bursa: Dora, 2013, s. 3.
[2] Yahya Deryal, **Temel Hukuk Bilgisi**, 1. b, Trabzon: Derya Kitabevi, 2007, s. 1-2.
[3] Erol Cansel vd., **Hukuka Giriş**, 1. b, Ankara: Seçkin Yayıncılık, 2012, s. 19.

gerektirmiştir. Bu tür organizasyonların yürütülebilmesi için ise, yönetim faaliyetlerine sürekli olarak odaklanabilecek yöneticilere ihtiyaç duyulmuştur. Bu yöneticilerin zamanla kurumsallaşması ve meşruiyet kazanmaları, devletin örgütsel yapısının oluşumuna zemin hazırlamıştır. Tarihsel süreçte ilk devletlerin ortaya çıkışı; büyük ölçekli sulama tarımına geçiş, artan nüfusun kontrol altına alınamaması, savaşların yaygınlaşması, çevresel kaynakların sınırlılığı ve uzun mesafeli ticaretin gelişmesi gibi birbirinden farklı ve bağımsız dinamiklerin etkisiyle gerçekleşmiştir. Farklı coğrafi özelliklere sahip ve sosyal yapıları birbirinden önemli ölçüde ayrışan toplumların, tek bir ortak nedene bağlı olarak devletleşmiş olmaları olasılığı oldukça düşüktür. Dolayısıyla, devletin ortaya çıkışı çok boyutlu, o bölgeye özgü ve tarihsel bağlamdan bağımsız ele alınamayacak bir olgudur. [4] Devlet kurmak isteyen bir topluluğun, amaçlarını gerçekleştirebilmesi için en temel gereksinimlerden biri fiziksel bir mekandır. Zira bir devletin varlığını suda, havada ya da soyut bir zeminde sürdürmesi mümkün değildir. Bu nedenle, söz konusu topluluğun öncelikli olarak bir toprak parçası üzerinde egemenlik kurması gerekir. Ancak modern dünya düzeninde, herhangi bir siyasi otoritenin denetimi dışında kalan toprakların kalmamış olması, bu tür bir girişimin önünde ciddi bir engel teşkil etmektedir.[5] Devletin kuruluşunu tek bir nedene ve etkene bağlamak ve açıklamaya çalışmak mümkün değildir. Bu nedenle konu çok boyutlu ve karmaşık bir yapıdadır.

Zaman içerisinde toplumsal eşitsizlikler derinleşmiş; ekonomik, sosyal ve siyasal farklılıklar belirginleşmiş ve bu durum toplumun katmanlara ayrılmasına yol açmıştır. Nihayetinde, bu katmanlaşmanın ve eşitsizliğin en ileri biçimi olarak devlet ortaya çıkmıştır. Devletin oluşum sürecinde fetih gibi dışsal dinamikler etkili olsa bile, bu sürecin nihai amacı toplumun "yönetenler" ve "yönetilenler" şeklinde iki ana gruba ayrılmasıdır. Ancak bu ayrımın kalıcı bir kurumsal yapı kazanması ve toplumsal düzeyde meşruiyet kazanması zaman almıştır.[6] Birey, her zaman daha iyiye ulaşma, onurlu ve insanca bir yaşam sürdürme arzusundadır. Ancak, herkesin sadece kendi çıkarını önceledeği ve güç temelli bir rekabetin öne çıktığı bir ortamda çatışmalar kaçınılmaz olur. Bu nedenle, toplum içinde oluşan maddi ve manevi değerlerin bireyler arasında adil bir şekilde dağıtılabilmesi için, hukuk kurallarına ya da kamu vicdanından beslenen sosyal normlara gereksinim duyulmaktadır. Bu normlar, toplumsal yaşamı düzenleyen ve

[4] Oktay Uygun, **Devlet Teorisi**, 8. b, İstanbul: On iki Levha Yayıncılık, 2021, s. 59-61.
[5] Kemal Gözler, **Devletin Genel Teorisi**, 4. b, Bursa: Ekin Yayınevi, 2012, s. 9-10.
[6] Uygun, **a.g.e.,** s. 65.

adaletin sağlanmasına hizmet eden temel yapı taşlarıdır. Öte yandan, insanlık tarihinin büyük bir bölümünde devlet kurumsallaşmış bir yapı olarak var olmamıştır.[7] İnsanlık tarihinin çok büyük bir kısmında devlet bulunmamaktaydı. İlk devletler, yüzbinlerce yıllık insanlık tarihinin son 5.300 yılı içinde ortaya çıkmıştır. Bu durum her zaman toplu halde yaşamış olsalar da insanların tarihin yalnızca küçük bir kesitini devlet çatısı altında geçirdiklerini göstermektedir.[8]

Tarihsel açıdan bakıldığında, insanın başlangıçta yalnız ve savunmasız bir varlık olduğu, ancak zamanla güvenliğini sağlamak ve yaşamını sürdürmek amacıyla topluluklar oluşturduğu görülmektedir. Önce aile ve akrabalık temelli gruplar, ardından kabileler ve daha sonra şehir-devletleri ortaya çıkmıştır. Bu küçük siyasi birimlerin birleşmesiyle zamanla daha büyük ölçekli imparatorluklar meydana getirmiştir. Nihayetinde, bireylerin hak ve özgürlüklerini koruma amacıyla kurumsallaşan yapı olarak devlet ortaya çıkmıştır. Devlet, bu anlamda sadece bir otorite değil; aynı zamanda bireyin güvenliğini ve temel haklarını güvence altına alan toplumsal bir mekanizma olarak da işlev görür.[9] Hiç kuşkusuz önceleri bir başınaydı insan. Yalnız ve korunmasız halde. Sonraları, yaşam hakkını güvenceye bağlamak, korkusuz yaşamak isteğiyle aile, kabile, derken site-devletleri kuruldu. Sitler birleşti, devletler, imparatorluklara dönüştü. Özgürlükler ve hakların güvenceye bağlanması amacıyla yaratılan kurum devlet ortaya çıktı.[10] Devlet kurumunun bir anda ortaya çıkmadığı insanlığın yaşadığı birikimler sonucu zamanla ortaya çıktığı görülmektedir.

Devlet, belirli bir coğrafi alan üzerinde egemenlik kurmuş, organize bir insan topluluğunun oluşturduğu siyasal ve hukuki bir yapıdır. Devletin klasik tanımı incelendiğinde, bu oluşumun üç temel unsurdan meydana geldiği görülmektedir: insan topluluğu, ülke (toprak) ve egemenlik. Birinci unsur olan insan topluluğu, hukuk literatüründe "millet" kavramıyla ifade edilir. Millet, tarihsel, kültürel, dilsel ya da duygusal bağlarla birbirine bağlı bireylerden oluşan sosyal bir birlikteliktir. Ancak, bu topluluğun varlığı tek başına devletin kurulması için yeterli değildir. İkinci unsur ise, coğrafi unsurdur; yani ülke. Ülke, belirli sınırlarla tanımlanmış, insan topluluğunun

[7] Deryal, **a.g.e.,** s. 2-3.
[8] Uygun, **a.g.e.,** s. 1.
[9] İsmail Kayar ve İlhan Üzülmez, **Hukukun Temel Kavramları**, 7. b, Ankara: Detay Yayıncılık, 2011, s. 1.
[10] Sami Selçuk, **Zorba Devletten Hukukun Üstünlüğüne**, 3. b, Ankara: Yeni Türkiye Yayınları, 1999, s. 13.

sürekli yerleşim sağlayabileceği ve üzerinde siyasi otoritenin tesis edilebileceği bir toprak parçasını ifade eder. Toplumun varlığına ek olarak, bu topluluğun yaşadığı mekânın belirgin sınırlarla tanımlanması devletin kurulabilmesi açısından zorunludur. Üçüncü ve belki de devletin hukuki meşruiyetini tanımlayan en önemli unsur egemenliktir. Egemenlik, devletin hem iç hem dış ilişkilerde en üstün ve bağımsız karar alma yetkisini ifade eder. Bir devletin varlığından söz edilebilmesi için, belirli bir insan topluluğunun, belirli bir toprak parçası üzerinde en yüksek otoriteye sahip olması gerekir. Devletin tanımı, bu üç unsurun birlikte varlığına dayanır ve bu unsurlar arasında hiyerarşik bir üstünlük söz konusu değildir. Her biri devletin varlık koşulu açısından eşit derecede asli niteliktedir. Dolayısıyla, devletin unsurları arasında asli ya da tali ayrımı yapmak yerine, bunların birbirini tamamlayan ve birlikte anlam kazanan yapılar olarak değerlendirilmesi gerekir.[11]

Her ne kadar bazı akademisyenler devletin temel unsurları olan insan, toprak ve egemenliğin eşit derecede önemli olduğunu savunsa da biz bu görüşe katılmamaktayız. İnsan unsuru, devlet kavramının öznesi olarak diğer unsurlardan ayrışmakta ve devleti var kılan temel unsur olarak değerlendirilmektedir. Çünkü insanın var olmadığı bir ortamda devletin varlığından söz etmek mümkün değildir. Devleti kuran, ona isim veren, belirli bir toprak üzerinde egemenlik iddia eden ve bu amaç doğrultusunda organize olan güç, özünde insan unsurudur. İnsan olmadan devlet, toprak ve egemenlik kavramları anlamını yitirir ve soyut kavramlar olarak kalır. Dünya üzerinde birçok gezegen bulunsa da, bunlarda devlet benzeri siyasi organizasyonlar henüz oluşmamıştır. Gelecekte insanlığın Mars gibi başka gezegenlerde koloniler kurması halinde bile, bu bölgelerde devlet ve toprak tanımlarının ne şekilde şekilleneceği, tartışmaya açık bir konu olacaktır. Bu tür tartışmaların da özünde yine insan unsurunun varlığı ve rolü belirleyici olacaktır.

"Devlet" terimi Türkçeye Arapça kökenli "devle" kelimesinden geçmiştir ve temel anlamı "elden ele geçen" veya "tedavül eden" şeklindedir. Bu kavram, farklı dillerde çeşitli şekilde ifade edilmektedir: Fransızca'da Etat, İngilizce'de State, Almanca'da Staat ve İtalyanca'da Stato olarak kullanılmaktadır. Tüm bu terimlerin kökeni, Latince'de "hal, durum, vaziyet" anlamına gelen Status kelimesine dayanmaktadır. Antik Yunan'da ise, devlet kavramı için "polis" terimi tercih

[11] Gözler, **a.g.e.,** s. 4-5.

edilmekteydi; bu kelime şehir ya da site anlamına gelmektedir. Roma uygarlığında ise, devlet anlamını karşılamak üzere civitas ve res publica terimleri kullanılmıştır. Bu tarihsel ve dilsel kökenler, devlet kavramının farklı kültürlerdeki biçimlenişine ışık tutmaktadır.

Yeni bir devletin kuruluşu, belirli bir insan topluluğunun belli bir toprak parçası üzerinde egemenlik tesis etmesiyle gerçekleşir. Bu bağlamda, devlet; belirli bir nüfusun, sınırları belirlenmiş bir alanda siyasi hakimiyet kurması sonucu ortaya çıkan siyasi bir varlıktır. Daha önce devletin var olmadığı bir bölgede kurulan devletlere birincil devletler denir. Buna karşılık, ikincil devletler, önceden kurulmuş bir devletin etkisi ve etkileşimi sonucu oluşan devletlerdir. [12] Bir bölgede devlet ortaya çıktığında, çevresindeki toplumlarda hızla devletleşme sürecine girer. Bunun nedenleri çeşitlidir. Sık görülen üç nedeni şöyle sıralayabiliriz:

1-Çevredeki çok sayıda kabile veya şeflik; daha önce kurulan devletin egemenliği altına girmek istemediği için birleşip ortak bir savunma gücü oluşturmak üzere devletleşebilir,

2-Mevcut devletin zengin kentlerini yağmalamak için güçlerini birleştirmek amacıyla devletleşebilir,

3-Mevcut devletin güvence altına aldığı ticaret yolarının kontrolünü ele geçirmek üzere devletleşebilir. Bu ve benzeri nedenlerle devletleşemeyen ilkel toplumlar, kaçınılmaz biçimde mevcut devletin kontrolü altına girecektir.[13]Devletler, evrensel bir biçimde ve her dönemde aynı özelliklere sahip olarak ortaya çıkmazlar. Yapısal özellikleri ile bağımsızlık dereceleri açısından farklılıklar gösterirler. Bu farklılıkları kavrayabilmek için öncelikle devlet türlerini sınıflandırmak amacıyla bir çerçeve sunmak, ardından bu sınıflandırma kapsamında yer alan devletleri milletlerarası hukuk perspektifinden değerlendirmek gerekmektedir. [14]

Devletin ortaya çıkışına ilişkin çeşitli düşünürler ve kuramcılar tarafından farklı teoriler geliştirilmiştir. Bu teorilerden bazıları aşağıda özetlenmiştir:

[12] Gözler, **a.g.e.,** s. 11.
[13] Uygun, **a.g.e.,** s. 59.
[14] Edip F. Çelebi, **Milletlerarası Hukuk**, İstanbul: Fakülteler Matbaası, 4. b, 1980, s. 355-356.

1-Aile Teorisi: Modern devlette iktidarın doğası, ailede babanın sahip olduğu otoriteyle karşılaştırılamaz. Ancak, günümüzde geçerliliğini yitirmiş olsa da aile teorisinin devlet gücü ve özellikle devlet başkanına ilişkin algılar üzerindeki etkileri, çağdaş toplumlarda hala gözlemlenmektedir. Örneğin, ülkemizde devleti vatandaşlar karşısında bir otorite figürü olarak baba metaforuyla değerlendiren bireylerin sayısı oldukça fazladır. Bu durum, birçok vatandaşın zihninde devletin baba imgesiyle ilişkilendirildiğine işaret etmektedir.[15] Bu yaklaşım, devletin aynı soydan gelen bireyler ve ailelerin büyüyüp genişlemesiyle şekillendiğini ileri sürer.

2-Biyolojik Teori: Biyolojik teori, devleti yaşayan bir organizmaya benzetmektedir. Bu yaklaşımda devlet, doğuş, gelişme ve sonlanma süreçlerini yaşayan bir varlık olarak ele alınmaktadır. Teoriye göre, devleti oluşturan unsurlar, bir organizmadaki organların işlevleri gibi birbirleriyle uyum içinde çalışmaktadır. Devletlerin zaman içinde ortaya çıktığı, evrildiği ve nihayetinde sona erdiği düşüncesi bu teorinin temelini oluşturur. Bu perspektifi benimseyen düşünürler, devlet olgusunu bu canlı organizma modeli çerçevesinde değerlendirmektedir. Devleti, diğer canlı organizmalar gibi doğan, gelişen ve nihayetinde varlığı sona eren canlı bir organizma olarak tanımlar.

3-Kuvvet ve Mücadele Teorisi: Devletlerin yalnızca zor kullanımıyla kurulduğu ve otoritelerinin tamamen güç temelli olduğu iddiası aşırı bir genellemedir. Kuşkusuz, devletler otoritelerini sağlamak için gerektiğinde güç kullanımına başvurabilirler; ancak aynı zamanda vatandaşlarını, otoritelerinin meşruiyetine ikna etmeye çalışırlar. Devletler, yönetimlerinin adalet ilkeleri doğrultusunda gerçekleştiğini ileri sürer ve bu çabalarında belli oranda başarı sağlarlar. Eğer devletler sadece güç kullanarak varlıklarını sürdürseydi, sürekli isyan ve iç karışıklıklarla karşı karşıya kalmaları kaçınılmaz olurdu. Oysa tarih boyunca egemenliklerini uzun süre koruyabilmiş, istikrarlı birçok devlet örneği bulunmaktadır. Bu devletlerin yalnızca zor kullanmakla ayakta kaldığını iddia etmek gerçekçi değildir.[16] Bu teori, güçlü olanların zayıflar üzerinde baskı kurarak bir yapı oluşturmasıyla devletin meydana geldiğini savunur.

[15] Gözler, **a.g.e.,** s. 31.
[16] Gözler, **a.g.e.,** s. 33.

4-Ekonomik Teori: Marksist teori içerisinde sınıf mücadelesi temel kavramlardan biri olarak kabul edilir. Karl Marx'a göre, tarih; sınıflar arasındaki çatışmaların tarihidir. Her dönemde toplumda birbirleriyle zıtlaşan iki temel sınıf bulunur ve bu sınıflar, üretim araçlarının mülkiyetini elde tutma mücadelesi verirler. Üretim araçlarına sahip olan sınıf, aynı zamanda siyasi iktidarı da elinde bulundurur. Bu sınıfa "egemen sınıf" ya da "sömüren sınıf", karşıt olan diğer sınıfa ise, "sömürülen sınıf" denir. Egemen sınıf, üretim araçları üzerindeki mülkiyetini sürdürmek için zor kullanmaya başvurmak zorundadır; bu amaçla baskı araçlarına ihtiyaç duyar ve bu da devletin kuruluş amacını oluşturur. Devlet, egemen sınıfın sömürülen sınıf üzerindeki baskısını örgütleyen bir yapı olarak tanımlanır ve üretim araçları sahiplerinin jandarması işlevi görür. Marksist teori, diğer teoriler gibi tarihsel süreci kendi perspektifinden yorumlayan ve inceleyen bir yaklaşımdır.[17] Ayrıca Marksistler, ilkel toplumun kendi iç dinamiklerinin, ekonomik alt yapının yavaş yavaş değişmesinin devleti ortaya çıkardığını savunur.[18] Devletin ekonomik temeller üzerine inşa edildiğini öne süren bu yaklaşımın önemli temsilcilerinden Karl Marx, Marksist felsefe çerçevesinde, sömüren ve sömürülen sınıflar arasındaki çatışmanın devletin ortaya çıkışını tetiklediğini belirtir.

5-Sosyal Sözleşme Teorisi: Devletin ortaya çıkışına ilişkin sosyal sözleşme kuramı, bireylerin devlet öncesi doğal bir durumda yaşadıkları varsayımına dayanır. Bu dönem, insanların organize bir siyasal yapıya sahip olmadan önceki yaşam biçimini ifade eder. Sosyal sözleşme kuramına göre, insanlar, belirli bir noktada akıl ve iradelerini kullanarak bu doğal durumdan çıkmayı tercih etmiş ve kendi aralarında bir anlaşmaya varmışlardır. Bu anlaşma, literatürde "sosyal sözleşme" (social contract) olarak adlandırılır. Devletin temeli de bu sözleşmeye dayandırılmaktadır. Başka bir deyişle, devlet insanların rasyonel tercihleri ve iradeleriyle oluşturdukları bir kurumdur. İngiliz düşünür Thomas Hobbes'a göre, doğal yaşam dönemi sürekli bir çatışma haliydi. Bu dönemde, bireyler arasında devamlı bir savaş yaşanmakta, herkes birbirine düşman gibi davranmaktaydı. Hobbes, bu durumu "homo homini lupus" (insan insanın kurdudur) ifadesiyle açıklamıştır. Süregelen bu kaotik ortamda bireyler, güvenlik ve düzen arayışıyla bir araya gelerek kendi özgürlüklerini güçlü bir otoriteye devretmişlerdir. Hobbes, bu otoriteyi "Leviathan" (dev ya da ejderha) metaforuyla tanımlar ve Leviathan'ı

[17] Gözler, **a.g.e.,** s. 34-36.
[18] Uygun, **a.g.e.,** s. 51.

devletin somutlaşmış biçimi olarak görür. Fransız filozof Jean-Jacques Rousseau ise, doğal durumun başlangıçta eşitlik, barış ve mutlulukla karakterize olduğunu ileri sürer. Ancak zamanla bireylerin artan ihtiyaçlarını karşılayabilmek için çalışmaya başlamaları ve özel mülkiyetin ortaya çıkışı, toplumsal eşitliği bozmuştur. Bu durum toplumsal çatışmalara ve güvensizliğe yol açmıştır. Bu bozulmuş yapıyı düzeltmek ve toplumsal güveni yeniden inşa etmek amacıyla insanlar kendi rızalarıyla bir sosyal sözleşme yapmışlardır. Rousseau'ya göre, bu sözleşme sonucunda ortaya çıkan irade, "genel irade" (volonte generale) olarak adlandırılır ve bu irade halk egemenliğinin temelini oluşturur.[19] Bu çerçevede Jean-Jacques Rousseau, siyasal iktidarın meşru temsiline ilişkin olarak egemenliğin halkın ortak iradesi olan genel iradeye dayandırılması gerektiğini savunur. Rousseau'ya göre, yönetim yetkisini kullanan yapının meşruiyeti, tüm bireylerin bu genel iradenin oluşumuna katkıda bulunmasıyla sağlanır.[20]

John Locke'un siyasal düşüncesi, temel hatlarıyla Thomas Hobbes'un sistematiğini takip eder gibi görünse de önemli noktalarda ondan ayrılır. Locke'un kuramında da doğal durum, güvenlik arayışı ve toplumsal sözleşme temel bileşenlerdir. Ancak Locke, egemenliğe dair anlayışında mutlakiyetçiliğe karşı bir tutum sergiler. Ona göre, siyasal iktidarın meşruiyeti, bireylerin haklarını koruma yükümlülüğüne bağlıdır; bu yetki, keyfi biçimde kullanılamaz. Locke, halkın yalnızca yönetime katılma değil, aynı zamanda adaletsizlik ve hukuksuzluk durumunda direnme hakkına da sahip olduğunu savunur. Egemen güç, yasal çerçeveyi ihlal ettiğinde halk, meşru müdafaa bağlamında kuvvet kullanma hakkına sahiptir. Ancak bu direnme hakkının keyfi biçimde kullanılmaması gerekir. Locke'a göre, bu hak, yalnızca bireysel rahatsızlık yaşayan kişiler tarafından değil; kötü yönetim nedeniyle geniş toplum kesimlerinin zarar gördüğü koşullarda, halkın çoğunluğu tarafından kolektif biçimde kullanılmalıdır. Bu yaklaşım, hem bireysel özgürlüklerin güvence altına alınmasını hem de siyasal düzenin istikrarını sağlamayı amaçlamaktadır.[21]

Bu teori, insan topluluklarının mevcut koşullarını iyileştirmek amacıyla bir araya gelerek üzerinde mutabık kaldıkları kurallardan oluşan sosyal bir sözleşme aracılığıyla

[19] Gözler, **a.g.e.,** s. 37-40.
[20] Hamit Emrah Beriş, **Egemenlik & Bir Kavramın Geçmişi, Bugünü ve Geleceği**, 1.b, İstanbul: Tezkire Yayıncılık, 2014, s. 73-74.
[21] Hasan Basri Pehlivan, **Türk Anayasalarında Egemenlik Kavramı**, 1. b, İstanbul: Doğu Kütüphanesi, 2020, s. 37.

devlet olgusunun ortaya çıktığını savunur. Thomas Hobbes, John Locke ve Jean-Jacques Rousseau gibi düşünürler bu görüşün önemli savunucuları arasında yer alır. Sonuç olarak, devletin doğuşunun insanlığın tarihsel deneyimleri, birikimleri ve yaşamsal tecrübeleri sonucunda şekillendiği açıktır. Her toplumun coğrafi konumu, yaşam biçimi, dini inançları, etnik kökeni, kültürel değerleri ve ihtiyaçları gibi çok çeşitli faktörler, devlet yapılarının farklı biçimlerde ortaya çıkmasına zemin hazırlamıştır. Devletin tek bir sebeple ve tek boyutlu olarak oluştuğunu söylemek mümkün değildir. Bu nedenle, devletin kökenine ilişkin birçok düşünür farklı teoriler geliştirmiş ve devletin kuruluşunu çeşitli açıklamalara dayandırmıştır. İnsanlık var olduğu sürece, devlet kavramı, yapısı ve örgütlenme biçimi sürekli bir dönüşüm ve yenilenme süreci içerisinde olacaktır. Zira insan, değişken ve dinamik bir varlık olup, zamanın gereksinimlerine uyum sağlayarak hem kendisini hem de sosyal düzeni sürekli yeniden şekillendirmekte ve yeni düşünceler üretmektedir. Yukarıda özetlenen ana başlıklar, devletin ortaya çıkışını açıklayan temel görüşlere dair genel bir bakış sunmaktadır.

1.1. Devleti Oluşturan Unsurlar

Bir devletin varlığından söz edebilmek için üç temel unsurun bir araya gelmesi gerekmektedir. Bu unsurların ikisi maddi, biri ise, manevi nitelik taşır. Devletin oluşumundaki ilk maddi unsur, belirli bir insan topluluğunun mevcudiyetidir. İkinci maddi unsur ise, bu topluluğun sürekli olarak yaşayabileceği, sınırları belirlenmiş bir coğrafi alan, yani ülkedir. Üçüncü yani manevi unsur ise, egemenliktir. Devletin maddi ve manevi temelleri, yalnızca fiziksel birlikteliklerle sınırlı değildir; aynı zamanda toplumsal ve kültürel aidiyet unsurlarını da içermektedir. Nitekim ABD ve İsviçre örneklerinde görüldüğü üzere, dil, din ve etnik köken farklılıklarına rağmen tarihsel ortaklık bilinci ve geleceğe dair ortak hedefler, bu toplumların ulusal kimliklerini inşa etmelerinde etkili olmuştur. Bu bağlamda, millet olgusunun temelinde geçmişe dair ortak hatıralar ile geleceğe yönelik paylaşılan amaç ve idealler yer alır. Ortak menfaatler doğrultusunda birleşen bireyler, bu birlikteliğin devamını arzuladıklarında bir ulusal dayanışma ruhu oluşur. Bu duygusal bağlılık, milletin oluşumundaki temel yapı taşını meydana getirir. Öte yandan, devletin ülkesi yalnızca kara parçası ile sınırlı değildir. Devletin egemenlik alanı, kara topraklarının yanı sıra, bu toprakların üzerindeki hava sahasını ve karasularını da kapsar. Örneğin, bir devletin hava sahasından uçakla geçiş yapabilmek için önceden izin alınmasının gerekliliği, hava sahasının da ülke unsuruna

dahil olduğunu göstermektedir. Aynı şekilde, bir devletin denize kıyısı varsa, belirli sınırlar içinde kalan karasuları da egemenlik alanı içerisinde yer alır. Ayrıca, ülke sınırları içinde bulunan akarsular, göller ve diğer iç su kaynakları da bu kapsamda değerlendirilir. Bu çerçevede, ülke unsuru, devletin fonksiyonlarını yerine getirebilmesi için zorunlu bir koşuldur. Devletin egemenlik yetkisi yalnızca vatandaşları üzerinde değil, aynı zamanda bu vatandaşların yaşadığı topraklar üzerinde de geçerlidir. Dolayısıyla, egemenlik hakkının hem beşerî hem de coğrafi boyutu olduğu kabul edilmelidir. [22]

Devletin yapısını ve oluşum sürecini daha sağlıklı biçimde kavrayabilmek adına, onu meydana getiren temel unsurların belirli başlıklar altında incelenmesi gereklidir. Bu unsurlar, devlet kavramının hem kuramsal çerçevesini çizmekte hem de tarihsel oluşum sürecini açıklamada işlevsel bir temel sunmaktadır. Her ne kadar bazı yaklaşımlar bu üçlü ayrımın ötesinde farklı unsurların da devletin yapısına katkıda bulunduğunu ileri sürse de devletin temel bileşenlerini sade bir biçimde anlamlandırmak açısından bu üç unsur üzerinden yapılan tasnif açıklayıcılığını korumaktadır. Dolayısıyla, bu çalışmada devletin yapısı ve doğası, söz konusu temel unsurlar üzerinden analiz edilecektir.

1.1.1. Beşerî Unsur: Millet

Devletin temelini oluşturan unsurlardan biri, beşerî yani insan topluluğudur. Ancak bir grubun yalnızca aynı coğrafyada birlikte bulunması, onların doğrudan bir devlet yapısı oluşturduğu ya da devletin bir unsurunu meydana getirdiği anlamına gelmemektedir. Tarihsel süreçte yalnızca belirli sosyal, kültürel ve siyasal bağlarla birbirine bağlanmış insan topluluklarının devlet kurma yetisini kazandıkları görülmektedir. Bu bağlamda, bir topluluğun devlet kurabilme kapasitesi, üyeleri arasında ortak bir kimlik, amaç birliği ve karşılıklı bağlılık gibi niteliklerin bulunmasına bağlıdır. Söz konusu bağların yokluğunda, topluluk yalnızca rastlantısal bir kalabalıktan ibaret kalır ve siyasi örgütlenme kapasitesine sahip bir yapı oluşturamaz. Diğer bir ifadeyle, bu tür bir topluluk, organize bir siyasi yapıdan ziyade, plansız bir topluluk ya da "sürü" niteliğinde kalır. Devlet kurma potansiyeline sahip topluluklar ise, bu rastlantısallığın ötesine geçerek, aralarındaki duygusal, kültürel, tarihi ve sosyal bağlar sayesinde millet bilincini oluşturmuş olanlardır. Dolayısıyla, bir insan topluluğunun devlet kurabilmesi

[22] Adnan Güriz, **Hukuk Başlangıcı**, 12. b, Ankara: Siyasal Kitabevi, 2009, s. 33-35.

için "millet" olma niteliğini kazanmış olması ön koşul niteliğindedir. Millet niteliğinden yoksun bir topluluğun kalıcı ve meşru bir devlet kurması mümkün değildir.[23]

Bireylerin oluşturduğu bir insan topluluğunun devletin kurucu unsurlarından biri olarak kabul edilmesi için, bu topluluğun süreklilik arz eden bir yapı göstermesi gerekmektedir. Ancak bu süreklilik, bireysel düzeyde değil, topluluk düzeyinde ele alınmalıdır. Başka bir ifadeyle, bireylerin geçici ya da kalıcı olarak topluluktan ayrılmaları, eğer topluluğun bütünsel varlığı devam ediyorsa, devlet olgusunun temelini oluşturan insan unsuru açısından bir sakınca teşkil etmemektedir. Devletin insan unsurunu meydana getiren bireyler arasındaki bağın mahiyetine ilişkin olarak ise, bu bağın mutlaka tek bir etnik ya da ulusal kimliğe dayanması zorunlu değildir. Nitekim, günümüzde ABD gibi çok uluslu yapıya sahip devletlerin mevcudiyeti, etnik homojenliğin bir ön koşul olmadığını açıkça ortaya koymaktadır. Dolayısıyla, tek bir ulus kimliğinin varlığı, devletin beşerî unsurunun tanımlanmasında hukuki bir gereklilik olarak kabul edilmemektedir. Milletlerarası hukuk perspektifinden bakıldığında ise, bireylerin devlete olan aidiyetini belirleyen temel kriter, uyrukluk bağıdır. Bu bağ, birey ile devlet arasındaki karşılıklı hak ve yükümlülük ilişkisini tanımlar ve bireyin o devlete mensubiyetini hukuken geçerli kılar. Bu nedenle, insan unsurunun devletin oluşumundaki geçerliliği, etnik ya da kültürel bağlardan ziyade, hukuki uyrukluk ilişkisi temelinde değerlendirilmektedir.[24]

Milletlerarası hukuk açısından, bir insan topluluğunun sayısal büyüklüğü devlet olgusunun geçerliliği bakımından belirleyici bir unsur değildir. Önemli olan, bu topluluğun toplumsal düzeyde süreklilik gösteren bir birliktelik içinde bulunmasıdır. Bu bağlamda, bireylerin geçici ya da kalıcı olarak topluluktan ayrılması, eğer topluluk bütün olarak varlığını sürdürüyor ise, bu durum devletin beşerî unsuru olma niteliğini ortadan kaldırmaz. Dolayısıyla, insan unsurunun sürekliliği bireysel değil, toplumsal bütünlük esas alınarak değerlendirilmelidir. Bu çerçevede, topluluğun varlığını devam ettirdiği sürece, sınırlı sayıdaki bireysel kopuşlar devletin kurucu unsurlarından biri olan insan topluluğunun geçerliliğini etkilemez.[25]

---

[23] Gözler, **a.g.e.,** s. 50-51.
[24] Hüseyin Pazarcı, **Uluslararası Hukuk**, 20. b, Ankara: Turhan Kitabevi, 2021, s. 144-145.
[25] Hüseyin Pazarcı, **Uluslararası Hukuk Dersleri II. Kitap**, Ankara: Ankara Üniversitesi Siyasal Bilgiler Fakültesi ve Basın-Yayın Yüksekokulu Basımevi, 1989, s. 7.

1.1.2. Toprak Unsuru: Ülke

Hem iç hukukta hem de milletlerarası hukuk alanında genel kabul gören görüşe göre, bir devletin ülkesi kara, deniz ve hava alanlarından oluşan bir bütündür. Devletin sahip olduğu ülke sınırlarının büyüklüğü hukuki açıdan belirleyici değildir. Ayrıca, devletin ülkesi mutlaka coğrafi olarak kesintisiz bir kara parçasından ve ona bağlı deniz ve hava sahasından ibaret olmak zorunda değildir. Pratikte birçok devlet, birden fazla ayrı parça halinde bulunan kara ve deniz alanlarına sahip olabilir. Örneğin, Yunanistan gibi adalardan oluşan bir ülke ya da Türkiye gibi iki farklı kıtada kara parçaları bulunan devletler, hukuken bir bütün olarak değerlendirilir. Benzer şekilde, yalnızca adalardan (İngiltere, Japonya, Endonezya) ya da başka devletlere ait kara bölgeleri ile ayrılan parçalar (ABD'nin ana kara bölgesi ve Alaska) devletin egemenlik alanı içinde sayılır ve bu durum hukuki açıdan devlet statüsünü etkilemez. Devletlerin münhasır egemenlik haklarını kullanabilmeleri için, egemenlik alanlarının sınırlarını belirlemeleri zorunludur; bu durum milletlerarası hukukta hem bir hak hem de bir yükümlülük olarak kabul edilmektedir. Çünkü devlet otoritesinin geçerli olduğu alanın net bir şekilde tanımlanması ancak sınırların belirlenmesiyle mümkün olur.[26] Devletin münhasır egemen yetkileri kullandığı ülkesinin sınırlarını belirlemesi milletlerarası hukukun verdiği bir hak ve öngördüğü bir yükümlülüktür. Çünkü devlet otoritesini geçerli olduğu alanı bilmek sınırların belirlenmesi ile mümkündür. Ülke üç boyutludur, yeryüzündeki belirli bir alan ile onun altı ve üstünü de kapsar. Geniş anlamıyla sınır terimi sadece iki kara ülkesini ayran bir çizgiyi değil, buna ek olarak bir devlet ülkesini milletlerarası alanlardan ve uzaydan ayırmaya yarayan farazi çizgiyi ifade eder. [27]

Hem ulusal hukukta hem de milletlerarası hukukta genel kabul gören yaklaşıma göre, bir devletin ülkesel varlığı kara, deniz ve hava sahasından oluşan üç temel bileşeni içermektedir. Kara ülkesi yalnızca yüzeyle sınırlı kalmayıp, bu alandaki göller, nehirler gibi iç su kaynaklarını da kapsamaktadır. Ayrıca, kara ülkesine yer altı kaynakları da dahildir; dolayısıyla bu unsur sadece yüzeysel bir tanımlamayla sınırlandırılamaz. Bu

[26] Pazarcı, Uluslararası…, 2021, **a.g.e.,** s. 147-148.
[27] Enver Bozkurt, Yasin Poyraz ve Selcen Erdal, **Devletler Hukuku**, 11. b, Ankara: Yetkin Yayınları, 2021, s. 86.

kapsamda değerlendirildiğinde, deniz ülkesine dahil olan karasuları devletin egemenlik sahası içindedir.[28]

Devletin varlığı için, toplumsal birliği oluşturan bireylerin belirli bir toprak parçası üzerinde egemenlik kurmuş olması zorunlu bir şarttır. Bu bağlamda, bir milletin herhangi bir fiziki mekâna hâkim olmadan bağımsız bir devlet teşkil etmesi mümkün değildir. Aynı şekilde, hâlihazırda kurulmuş bir devletin egemenlik kurduğu toprakları kaybetmesi durumunda, devlet niteliğini sürdürmesi imkânsız hale gelir. Bu nedenle, her devlet kendi ülkesine ilişkin toprak bütünlüğünü titizlikle koruma eğilimindedir. Devletin sahip olduğu ülkenin yüzölçümünün geniş ya da dar olması, hukuki açıdan bir fark yaratmaz; esas olan, bu toprakların sürekli yerleşime elverişli olması ve egemenliğin fiilen tesis edilmiş bulunmasıdır. Örneğin, dünya üzerinde geniş topraklara sahip olan Rusya ve ABD gibi ülkelerin yanı sıra, oldukça küçük yüzölçümüne sahip devletler de mevcuttur. Bu duruma örnek olarak, 11 Şubat 1929 tarihinde İtalya ile Papalık arasında imzalanan Laterano Antlaşması çerçevesinde kurulan Vatikan verilebilir; söz konusu devletin yüzölçümü yalnızca 44 hektar, yani 440 dönümdür.[29]

Devletin ülkesi, yeryüzünde o devletin egemenliği altında bulunan ve sınırları belirlenmiş coğrafi alanı ifade eder. Devlet, kara ülkesinden bağımsız olarak deniz ve hava alanlarındaki egemenlik haklarını devredemez ya da terk edemez. Bu alanların devlet egemenliği kapsamına dahil olması, kara ülkesine bitişik olmaları durumunda milletlerarası hukuk tarafından kabul edilen bir hukuki sonuçtur. Kara ülkesinin sınırları ya milletlerarası bir antlaşmayla ya uzun süreli ve sorunsuz bir uygulamayla ya da milletlerarası mahkemelerin kararlarıyla belirlenmiş olabilir. Her durumda, sınırlar erga omnes niteliğindedir; yani üçüncü devletler karşısında da geçerlilik taşır. Kara sınırlarının tespiti sürecinde, doğal unsurlar göz önünde bulundurulduğunda bu sınırlar "doğal sınırlar" olarak, coğrafi ya da yapay ölçütlere dayanıyorsa "yapay sınırlar" olarak sınıflandırılır. Dağlar, nehirler, göller gibi doğal oluşumlara dayalı sınırlar doğal sınırlar olarak kabul edilirken, paraleller, meridyenler veya yollar gibi insan yapımı referanslar esas alındığında sınırlar yapay olarak nitelendirilir. Sınırların belirlenmesinde uygulanan genel ilkeler de mevcuttur. Örneğin, nehirlerin sınır oluşturduğu durumlarda, ulaşıma elverişli olmayan nehirlerde orta hat, ulaşıma uygun olanlarda ise, en derin kanal hattı

[28] Pazarcı, Uluslararası Hukuk Dersleri…, 1989, **a.g.e.,** s. 11-12.
[29] Gözler, **a.g.e.,** s. 65-66.

(thalweg) sınır olarak benimsenir. İki veya daha fazla devlet arasında sınır oluşturan göl ve kapalı denizlerde, sınır genellikle kıyılar arasındaki eşit uzaklık hattı olarak belirlenen orta çizgidir. Bu ilkeler, tarafların anlaşmasıyla değiştirilebilir ve farklı uygulamalara da açık olabilir. Devletin hava sahası sınırları ve deniz ülkesinin dış sınırları ise, res communis (milletlerarası toplumun ortak alanları) olarak kabul edilen bölgelerden ayrılması bakımından önem taşır. Bu nedenle, hava ve deniz sınırlarının belirlenmesi tüm devletleri ilgilendiren bir konu olup, ancak milletlerarası hukukun genel ilkeleri çerçevesinde düzenlenebilir. Devletlerin deniz ve hava sahalarının dış sınırlarını belirleyen anlaşmalar, genel hukuki kurallardan sapma içerdiğinde erga omnes etkisi kazanmaz; yani üçüncü devletlere karşı ileri sürülemez. Bu hakka sahip olmaları için ilgili devletlerin söz konusu düzenlemeleri kabul etmeleri ya da itiraz etmemeleri gerekir. Hava ve deniz sınırlarının tespiti milletlerarası hukukta halen tartışmalı ve karmaşık bir konudur.[30]

1.1.3. Egemenlik Unsuru

Belirli bir insan topluluğunun, belirli bir toprak parçası üzerinde siyasal ve hukuksal bir düzen kurması, devlet olmanın temel maddi şartlarından biridir. Ancak, bu düzenlemenin yalnızca var olması, onu diğer kamu teşkilatlarından ayırmaya yetmez. Çünkü devlet bünyesinde, bu niteliklere sahip yerel yönetimler veya vilayetler gibi idari birimler bulunmakta; milletlerarası alanda ise, henüz devlet statüsüne sahip olmayan vesayet altındaki bölgeler ya da örgütlenmiş topluluklar mevcuttur. Devlet ile bu tür ulusal ya da milletlerarası düzeydeki kamu yönetimleri arasındaki temel ayrım, devletin doğası gereği hiçbir dış otoriteye bağımlı olmamasıdır. Bu bağlamda, egemenlik yetkisinin milletlerarası hukuk kapsamında taşıdığı anlam şu şekilde özetlenebilir: Birincisi, devlet, bu yetkiyi kullanırken milletlerarası hukukun öngördüğü yükümlülükler haricinde herhangi bir dış otoriteye tabi değildir; ikincisi, devlet, kendi toprakları üzerinde egemenlik yetkisini münhasıran kullanma hakkına sahiptir.[31]

Yeni bir devlet kurmayı amaçlayan bir insan topluluğunun öncelikli görevi, mevcut bir devletin egemenliği altında bulunan tüm ya da belirli bir toprak parçasını bu egemenlikten bağımsızlaştırarak kendi hakimiyetini tesis etmektir. Bu süreç barışçıl ya

[30] Sevin Toluner, **Milletlerarası Hukuk Dersleri & Devletin Yetkisi (Yer ve Kişiler Bakımından Çevresi ve Niteliği)**, 2. b, İstanbul: Fakülteler Matbaası, 1979, s. 37-38.
[31] Pazarcı, Uluslararası…, 2021, **a.g.e.,** s. 152-153.

da zorlayıcı yollarla gerçekleşebilir. Barışçıl yolla devlet kurma talebinde bulunan topluluk, mevcut devletten ilgili toprak parçasının kendilerine devredilmesini talep eder. Eğer mevcut devlet bu talebi kabul ederse, yeni bir egemenlik alanı ortaya çıkar ve böylelikle yeni bir devlet şekillenmiş olur. Ancak devletler, genellikle kendi toprak bütünlüklerini koruma amacıyla böyle bir devri gönüllü olarak kabul etmezler. Bu tür kararlar, bazen içsel etnik sorunların çözümü gibi stratejik nedenlere dayanabilir. Tarihsel olarak da bazı devletlerin topraklarını mali karşılıklar karşılığında başka devletlere devrettikleri örnekler mevcuttur; örneğin, Rusya'nın 1867'de Alaska'yı ABD'ye satması buna örnek teşkil eder. Bununla birlikte, devlet kurulmasında daha yaygın olan yöntem, kuvvet kullanımıdır. Devlet kurmak isteyen topluluklar, mevcut devlete karşı silahlı mücadele başlatır ve başarılı olmaları durumunda, ülkenin tamamı ya da belirli bir bölgesi üzerinde egemenlik tesis ederler. Bu tür örnekler arasında Sırbistan ve Yunanistan'ın bağımsızlık süreçleri sayılabilir. Ayrıca, yeni devlet kurma çabalarına dış devletlerin destek vermesi de yaygın bir durumdur. Bazı durumlarda ise, mevcut devletin bir bölgesi başka bir devlet tarafından işgal edilerek burada yeni bir devlet oluşturulabilir; Bulgaristan'ın kuruluşu bu duruma örnek olarak verilebilir. Sonuç olarak, mevcut devletler kendi toprakları üzerindeki egemenlik haklarından gönüllü olarak vazgeçmedikçe, yeni bir devletin kurulabilmesi çoğunlukla zorlayıcı yöntemlerin kullanılmasını gerektirir. Bu bağlamda, bir insan topluluğunun başka bir devletin toprak parçası üzerinde egemenlik kurması ve bunu sürdürmesi, devletin temel unsurlarından biri olarak kabul edilir.[32]

Toplumların tümünde belirli bir kesim, çeşitli sebeplerle diğer gruplar üzerinde üstünlük kurmaktadır. Bu eşitsiz güç dağılımını ifade eden iktidar olgusu, tarih boyunca evrensel bir fenomen olarak farklı biçimlerde ortaya çıkmıştır. İktidarın kökenlerine inildiğinde, insanlığın ilk toplumsal oluşumlarına kadar uzandığı görülür. Toplumsallaşma süreci, beraberinde iktidar ilişkilerinin doğmasını kaçınılmaz kılmış; toplum üyeleri arasındaki farklılaşma, doğal olarak iktidarın varlığını da beraberinde getirmiştir. Bu bağlamda, insan topluluklarında ortaya çıkan iktidar ilişkileri, toplumsallaşmanın başladığı andan itibaren evrensel bir olgu olarak varlığını sürdürmüştür. Her toplumda yönetici ve yönetilenler arasında bir ayrım bulunmasına rağmen, 15. yüzyıl itibarıyla işlevsel bir siyasal mekanizma olarak ortaya çıkan modern

[32] Gözler, **a.g.e.,** s. 77-78.

devlet, insanlık tarihinin oldukça yeni bir oluşumudur. "Egemenlik" kavramı da bu modern devletin ürünü olup, modernitenin yarattığı toplumsal, ekonomik ve siyasi ilişkilerin bir sonucudur. Kavramların tanımlanmasının kaçınılmaz olarak bazı sınırlandırmalar içerdiği ve dolayısıyla kavramın bütün boyutlarının kapsanamayabileceği gerçeği göz önünde bulundurulduğunda, egemenlik en genel anlamıyla "siyasal toplum içindeki en üstün yönetim yetkisi" olarak tanımlanabilir. Bu tanım, birtakım eksikliklerine rağmen, 1576 yılında Jean Bodin'in yayımladığı "Devletin Altı Kitabı" adlı eserle literatüre kazandırılan ve siyasal iktidarı tek bir otorite altında toplama amacını taşıyan görüşle uyum içerisindedir.[33] Bu tanımın içeriğine bakıldığında, Batıda gelişen siyasal tarihin oluşturduğu iktidar mücadeleleri karşısında, iktidarın Ortaçağ'daki ontolojik ve hukuki parçalanmışlığının neticesinde meydana gelen ve bir iktidar mücadelesinin neticesini oluşturan boyutlarını ihtiva etmektedir.[34] Egemenlik, devletin varlığını sürdürebilmesi açısından vazgeçilmez bir unsur olarak kabul edilmekte olup, aynı zamanda devlet olgusunun en temel ve belirleyici kriteri olarak değerlendirilmektedir.[35]

1.1.3.1. Egemenliğin Tanımı ve Tarihsel Gelişimi

16. ve 17. yüzyıllarda ortaya çıkan modern ve merkezî devlet anlayışında, devletin diğer örgütlenmiş topluluklardan ayrılmasını sağlayan temel güç olarak egemenlik yetkisi kabul edilmiştir. Milletlerarası hukuk kapsamında egemenlik ya da bağımsızlık kavramı şu şekilde tanımlanabilir: Devlet, hukuki açıdan herhangi bir dış ya da üstün otoriteye bağlı olmaksızın; yalnızca milletlerarası hukuk normları veya kendi benimsediği yükümlülüklerle sınırlandırılmış biçimde, karar verme özgürlüğüne sahip olan varlıktır.[36]

Egemenlik kavramı hem iç hukuk hem de milletlerarası hukuk alanlarında en karmaşık, tartışmalı ve değişken kavramlardan biri olmaya devam etmektedir. Tarihsel süreç içerisinde egemenlik, genellikle mutlak ve herhangi bir denetime tabi olmayan üstün bir iktidar olarak tanımlanmıştır. Bu bağlamda egemenlik, tam ve kesin bir yetki anlamına gelmektedir. Egemenliğin bu tür tanımları olumlu ve olumsuz olmak üzere iki

[33] Beriş, **a.g.e.,** s. 3-4.
[34] Sercan Yılmaz ve Murat Akçakaya, "Türklerde Egemenlik ve Devlet Kanunu", **Çankırı Karatekin Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi**, S.2, C.13, 2023, s. 537.
[35] Abdülkadir Akıl, **Küreselleşen Hukuk ve Ulusal Egemenliğe Etkisi**, 1. b, İstanbul: Kitap Yayınevi, 2023, s. 264.
[36] Pazarcı, Uluslararası Hukuk Dersleri…, 1989, **a.g.e.,** s. 18-20.

yönü barındırır. Olumlu anlamda, egemenlik herhangi bir kısıtlamaya tabi olmaksızın emir verme yetkisini içerirken; olumsuz anlamda ise, başka bir iradeden emir almama durumunu ifade eder. Böylece egemenlik, devletin hem iç işlerinde hem de milletlerarası ilişkilerinde özgürce hareket etmesini sağlayan, kesin ve denetime kapalı bir iktidar biçimidir. Egemenliğin sınırlandırılması durumunda ise, bu sınırlar yalnızca devletin kendi rızasıyla kabul ettiği sınırlamalar olabilir. Öte yandan, egemenliği devletin zorunlu unsuru olarak gören bazı hukukçular, egemenlik kavramını hukuk dışı veya hukuk üstü bir olgu olmaktan çıkarıp, hukukun denetimi altında olan bir yetki biçimi haline getirmeye yönelik "sınırlı egemenlik" anlayışını geliştirmişlerdir. Modern dönemde egemenlik kavramı, bu yumuşatılmış haliyle karşımıza çıkmaktadır.[37]

Tarihsel süreç içerisinde devletlerin egemenlik ve bağımsızlık kavramları, Avrupa'da 1648 yılında imzalanan Vestfalya Barışı ile belirgin bir biçimde ortaya çıkmıştır. 1618'de başlayan ve 1648'de sona eren, büyük çoğunluğu Avrupa devletlerinin katıldığı, Katolik ile Protestan kutuplar arasında cereyan eden yıkıcı mezhep savaşları, "Otuz Yıl Savaşları" olarak bilinmektedir. Savaşın sona ermesiyle sonuçlanan Vestfalya Antlaşmaları, Habsburg İmparatorluğu'nun temsilcilerinin Fransa ile Münster'de ve İsveç ile Osnabrück'te gerçekleştirdiği görüşmeler sonucu kabul edilen antlaşmaların ortak adıdır. Vestfalya egemenlik sistemi, dört temel prensip üzerine inşa edilmiştir: "ülkesellik", "özerklik", "karşılıklı tanıma" ve "denetim". Ülkesellik ilkesi, siyasi otoritenin sınırları belirlenmiş bir coğrafi alan üzerinde kullanılmasını ifade eder; bu, kabile tipi yapılar gibi belirli bir topluluk üzerinde sınırlı bir yetki değil, belirlenmiş bir toprak parçası üzerinde egemenlik anlamına gelir. Özerklik prensibi, herhangi bir dış unsurun devletin sınırları içerisinde yetki kullanmasının mümkün olmadığını belirtir. Karşılıklı tanıma, bağımsız devletlerin birbirlerinin milletlerarası antlaşma yapma yetkisi ve varlıklarını kabul etmelerini sağlar. Son olarak, denetim unsuru, devletlerin kendi sınırları içinde yasama, yürütme ve bu sınırlar dahilindeki tüm faaliyetleri düzenleme ve kontrol etme hakkına sahip olduklarını vurgular. Vestfalya sisteminde, dış aktörlerin başka bir devletin iç işlerine müdahale etmesi veya orada iç otorite oluşturmalarının önüne geçilmeye çalışılmıştır.[38]

[37] Çelebi, **a.g.e.,** s. 324-326.
[38] Pehlivan, **a.g.e.,** s. 19-20.

Tarihsel süreçte, bazı devletlerin kendi rızalarıyla ülkelerinin belirli bölgeleri üzerindeki egemenlik haklarından feragat ederek bu toprakları başka devletlere devrettikleri vakıalar görülmüştür. Ancak hiçbir devlet, egemenlik hakkının tamamından vazgeçmeyi kabul etmez; zira bu durum, o devletin varlığının sona ermesi anlamına gelir. Dolayısıyla, bir devletin sona ermesi ya da ülkesel egemenliğini bütünüyle yitirmesi genellikle zorla, yani savaş yoluyla gerçekleşir. Tarihte, askeri işgal sonucunda hukuki varlığı sona eren birçok devlet örneği mevcuttur. Devletin egemenlik kaybı sonucu sona ermesi ister barışçıl ister zorlayıcı yollarla olsun, çeşitli biçimlerde ortaya çıkar. Bu süreçler arasında fesih, ayrılma veya bölünme, birleşme, ilhak ve gönüllü iltihak ya da emilme gibi yöntemler yer almaktadır. Örnek vermek gerekirse, Yugoslavya'nın feshi bu kapsamda değerlendirilebilir. Ayrılma ya da bölünme örneği olarak Sovyet Sosyalist Cumhuriyetler Birliği (SSCB) verilebilir. Birleşmeye dair bir vakıa, Kuzey ve Güney Vietnam devletlerinin birleşerek Vietnam Sosyalist Cumhuriyeti'ni oluşturmasıdır. İlhak örneği olarak ise, 1940 yılında Estonya, Litvanya ve Letonya'nın SSCB tarafından ilhak edilmesi gösterilebilir. Gönüllü iltihak ve emilme sürecine ilişkin ise, 1990 yılında Demokratik Almanya Cumhuriyeti'nin (Doğu Almanya) Federal Almanya Cumhuriyeti'ne (Batı Almanya) katılarak onun bünyesinde erimesi verilebilir.[39]

Devlet düzeni, çeşitli sosyal varlıkların otorite açısından hiyerarşik bir yapıya tabi tutulması anlamına gelir. Devlet yapısı, genel olarak insan topluluğunu iki ana gruba ayırır: yönetenler ve yönetilenler. Her ne kadar bu iki grup arasında kesin sınırlar her zaman belirgin olmasa da devletin varlığından söz edilebilmesi için yönetenler ile yönetilenler arasındaki ayrımın ortaya çıkması gereklidir. Devletin mevcudiyeti açısından, devlete tanınan üstün otoritenin toplumdaki diğer tüm iktidar ve otoritelerin üzerinde bulunması zorunludur. Toplum yaşamını düzenleyen ve yönetimde birlik sağlayan bu en üst siyasi ve hukuki otoriteye "devlet iktidarı" veya "devlet kudreti" denir. Devlet sayesinde bireylerin yaşamı ve toplumsal faaliyetleri düzen altına alınır. Devlet, bireylerin tabi olduğu bir otorite düzenini ifade eder. Devlet kavramından bahsedebilmek için, belirli bir tüzel kişiliğin varlığı gereklidir. Bu tüzel kişilik, ülke içi ve dışı ilişkilerini temsilcileri aracılığıyla yönetir ve kanunları, organları yoluyla uygular. Bir ülkede birçok

[39] Gözler, **a.g.e.,** s. 15-17.

tüzel kişilik bulunabilmesine karşın, egemenlik hakkına sahip devlet tüzel kişiliği, ülke içerisindeki diğer tüm gerçek ve tüzel kişilerin üzerinde konumlanır.[40]

Devlet iktidarının özellikleri, toplumun yapısına göre, farklılık göstermektedir. Örneğin, kent devleti, feodal devlet ve ulus devletin iktidar biçimleri ve işlevleri birbirinden önemli ölçüde ayrılır. Günümüzde ulus devlet iktidarını önceki devlet modellerinden ayırmak amacıyla sıklıkla "egemenlik" kavramı kullanılmaktadır. Ancak bu kavram, çağdaş devletlerin tümünü yapısal açıdan aynılaştırmakta ya da eşitlemekte değildir. Üniter devletler ile federal devletler, demokratik rejimler ile otokratik yönetimler arasında egemenliğin kaynağı, kullanımı ve niteliği bakımından önemli farklılıklar bulunmaktadır. Bazı akademisyenler egemenliği devletin ayırt edici temel özelliği olarak görür ve yalnızca modern dönemde ortaya çıkan egemen iktidarları devlet olarak tanımlar. Bu yaklaşıma göre, devletin ilk biçimleri 16. yüzyılda Avrupa'da ortaya çıkmıştır. Buna karşılık, devlet kavramını daha geniş perspektiften ele alan diğer bazı düşünürler, küresel toplulukların tamamını kapsayan siyasal iktidarları da devlet iktidarı kapsamında değerlendirmektedir. İlkel toplumlar, yöneten ve yönetilen ayrımının henüz oluşmadığı, toplumsal iktidarın belirli bir kesime devredilmediği, kolektif yönetim biçimlerinin hâkim olduğu toplumlardır. Devlet ise, yöneten ve yönetilen kesimlerin net olarak ayrıldığı hiyerarşik bir toplumsal yapıyla birlikte ortaya çıkmıştır.[41]

Egemenlik kavramı, tarih boyunca uzun süre Tanrı'nın dünya üzerindeki mutlak hakimiyetini ifade etmek amacıyla kullanılmıştır. Dünyevi ilişkileri düzenleyen, belirleyen ve insanlara belirli davranışlarda bulunma ya da bulunmama yetkisi veren merkezi otorite olarak Tanrı kabul edilmiştir. Kutsal metinlerde, Tanrı'nın insanların kaderini tayin eden yegâne güç olduğu ve bu nedenle insanlara koşulsuz itaat borcu bulunduğu sıklıkla vurgulanmaktadır. Örneğin, Roma yönetim anlayışının temel taşlarından biri olan imperium kavramının yanı sıra, yönetimin uhrevi dayanağını simgeleyen sacerdotium kavramını doğal olarak elinde bulunduran Kilise'nin siyasal iktidarı tek başına ele geçirme yönündeki çabaları, egemenlik kavramının gelişimine zemin hazırlamıştır. Egemenlik teriminin siyaset literatürüne girişi, dini otoritelerin dünyevi güç üzerindeki hakimiyet iddialarının tartışıldığı bir dönemin geride kalmasıyla mümkün olmuştur. Egemenlik teorisi sayesinde devletin meşruiyeti, dini unsurlardan

[40] Güriz, **a.g.e.,** s. 35.
[41] Uygun, **a.g.e.,** s. 10-11.

bağımsız, kendine özgü bir nitelik kazanmıştır. Bu bağlamda, siyasal alanın laikleşmesi ile egemenlik kuramının ortaya çıkışı arasında güçlü bir ilişki bulunmaktadır. Modern devlet anlayışında egemenlik, bireylerin kaderini belirleme işlevinin devlete intikal etmesi ve dini etkilerin siyasal sahneden uzaklaştırılması anlamına gelir. Öte yandan, kavramlar ile toplumsal gerçeklikler arasında karşılıklı bir etkileşim olduğu açıktır. Toplumsal ve tarihsel olgular, kavramların ortaya çıkışı, anlam kazanması ve zaman içinde dönüşümünde belirleyici rol oynamaktadır. 16. yüzyıldan itibaren Avrupa'da ekonomik ilişkilerin şekillenmesinde kapitalizmin etkisinin artması, güçlü bir merkezi devlet yapısının oluşumunu zorunlu kılmış ve siyasal iktidarın "birliği" fikrine dayanan egemenlik anlayışının gelişimini kolaylaştırmıştır. Bu birlik, mutlak monarşilerin zirveye ulaştığı dönemlerde kralın kişiliğinde somutlaşmıştır. Ancak tarihsel süreçte yaşanan değişimler, egemenliğin temsil ettiği "birlik" anlayışının merkezini değiştirmiş; özellikle Fransız Devrimi sonrası egemenlik ulus devlet kavramıyla özdeşleşmiştir.[42]

Kamu düzeni ve güvenliğinin korunmasından sorumlu iktidarın, varlığını dayandırdığı siyasal düzenin temel ilkeleri dışında herhangi bir dini veya geleneksel kurala bağlı olmaması, hem Machiavelli'nin laik siyaset alanını genişletme çabasını hem de siyasetin dışsal referanslardan bağımsız, özerk bir alan olarak kurgulanabilmesini mümkün kılmıştır. Machiavelli, siyasal teorisini bu perspektifte oluştururken "egemenlik" terimini doğrudan kullanmamış olmakla birlikte, siyasal sahnede özerk bir "egemen" figürünün ortaya çıkmasının önünü açmıştır. Bu sürece Jean Bodin'in katkısıyla, egemenlik kavramı ilk kez teorik bir zeminde netlik kazanmış ve "egemen" kavramı daha belirgin bir tanıma ulaşmıştır. Böylece siyasal alan, kilise gibi dışsal etkilerden arındırılmış ve özerk bir yapı halini almıştır. Bodin, siyasetin bağımsızlığını temin etme sürecinde Machiavelli'nin izinden giderek, egemenliği mutlak, sürekli, devredilemez ve bölünemez niteliklerle tanımlamıştır. Bu çerçevede devletin en yüksek karar verme yetkisi, mutlak bir güç olarak herhangi bir sınırın dışına çıkmaz; kamu alanında devletin varlığına içkin olan egemenlik, kişisel olmaktan öte, sürekli ve devredilemez bir kavramdır. Egemenlik, siyasal yapının ruhu olarak kabul edilir ve devlet iktidarının bölünmezliği ile ikinci bir otoriteye devredilmezliğini garanti eder.[43]

[42] Beriş, **a.g.e.,** s. 1-2.
[43] Yılmaz ve Akçakaya, **a.g.e.,** s. 538-539.

1.1.3.2. Egemenliğin Çeşitleri

Devlet egemenliği ilkesinden türeyen iki temel prensip bulunmaktadır: Bunlardan biri devletlerin egemen eşitliği ilkesi, diğeri ise, devletlerin iç işlerine müdahale etmeme ilkesidir. [44] Egemenliğin çeşitleri konusunda birçok düşünür farklı kıstaslar kullanarak farklı ayrımlar yapabilmektedir. Biz bu çalışmamızda egemenliği iç egemenlik ve dış egemenlik olarak iki alt başlıkta değerlendireceğiz.

1.1.3.2.1. Dış Egemenlik

Klasik egemenlik anlayışının geçerli olduğu dönemdeki siyasal yapılar, büyük ölçüde mutlak monarşiler tarafından temsil edilmekteydi. Bu dönemde egemenlik kavramı, mutlaklık, sınırsızlık, tekillik, bölünmezlik ve devredilemezlik özellikleriyle tanımlanmış; dolayısıyla bu niteliklerin en iyi biçimde tek bir otorite, yani monark tarafından somutlaştırıldığı kabul edilmiştir. Egemen gücü, ne ülke sınırları içinde ne de dışında kısıtlayabilecek herhangi bir üst otorite bulunmamaktaydı.[45]

17 Temmuz 1998 tarihinde kabul edilen Uluslararası Ceza Mahkemesi Roma Statüsü, devletlerin içişlerine müdahale edilmemesi ilkesine ve dolayısıyla egemenlik hakkına yönelik bazı düzenlemeler içermektedir. Bu antlaşma, 2002 yılında faaliyete geçen Uluslararası Ceza Mahkemesi'ne; soykırım, insanlığa karşı suçlar ve savaş suçları gibi ciddi suçları işleyen bireyleri yargılama yetkisi tanımaktadır. 2005 yılı itibarıyla yaklaşık 100 devlet taraf olmuştur. ABD, Çin, Rusya ve İsrail gibi birçok ülke, devlet egemenliği ilkesine aykırı olduğu gerekçesiyle antlaşmayı imzalamaktan kaçınmıştır. [46]

1.1.3.2.2. İç Egemenlik

Egemenlik yetkisi üç temel alanda toplanmaktadır: yasama, yürütme ve yargı. Kuvvetler ayrılığı teorisi kapsamında, bu üç yetki eşit ve bağımsız güçler olarak kabul edilir. Ancak, yasama yetkisinin yürütme ve yargı yetkilerine göre, daha üstün olduğu görüşü savunulabilir. Bunun temel nedeni, yürütme ve yargı organlarının yetkilerini ancak yasama tarafından oluşturulan kanunlar çerçevesinde kullanabilmeleridir. Yasama

[44] Gözler, **a.g.e.,** s. 79.
[45] M. Nazan Arslanel ve Ertuğrul Eryücel, "Küreselleşme Sürecinde Egemenlik Kavramının Dönüşümü", **Atatürk Üniversitesi Sosyal Bilimler Enstitüsü Dergisi**, C.17, S.1, 2013, s. 27.
[46] Gözler, **a.g.e.,** s. 81.

organı, kanunları yapmakla yükümlü olup, dolayısıyla yürütme ve yargı organları, yasama organının koyduğu kuralları uygulamakla sorumludur. Dahası, yasama organı, yürütme ve yargı organlarının kuruluşunu düzenleyip kanunlarla bu organları oluşturabilir veya kaldırabilir. Ayrıca, yasama yetkisi, bu organların görev ve yetki alanlarını belirleme ve gerektiğinde değiştirme yetkisini de elinde bulundurmaktadır.[47] Devlet iktidarının ülke sınırları içinde en üstün otoriteye sahip, mutlak nitelikte, herhangi bir sınırlamaya tabi olmayan, tek ve bölünmez bir güç olarak devredilemez bir yetkiyi temsil ettiğini ortaya koymaktadır.[48]

1.2. Egemenliğin Sahibi Konusunda Teoriler

Egemenliğin sahibine dair farklı kuramsal yaklaşımlar geliştirilmiştir. Biz bu çalışmamızda egemenliğin sahibi konusunu; teokratik egemenlik teorileri ve demokratik egemenlik teorileri olarak ikiye ayırarak inceleyeceğiz.

1.2.1. Teokratik Egemenlik Teorisi

Egemenliğin kaynağı olarak Tanrı kabul edilmekle birlikte, Tanrı'nın bu egemenliği doğrudan ve fiilen yeryüzünde kullanamayacağı düşünülür. Bu nedenle, Tanrı adına bu yetkiyi temsil edecek ve uygulayacak kişilere ihtiyaç duyulur. Teokratik teorilerde ise, egemenliğin yeryüzündeki temsilcilerinin kimler olacağı ve bu kişilerin nasıl belirleneceği konusunda ortak bir görüş birliği bulunmamaktadır.[49]

1.2.2. Demokratik Egemenlik Teorisi

Demokratik egemenlik teorileri, egemenliğin artık Tanrı yerine insana ait olduğunu savunur; yani egemenliğin kaynağı insan olarak kabul edilir. Ancak, bu teorilerin doğrudan demokratik bir rejime dönüşüp dönüşemeyeceği oldukça tartışmalıdır. Bu nedenle, bu yaklaşımlara "beşerî egemenlik teorileri" adının verilmesi daha uygun görülmektedir.[50]

---

[47] Gözler, **a.g.e.,** s. 82.
[48] Arslanel ve Eryücel, **a.g.m.,** s. 27.
[49] Gözler, **a.g.e.,** s. 87-88.
[50] Gözler, **a.g.e.,** s. 89.

İKİNCİ BÖLÜM

2.DEVLETİN EGEMENLİK HAKLARI VE SINIRLARI

Egemenlik, "ülke" ve "halk"la birlikte devletin varlık koşullarından biri olarak gösterilir. Ancak diğer iki unsurun aksine, egemenlik, somut bir gerçekliğe karşılık gelmez. Devletin bu kurucu unsuru, hukuksal ve siyasal bir ilkedir.[51]

Egemenlik kavramı, özellikle Vestfalya Ulus Devlet sisteminin güçlenmesiyle birlikte daha fazla önem kazanmıştır. Bu dönemde ulus devletler, uluslararası sistemin temel ve önde gelen aktörleri olarak öne çıkmış, böylece egemenlik anlayışı yeniden şekillenmiştir. Merkezi otoritelerin güçlenmesiyle birlikte, egemenlik kavramı hem tanım hem de işlev açısından farklılaşmış; devletler, egemenliklerini kanıtlamak ve görünür kılmak amacıyla sınır kontrolü, gümrük uygulamaları gibi araçları geliştirmiş ve merkezi yönetimlerinin denetimini artırma yoluna gitmiştir. Uluslararası sistem ve ulus devletlerin temel unsurlarından biri olan egemenlik, değişen küresel koşullar doğrultusunda dönüşmek zorunda kalmıştır. 19. yüzyıl sonlarından başlayarak, 20. yüzyılda hızlanan teknolojik ilerlemeler sosyal, siyasi, ekonomik ve toplumsal alanlarda köklü değişikliklere yol açmış, mesafeleri kısaltarak devletler arası sınırların geçilmesini kolaylaştırmıştır. Özellikle internet ve sosyal medya gibi iletişim araçlarındaki devrimsel değişimler, geleneksel egemenlik anlayışını sorgulanabilir hale getirmiştir. Bu yeni tehditler ve zorluklarla başa çıkmak için geliştirilen kavramlardan biri de siber egemenliktir. Günümüzde enformasyon ve iletişim teknolojilerindeki gelişmeler, günlük yaşamı köklü biçimde dönüştürürken, bu değişimler siyaset alanında da etkisini göstermiş ve egemenliğin klasik tanımının yeniden tartışılmasına yol açmıştır.[52]

Devletler, uluslararası sistemin bir parçası olmayı sürdürebilmek için, milletlerarası hukukun temel ilkelerini ve değerlerini korumayı amaçlayan yargı organlarının kararlarına uymak zorunda kalmakta, bu çerçevede egemenlik yetkilerinin

[51] Arslanel ve Eryücel, **a.g.m.,** s. 25.
[52] Mehmet Erkan Kıllıoğlu, "Siber Egemenlik Konusu", **Mehmet Akif Ersoy Üniversitesi Sosyal Bilimler Enstitüsü Dergisi**, S.40, 2024, s. 144.

belirli ölçüde sınırlandırılmasını kabul etmektedir. İnsan hakları alanında tartışılan önemli konulardan biri de insani müdahale kavramıdır. İnsan haklarının evrensel bir değer olarak benimsenmesi, bu haklara yönelik ihlalleri önlemek amacıyla uluslararası toplumun gerektiğinde müdahalede bulunmasını beraberinde getirmiştir. Bu tür insani müdahaleler sonucunda, müdahale edilen devletin egemenlik yetkileri geçici olarak sınırlandırılmakta veya bağımsızlığı askıya alınabilmektedir. Klasik anlamda iç egemenlik, devletin kendi toprakları üzerinde yasama ve yürütme yetkisini mutlak biçimde kullanabilme gücünü ifade ederken; insan haklarının gelişimiyle birlikte bu mutlakiyet önemli ölçüde zayıflamıştır. Devletler, uluslararası insan hakları belgelerini ve antlaşmaları onaylayarak, kendi hukuk düzenleri dışında doğan normlara uyacaklarını kabul etmiş ve bu normlara aykırı davranmaları halinde uluslararası mahkemelerin yaptırımlarına tabi olmayı taahhüt etmişlerdir. Benzer şekilde, klasik anlamda dış egemenlik, devletlerin diğer devlet veya dış aktörlerin müdahalelerinden tam bağışıklığını ifade ederken, insan haklarının evrenselleşmesiyle bu bağışıklık ilkesi de zayıflamıştır. Milletlerarası hukuk tarafından devletlere yönelik bağlayıcı normların ve yasal kısıtlamaların getirilmesi; insan haklarını sistematik biçimde ihlal eden devletlere karşı uluslararası toplum adına gerçekleştirilen insani müdahalelerin meşrulaşması, bu durumun en somut göstergesidir. Dolayısıyla, günümüzde devletler insan hakları ihlalleri söz konusu olduğunda "egemenlik hakkı" veya "içişlerine karışmama" ilkelerini mutlak biçimde ileri sürememektedir.[53]

2.1. Devletin Siber Alanla İlgili Hak ve Yükümlülükleri

Güvenlik, yalnızca bir gereklilik olmaktan çıkarak günümüzde önemli bir değer unsuru haline gelmiştir. Bu nedenle, devletlerin güvenlik politikaları daima öncelikli konular arasında yer almaktadır. Klasik anlamda devletler, milletlerarası sistemde temel aktör olarak varlıklarını korumayı hedeflerken, internet ve siber alanın yükselişi bu durumu değiştirmiştir. Siber uzayda çok sayıda farklı paydaş ve aktör bulunması, devletlerin güvenliklerini sağlama görevini öncekinden daha karmaşık hale getirmiştir. Teknolojinin ilerlemesiyle bilişim sistemlerinin yaygınlaşması, askeri, siyasi ve ekonomik alanların siber güvenliğe daha fazla odaklanmasına yol açmıştır. Siber uzayın gelişimi, ülkelerin varlıklarını sürdürme algılarını etkilemiş ve savunma stratejilerinde

[53] Arslanel ve Eryücel, **a.g.m.,** s. 30-31.

dönüşümlere sebep olmuştur. Bu bağlamda, bilişim sistemlerindeki siber tehditler, bireysel, ulusal ve milletlerarası düzeyde çeşitli güvenlik krizlerine neden olmaktadır. Geçmişte güvenlik ikilemi daha çok askeri güç ve ordular etrafında yoğunlaşırken, günümüzde siber alan, devletlerin bu ikileme daha sık ve tehlikeli biçimde maruz kalmasına yol açmaktadır. Bu durum, milletlerarası arenada karmaşık ve büyük bir güvenlik ikilemini beraberinde getirmektedir. Devletler, zaman zaman bireylere veya örgütlere karşı bile güvenlik ikilemleriyle karşı karşıya kalabilmektedir; bu da siber güvenliğin sağlanmasını zorlaştırmakta ve ikilemi derinleştirmektedir. 21. yüzyılda siber güvenlik, henüz sonuçları tam olarak öngörülemeyen, yüksek derecede karmaşık bir alan olarak önem kazanmaktadır. Birçok devlet, kritik saldırılar ve tehditler karşısında siber güvenlik alanında kapsamlı çalışmalar yürütmek zorunda kalmıştır. Özellikle İran'a yönelik gerçekleştirilen Stuxnet saldırısı, siber güvenlik disiplininde önemli bir dönüm noktası olarak kabul edilmektedir. Bunu takiben birçok ülke, siber güvenliği geliştirmeye yönelik eylem planları hazırlayarak bu alana önemli yatırımlar yapmaktadır. Bu eğilimin temelinde ise, ulusal güvenlik kaygıları ve güvenlik ikilemi yer almaktadır.[54]

1980'lerden itibaren iletişim ve ulaşım teknolojilerindeki hızlı ilerlemeler, küreselleşme sürecinin etkilerini artırmış ve ülkeler arası karşılıklı bağımlılığı derinleştirmiştir. Bu gelişmeler sonucunda devletler, güvenlik, ekonomi, enerji ve kültür gibi çeşitli alanlarda birbirine daha bağımlı hale gelmiştir. Teknolojideki ilerlemeler ve artan karşılıklı bağımlılık, geleneksel askeri tehditlerin yanında siber tehditlerin de ortaya çıkmasına zemin hazırlamış ve bu tehditler milletlerarası sistemde önemli bir yer edinmiştir. Bu çerçevede, siber saldırı, siber savaş, siber güç ve siber caydırıcılık gibi kavramlar güvenlik literatürüne dahil olmuştur. Güvenlik anlayışındaki bu genişleme, Soğuk Savaş döneminde nükleer silahların caydırıcılık stratejisi üzerindeki etkilerini çeşitlendirmiştir. Soğuk Savaş sırasında, nükleer caydırıcılık karşılıklı yıkım korkusuna dayanarak devletler arasındaki doğrudan çatışmayı engellerken, günümüzde siber alanın karmaşıklığı bu stratejiyi önemli ölçüde zorlamaktadır. Zira bugün caydırıcılık yalnızca devletler arasındaki çatışmaları önlemekle kalmayıp, çok sayıda anonim aktörün neden olabileceği saldırıları da engellemeyi amaçlamaktadır. Siber uzayın devlet dışı aktörler ve bireyleri de kapsaması, güç politikalarında önemli dönüşümlere yol açmaktadır.

[54] Fulya Köksoy, **Yeni Küresel Tehdit Siber Saldırılar, Siber Güvenlik ve Politika Uygulamaları**, 1. b, Nobel Akademik Yayıncılık, 2020, s. 43-47.

Ayrıca, devletlerin giderek daha çok dijital ağlara entegre olması; siber güvenlik, casusluk, gizlilik ve internet özgürlüğü gibi alanlarda yeni zorlukları beraberinde getirmiştir. Bu gelişmelerle birlikte, daha fazla ülkenin siber saldırı kapasitesine sahip olması, milletlerarası siber diyalog kültürünün gelişimini zorunlu kılmıştır. Sonuç olarak, devletlerin siber uzay politikalarını oluştururken iş birliği içinde hareket etmeleri gerektiği düşüncesi, siber diplomasi uygulamalarının yaygınlaşmasına önayak olmuştur.[55]

Milletlerarası hukukun belirlediği sınırlar dahilinde hareket edebilme özgürlüğü incelendiğinde, bu sözde egemenliğin temelinde devletlere hukuk tarafından tanınan yetkileri serbestçe kullanabilme imkânının yattığı anlaşılmaktadır. Başka bir ifadeyle, egemenlik esasen bir tür özgürlük olarak tanımlanabilir; bu özgürlük, milletlerarası hukukun sınırları çerçevesinde devletlerin özgürce hareket edebilme hakkını ifade etmektedir. Milletlerarası hukukun çizdiği sınırlar içinde serbestçe hareket edebilme özgürlüğü, gerçeklere dikkatle bakıldığı takdirde bu sözde egemenliğin arkasında saklı bulunan şeyin aslında devletlerin kendilerine hukuk tarafından tanınmış olan yetkileri serbestçe kullanabilmek iktidarından başka bir şey olmadığı görülür. Yani egemenlik aslında bir özgürlükten ibarettir. Milletlerarası hukukun çizdiği sınırlar içinde serbestçe hareket etme özgürlüğüdür.[56] Devletler egemenlik haklarını hem iç hukuk hem de milletlerarası hukuk ile koruyucu önlemler alamaya çalışmaktadır. Devletler egemenlik haklarını kendi devletinde yaşayan vatandaşları üzerinde bizzat uygulama hakkına sahiptir. Ayrıca devlet egemenlik yetkisine yönelik saldırı ve haksız fillere karşı korumak maksadıyla kanunlar çıkarmaktadır. Bu kanunlar ile amaçlanan asıl gaye ülkesi üzerinde tek egemen güç olduğunu herkese göstermektir. Devletler iç hukukta ceza kanunları çıkararak ülke içerisindeki düzeni korumaya çalışmaktadır.

Suçun işlendiği yerin tespiti, ceza yasalarının uygulanması bakımından büyük önem taşımaktadır. Özellikle suçla bağlantılı hareketlerin ve sonuçların farklı ülkelerde meydana gelmesi durumunda, suçun gerçekleştiği yerin belirlenmesi problemi ortaya çıkar. "Mesafe suçları" olarak adlandırılan bu tür suçlarda, suçun işlendiği ülke netleşmeden, yerel hukuka ilişkin kurallar uygulanamaz. Harekete öncelik veren görüşe göre, suç; failin iradesini ortaya koyduğu hareketin gerçekleştiği yerde işlenmiş sayılır.

[55] Köksoy, **a.g.e.,** s. 51-52.
[56] Çelebi, **a.g.e.,** s. 327-328.

Sonucun meydana geldiği yer ise, bu açıdan belirleyici değildir; çünkü sonuç, failin hareketinden bağımsız dışsal faktörlerin etkisiyle de ortaya çıkabilir. Ayrıca, suçla ilgili en önemli deliller genellikle hareketin yapıldığı yerde bulunur. Bu görüş, 1932 yılında Lahey'de düzenlenen Uluslararası Karşılaştırmalı Hukuk Kongresi ile 1938'de Münih'te toplanan Milletlerarası Ceza Hukuku Birliği Kongresi'nde ağırlıklı olarak desteklenmiştir. Diğer taraftan, sonuca öncelik veren görüş suçun gerçekleşmiş sayılmasının sonucun ortaya çıkmasına bağlı olduğunu savunur. Çünkü sonuç oluşmadan önce hukuki değerlendirme yapmak mümkün değildir. Bu nedenle, hakların ihlal edilmesi ve kamu düzeninin bozulması sonucunda suç meydana gelir ve suçun işlendiği yer, bu sonucun gerçekleştiği ülke olarak kabul edilir. Bu yaklaşımda dikkate alınan sonuçlar, doğrudan veya yakın sonuçlar olarak sınıflandırılır. Sonuca öncelik tanıyan bu görüş, 1931'de Cambridge'de gerçekleştirilen Uluslararası Hukuk Enstitüsü toplantısında benimsenmiştir. Karma görüş ise, suçun hem hareketin hem de sonucun gerçekleştiği yerlerde işlenmiş sayılması gerektiğini belirtir. Bu çerçevede ortaya çıkabilecek yargı yetkisi uyuşmazlıkları, suça ilk müdahale eden devletin yetkili sayılması suretiyle çözülür. Günümüzde birçok ceza kanunu bu karma görüş doğrultusunda düzenlenmiştir. Örneğin, Alman ceza kanunu, failin hareketi gerçekleştirdiği, ihmal durumunda hareket etmesi gerektiği ya da suç tipine uygun sonucun gerçekleştiği yerlerde suçun işlendiğini kabul eder. Benzer şekilde Avusturya ve İsviçre ceza kanunları da hareketin veya sonucun meydana geldiği yeri suçun işlendiği yer olarak tanımlar. Türkiye'de ise, 5237 sayılı Türk Ceza Kanunu'nun (TCK) 8. maddesinin birinci fıkrasında suçun işlendiği yer açıkça belirtilmiş olup, bu düzenleme karma görüşü benimseyerek suçun işlendiği yerin belirlenmesini sağlamaktadır.[57]

TCK Madde 8/1

"Türkiye'de işlenen suçlar hakkında Türk kanunları uygulanır. Fiilin kısmen veya tamamen Türkiye'de işlenmesi veya neticenin Türkiye'de gerçekleşmesi halinde suç, Türkiye'de işlenmiş sayılır."[58]

[57] Kayıhan İçel, **Türk Ceza Hukuku Genel Hükümler**, 6. b, İstanbul: Beta Yayınları, 2021, s. 163-164.
[58] Türk Ceza Kanunu, https://resmigazete.gov.tr/eskiler/2004/10/20041012.htm, (Erişim Tarihi: 29.06.2025).

2.1.1. Devletin Hak ve Yükümlülükleri

2.1.1.1. Savunma Hakkı

Milli yetki meselesi, milletlerarası hukuk alanında köklü ve uzun süredir tartışılan bir konu olup, Milletler Cemiyeti Misakı'nın 15. maddesinin 8. paragrafında "münhasır salahiyet" terimiyle yer aldıktan sonra önemini artırmıştır. Bu önem, daha sonra BM Antlaşması'nın 2. maddesinin 7. paragrafında da korunmuştur. Konuya ilişkin olarak, 1932 yılında Prof. Dr. Georges Scelle, bu sorunun çok sayıda karmaşık tartışmaya yol açtığını belirtmiştir. O tarihten günümüze kadar bu mesele önemini kaybetmemiş, aksine farklı açılardan ele alınarak incelenmiştir. Literatürde "mahfuz saha" kavramıyla da ifade edilen bu sorun, özellikle Milletler Cemiyeti Misakı ile BM Antlaşması metinleri temel alınarak analiz edilmektedir. Söz konusu Milletler Cemiyeti Misakı'nın, milletlerarası uyuşmazlıkların barışçıl çözümünü düzenleyen 15. maddenin 8. paragrafında ise, şu hüküm yer almaktadır.[59]

Milletler Cemiyeti Misakı 15. maddesi 8. paragraf

"Taraflardan biri, anlaşmazlığın uluslararası hukukun yalnız bu tarafın ulusal yetkisine bıraktığı bir soruna ilişkin olduğunu öne sürerse ve Konsey de bunu kabul ederse, Konsey bunu raporunda belirtecek, ancak hiçbir çözüm salık vermeyecektir."[60]

Bazı yazarlar ve devletler, milli yetki kavramını egemenliğin farklı bir ifadesi olarak değerlendirmiştir. Ancak bu alan, milletlerarası hukukun doğrudan düzenlemediği bir sahadır ve esasen devletlerin iç işlerine dair konuları kapsar. Bu nedenle, ilgili meselelerde nihai ve kesin karar yetkisinin devlete ait olduğu ileri sürülmektedir. Ancak bu yaklaşım tam anlamıyla kabul edilebilir değildir; zira milli yetki, milletlerarası hukukun çizdiği sınırlar içinde ve hukuka uygun olarak kullanılmalıdır. Ayrıca belirtmek

[59] Çelebi, **a.g.e.,** s. 331-332.
[60] Milletler Cemiyeti Misakı, https://hukukbook.com/milletler-cemiyeti-antlasmasi/, (Erişim Tarihi: 29.06.2025).

gerekir ki, Milletler Cemiyeti Misakı'nda yer alan "münhasır salahiyet" ifadesi ile BM Antlaşması'nda geçen "milli yetki" kavramı hem metinsel konumları hem de yazılış biçimleri bakımından farklılıklar taşımaktadır. Bununla birlikte, BM Antlaşması'ndaki düzenlemenin daha kapsayıcı ve tatminkâr olduğu değerlendirilir. Nitekim, BM Antlaşması'nın 2. maddesinin 7. paragrafında milli yetki kavramı şu şekilde ifade edilmiştir. [61]

BM Antlaşması 2. madde 7. paragraf

"İşbu Antlaşmanın hiçbir hükmü, Birleşmiş Milletlere herhangi bir devletin kendi iç yetki alanına giren konulara müdahale yetkisi vermediği gibi¸ üyeleri de bu türden konuları işbu Antlaşma uyarınca bir çözüme bağlamaya zorlayamaz; ancak, bu ilke VII. Bölümde öngörülmüş olan zorlayıcı önlemlerin uygulanmasını hiçbir biçimde engellemez." [62]

Milletler Cemiyeti döneminde münhasır yetki, yalnızca milletlerarası anlaşmazlıklar söz konusu olduğunda ileri sürülebilen ve Konsey'in bu konudaki müdahalelerini engelleyen istisnai bir durum olarak kabul edilmekteydi. Ancak BM sisteminde milli yetkinin bir ilke haline gelmesi çeşitli sonuçlar doğurmuştur. Bunlardan en önemlileri, milli yetki itirazının örgütün tüm faaliyetlerinde öne sürülebilmesi ve BM organlarının bu ilkeyi resen (ex officio) dikkate almak zorunda olmalarıdır. Terminolojik açıdan da Milletler Cemiyeti Misakı'nın 15/8 maddesindeki "münhasır salahiyet" ifadesi ile BM Antlaşması'nın 2/7 maddesinde yer alan "milli yetki" kavramı farklılık göstermektedir; ilki daha dar kapsamlı bir anlam taşırken ikincisi daha geniş bir alanı ifade etmektedir. Her iki düzenlemede de milli yetki kapsamına giren meselelerin sınırları açıkça belirlenmemiştir. Bu belirsizlik, hukuk uzmanlarını ulusal yetkinin kapsamını belirleyecek ölçütler aramaya yöneltmiş, ancak bu konuda kesin ve teorik bir ölçüt geliştirmek mümkün olmamıştır. Bu nedenle pek çok hukukçu, milli yetki alanına giren konuların ampirik bir listesini oluşturmayı tercih etmiştir. Ancak hem objektif bir ölçütün bulunamaması hem de milli yetki alanının tam bir listesinin yapılamaması, bu kavramın

[61] Çelebi, **a.g.e.,** s. 332-333.
[62] Birleşmiş Milletler Antlaşması, https://inhak.adalet.gov.tr/Resimler/SayfaDokuman/2212020141836bm_01.pdf, (Erişim Tarihi: 29.06.2025).

kesin sınırlarının olmamasından kaynaklanmaktadır. Milli yetkinin kapsamı, öncelikle milletlerarası ilişkilerin ve bu ilişkileri düzenleyen milletlerarası hukukun gelişimine bağlı olarak değişiklik göstermektedir. Örneğin, geçmişte milletlerarası hukukun düzenlemediği bazı konular devletlerin ulusal yetkisi kapsamında değerlendirilirken, zamanla milletlerarası hukuk tarafından düzenlenmeleri halinde bu konular milli yetki alanından çıkmaktadır. Ayrıca, devletler arasında yapılan anlaşmalar neticesinde bazı meseleler milli yetki sınırları dışına taşınabilmektedir. Dolayısıyla milli yetkinin sınırları devletler arasında farklılık gösterebilmektedir. Somut bir örnek vermek gerekirse, devletler genel olarak ülke topraklarında savunma tesisleri kurma hakkına sahiptir ve bu durum milli yetki kapsamında değerlendirilir. Ancak bir devletin milletlerarası bir anlaşma ile belirli bölgelerde savunma tesisleri kurmaktan vazgeçmesi halinde, bu konu onun ulusal yetkisi alanından çıkmış olur. Türkiye açısından bakıldığında, 1923 tarihli Lozan Boğazlar Sözleşmesi ile Türk Boğazları askerlerden arındırılmış ve bu bölgede Türkiye'nin savunma tesisleri kurması yasaklanmıştır. Böylece, o dönemde ülke sınırları içindeki savunma tesisleri kurma yetkisi genel olarak milli yetki kapsamında olmasına rağmen, Türkiye için bu hak sınırlandırılmıştır. Sonuç olarak, milli yetkinin sınırları sabit olmayıp, zaman içinde milletlerarası ilişkilerin gelişimine ve devletlerarası anlaşmalara bağlı olarak değişmekte ve devletten devlete farklılık göstermektedir. Ancak bu değişkenliğe rağmen, her somut olayda milli yetki sınırlarının belirlenmesi gerekmektedir. Bu nedenle kesin ve evrensel bir ölçütün olmaması, milli yetkinin değerlendirilmesini karmaşık hale getirmektedir.[63]

Devletin ülkesel yetkileri hem kişi hem de eşya bakımından değerlendirildiğinde, milletlerarası hukukun getirdiği sınırlamalar dışında, devletin toprakları üzerinde sürekli ya da geçici olarak bulunan herkes, yurttaşlar ve yabancılar dahil, taşınır ve taşınmaz mallar bu yetkinin kapsamına girer. Devlet, yabancıların ülkesine girişine izin verme konusunda tek yetkili makamdır. Bu bağlamda, iki devlet arasında aksi yönde bir anlaşma bulunmadığı sürece, bir devletin vatandaşları başka bir devletin sınırları içine girmek için o ülkenin iznini almak zorundadır. Uygulamada bu izin, genellikle vize sistemi aracılığıyla sağlanmaktadır. Bununla birlikte, bazı devletler ülkeye girişte vize uygulaması yapmayarak girişleri serbest bırakmakta, ancak belirli şahısları yasaklılar listesine alarak onların girişine engel olmaktadır. Öte yandan, olağandışı koşullar altında,

[63] Çelebi, **a.g.e.,** s. 333-336.

yabancıların sığınmacı olarak bir devlete kabul edilmesi de mümkündür. Sığınma, bir kişinin başka bir devletin topraklarına, diplomatik temsilciliklere, konsolosluk binalarına, savaş gemilerine ya da devlet uçaklarına girerek, kendi devleti veya başka bir devlet tarafından uygulanan baskı ve yasal kovuşturmalardan korunma talebinde bulunmasıdır. Sığınma talebinde bulunanlara ilişkin olarak, ilgili devletin ülkeye giriş koşullarında özel düzenlemeler yapması söz konusu olabilir. Ayrıca, bir devletin sınırları içinde bulunan yabancıların sınır dışı edilmesi de o devletin ülkesel yetkileri arasında yer almaktadır. Eğer devletler arasında yapılan anlaşmalar (örneğin adli yardımlaşma anlaşmaları) ile suç işleyen kişilerin iadesi düzenlenmemişse, ilgili devletin bu konuda takdir yetkisi bulunmaktadır ve suçluların iadesine ilişkin kararları kendisi verir.[64]

Bir hukuk düzeninde yetki kavramı, o düzen içindeki hukuk kişilerini temsil eden bireylerin iradelerini ortaya koyarak hukuki sonuçlar doğurma gücünü ifade eder. Bu bağlamda, her hukuk sistemi, hangi aktörlerin iradelerini açıklayarak hangi hukuki durumları yaratabileceğini belirler. Milletlerarası hukuk sistemi de temel hukuk kişisi olan devletlere belirli yetkiler tanımakta ve bu yetkilerin kapsamını çizmektedir. Geniş anlamda devlet yetkisi, devletlerin ikili veya çok taraflı anlaşmalar gibi çeşitli hukuki işlemleri, hukuka uygun olarak aldıkları kararları ve gerçekleştirdikleri eylemleri kapsar. Ancak milletlerarası hukuk uygulamasında, devletlerin milletlerarası hukuk normları oluşturma ve aralarındaki ilişkileri düzenleme faaliyetleri, yetki kavramının dışında tutulmaktadır. Bu nedenle, devletin yetkisi dar ve teknik anlamda; milletlerarası hukuka uygun şekilde gerçekleştirdiği hukuki işlemlerin, aldığı kararların ve yaptığı eylemlerin hangi coğrafi sınırlar içinde, kimler bakımından ve hangi ölçütlerle geçerli olduğunu belirlemek anlamına gelmektedir.[65]

Konvansiyonel silahlı saldırılara devletlerin yanıt verme biçimlerine ilişkin milletlerarası hukukta hem anlaşmalar hem de teamüller aracılığıyla belirlenmiş çeşitli normatif kaynaklar bulunmaktadır. Ancak siber saldırılar bağlamında benzer bir hukuki kesinlikten söz etmek zordur. Bunun temelinde, devletlerin ve bireylerin fiziksel güvenliğine dair kuralların siber güvenlik alanında da geçerli olup olmadığına dair belirsizlik; siber tehditlere karşı orantılılık ilkesinin uygulanabilirliği ve uygulanacaksa

[64] Pazarcı, Uluslararası Hukuk Dersleri…, 1989, **a.g.e.,** s. 29-31.
[65] Pazarcı, Uluslararası Hukuk Dersleri…, 1989, **a.g.e.,** s. 26-27.

bu orantılılığın nasıl değerlendirileceği; ayrıca hangi tür siber saldırıların meşru müdafaa hakkını doğurduğu gibi temel tartışmalar yer almaktadır.[66]

2.1.1.2. Suçu Önleme Hakkı

Devletin egemenlik hak ve yetkilerinin bir uzantısı olarak ceza yasalarının yer yönünden uygulanmasında temel ilke ülkesellik olarak kabul edilmektedir. Diğer ilkeler ise, genellikle sadece yurt dışında işlenen suçlara ilişkin özel durumlarda ve belirli koşullar çerçevesinde uygulanmaktadır. Örneğin, Alman Ceza Kanunu "yurt içinde işlenen suçlara Alman Ceza Hukuku uygulanır" ifadesiyle, Avusturya Ceza Kanunu "yurt içinde işlenen suçlara Avusturya ceza kanunları uygulanır" şeklinde, İsviçre Ceza Kanunu ise, "İsviçre'de işlenen suçlara bu kanun uygulanır" ifadeleriyle ülkesellik ilkesinin yer yönünden uygulamada temel kural olduğunu açıkça ortaya koymaktadır. Türkiye'de ise, 5237 sayılı TCK'nın 8/1. maddesi "Türkiye'de işlenen suçlar hakkında Türk kanunları uygulanır" hükmüyle, yasaların yer yönünden uygulanmasında ülkesellik ilkesini temel kural olarak benimsemiştir. Bu düzenleme ile Türkiye sınırları içinde, suçun kim tarafından kime karşı işlendiğine bakılmaksızın Türk yasalarının uygulanması öngörülmektedir. Ülkesellik ilkesinin uygulanabilmesi için öncelikle suçun Türkiye sınırları içinde işlenip işlenmediğinin tespiti gerekmektedir. Bu tespitin yapılabilmesi amacıyla, suçun işlendiği yerin ve Türk hukukunda "ülke" kavramının kapsamının netleştirilmesi zorunludur. TCK, ülkesellik ilkesini esas alarak Türkiye'nin kara ve hava sahaları ile kara sularını ülke sınırı olarak tanımlamış ve bu alanlarda işlenen suçların Türkiye'de gerçekleştiğini kabul etmiştir. Bu yaklaşım, Türkiye'nin egemenliğine tabi kara alanları, hava sahası ve kara sularını gerçek anlamda ülke sınırı olarak değerlendirmekte ve ülkesellik ilkesinin öncelikli olarak bu sınırlar içinde geçerli olduğunu vurgulamaktadır. Kanunda açıkça belirtilmemekle birlikte, Türkiye sınırları içindeki akarsular ve göllerin de ülke toprakları kapsamında değerlendirilmesi kuşkusuzdur.[67]

Uygulanan milletlerarası hukukta, devletin ülkesel yetkisini kullanırken karşılaştığı başlıca sınırlamalar arasında, diğer devletlere ve onların vatandaşlarına zarar vermeme yükümlülüğü ile başka devletlerin ülkesel yetkilerine saygı gösterme

[66] Köksoy, **a.g.e.,** s. 388.
[67] İçel, **a.g.e.,** s. 169-170.

zorunluluğu yer almaktadır. Günümüzde milletlerarası hukuk, devletlerin bu yetkilerini kullanırken diğer devletlere veya kişilere zarar vermemesi gerektiğini giderek daha kapsamlı biçimde kabul etmektedir. Bu bağlamda, bir devletin ülkesel yetkilerini kullanırken gerçekleştirebileceği zararlı eylemler veya ihmal durumları çeşitlilik göstermekte ve milletlerarası hukuk tarafından öngörülen yaptırımlar da bu farklılıklar doğrultusunda şekillenmektedir. Özellikle, bir devletin topraklarını başka devletlere karşı saldırı amacıyla kullanmasına izin vermemesi, ihlal edilmemesi gereken temel yükümlülüklerden biridir. Ayrıca, ilgili milletlerarası kararlar da belirtildiği üzere, devletler birbirlerinin toprak bütünlüğü ve saldırmazlık ilkelerine saygı gösterme sorumluluğunu taşımaktadırlar.[68]

Bir devletin, vatandaşlarının yurt dışında işledikleri belirli suçlar nedeniyle kendi hukuk kurallarını uygulaması, faile göre kişisellik ilkesi kapsamında değerlendirilmektedir. Bu ilke özellikle, suçluların iadesine ilişkin uygulamada vatandaşların iade edilmemesi kuralı karşısında önem kazanmıştır; zira bazı kişiler yurt dışında suç işleyip kendi ülkelerine kaçmak suretiyle ceza almaktan kurtulabilmektedir. Bu durumu engellemek amacıyla, faile göre, kişisellik kuralının işletilmesi zorunlu hale gelmiştir. Ülkeler, bu ilkenin uygulanmasına farklı şartlar getirebilmekte olup, Türkiye de TCK'nın 11. maddesiyle, yurt dışında suç işleyen Türk vatandaşlarının Türkiye'de yargılanabilmesine ilişkin koşulları düzenlemiştir.[69]

TCK'nın 11. maddesine göre, suçun işlendiği sırada failin Türkiye Cumhuriyeti vatandaşı olması gerekmektedir; bu şart sağlandığı takdirde, vatandaşlık sonrasında kaybedilmiş olsa dahi Türk kanunları uygulanmaya devam eder. Mağdurun Türk vatandaşı olması ya da olmaması ise, hukuki anlamda belirleyici değildir. Ancak, yabancı bir kişiye karşı işlenen fiilin Türkiye'de Türk yasalarına göre, yargılanabilmesi için, söz konusu eylemin işlendiği ülkede de suç olarak tanımlanması gerekmektedir. Zira, Türk vatandaşının eyleminden zarar gören yabancı, kendi ülkesinin kanunları tarafından korunmuyorsa, bu korumayı Türk yasalarından da talep etme hakkına sahip değildir. Ayrıca, TCK'nın 13. maddesinde belirtilen suçlar kapsamında olmaması gerekir. Bunun yanı sıra, söz konusu suçun Türk kanunlarına göre, cezasının bir yıldan az olmaması şartı aranır. Failin Türkiye'de bulunması ve ilgili suçtan dolayı yabancı bir ülkede henüz

[68] Pazarcı, Uluslararası Hukuk Dersleri…, 1989, **a.g.e.,** s. 33-34.
[69] İçel, **a.g.e.,** s. 172.

hüküm verilmemiş olması da kovuşturmanın ön koşullarındandır. Son olarak, işlenen suçun Türkiye'de kovuşturulabilir nitelikte olması gerekmektedir.

2.2. Devletin Milletlerarası Hukukta Hak ve Yükümlülükleri

Her toplumun kendine özgü hukuk kuralları olduğu gibi, milletlerarası toplumun düzenini sağlayan milletlerarası hukukta milletlerarası düzenin tesisinde temel bir işlev görmektedir. Ancak iç hukuk sistemlerinde toplumsal düzeni sağlamak amacıyla üstün ve teşkilatlanmış bir otorite ile sistemli müeyyide mekanizmaları bulunmasına karşın, milletlerarası hukukta bu düzeyde bir teşkilatlanma mevcut değildir. Buna rağmen milletlerarası hukuk, tıpkı diğer hukuk alanlarında olduğu gibi, zaman içinde gelişme göstermektedir.[70]

Milli yetki alanına giren bir konuda milletlerarası yükümlülüklerin bulunması, söz konusu meselenin milli yetki sınırları dışına çıkmasına neden olur. Bu ilke, milli yetkinin mutlak olmaması, zamanla ve devletler arasında farklılık göstermesi sorununa bir yanıt olarak ortaya çıkar ve bu kapsamda bir temel prensip niteliği taşır. Ancak, bu ilkede yer alan "milletlerarası yüküm" kavramının sınırları ve kapsamı açıklığa kavuşturulmalıdır. Burada, yalnızca milletlerarası antlaşmalar mı milletlerarası yükümlülük sayılır sorusu önemlidir. Bazı hukukçular, milli yetki alanındaki bir konunun sadece antlaşmalar yoluyla düzenlenmesi halinde milli yetkiden çıktığını savunmaktadır. Oysa milli yetki alanından çıkış yalnızca antlaşma varlığına bağlı değildir. Zira milli yetki, devletlere milletlerarası hukuk tarafından tanınan kullanma yetkisi olarak değerlendirildiğinde, ilgili konuda milletlerarası hukuk kurallarıyla (teamül hukuku da dahil) bir düzenleme yapıldığında, bu konu artık milli yetki kapsamında değerlendirilmemelidir. Bu durum, bazen antlaşmalarla, bazen ise, teamül kurallarıyla gerçekleşebilir. Özetle, milli yetkiye ilişkin bir konunun kapsamını belirlerken iki temel ilke dikkate alınır: Birincisi, ilgili konuda milletlerarası düzenlemenin varlığıdır; ikincisi ise, milli yetkinin kapsamı konusunda kuşku bulunduğunda, bu kuşkunun ulusal değil, milletlerarası otoriteler lehine çözülmesidir. Bu yaklaşım, "sınırlı bağımsızlık" kavramının doğal bir sonucudur; çünkü bağımsızlık, devletin milletlerarası hukuktan kaynaklanan yetkilerini özgürce kullanabilme iradesidir. Eğer bu yetkilerin varlığı konusunda şüphe varsa ve bu şüphe giderilemiyorsa, söz konusu yetkinin milletlerarası hukuk kapsamında olmadığı kabul

[70] Bozkurt, Poyraz ve Erdal, **a.g.e.,** s. 305.

edilir. Üçüncü ilke ise, milli yetkiye ilişkin anlaşmazlıkların ilgili devletler tarafından tek taraflı olarak çözülemeyeceğidir. Bu durum, BM Antlaşması öncesinde tartışma konusu değildi; zira Milletler Cemiyeti Konseyi, taraflardan biri iddiada bulunduğunda bu iddiayı inceler ve karar verir, devletlerin kendi yetkisini tayin etmelerine olanak tanımazdı. Ancak BM Antlaşması'nın 2. maddesi 7. paragrafında bu tür iddialarla ilgili bir karar merci belirtilmemiştir. Bazı hukukçular bunun devletlerin kendi yetkilerini belirleme hakkını tanıdığı görüşünü savunmuştur. Bu ise, milletlerarası teşkilatların işleyişini ve milletlerarası hukukun etkinliğini ciddi şekilde zayıflatır. Nitekim BM Teşkilatı, bu yetkiye sahip olmasına rağmen milli yetki iddialarını incelemekte ve karara bağlamaktadır. Milletlerarası Adalet Divanı'nın yargısı zorunlu olmamakla birlikte, taraf devletlerin önceden kabul ettikleri durumlarda, anlaşmazlıklarda doğrudan dava açılabilir. Ancak bazı devletler, bu tür yükümlülüklerine "milli yetki konusunda karar verme hakkı" şeklinde çekince koymuş, böylece milli yetki iddialarını reddetme yetkisini kendilerinde tutmuştur. Bu uygulama, Divan'ın görevini sınırlar.[71]

Milletlerarası hukukta kuvvet kullanımının yasaklanması ilk kez 16 Ekim 1925 tarihinde Almanya, İngiltere, İtalya, Fransa ve Belçika arasında imzalanan Ren Misakı ile kabul edilmiştir. Milletlerarası ilişkilerde kuvvet kullanımını evrensel ölçekte yasaklayan en önemli belge ise, BM Antlaşmasıdır. Günümüzde BM Antlaşması, devletlerin kuvvet kullanımını temel olarak yasaklasa da hukuka uygun kabul edilen belirli durumlara da imkân tanımaktadır.[72]

2.2.1. Milletlerarası Hukukta Savunma Hakkı

BM sisteminde temel prensip, milletlerarası uyuşmazlıkların barışçıl yollarla çözülmesidir. BM Antlaşması'nın birçok maddesi bu ilkeyi vurgulamaktadır. Örneğin, Antlaşma'nın önsözünde, BM üyelerinin "milletlerarası barış ve güvenliğin korunması amacıyla güçlerini birleştirme" ve "ortak çıkarlar dışında silah kullanımını önleyen prensipleri kabul edip yöntemler geliştirme" kararlılığı belirtilmiştir. Örgütün amaçları arasında yer alan milletlerarası barış ve güvenliğin korunması, Antlaşma'nın 1. maddesinin 1. fıkrasında öncelikli hedef olarak ifade edilmiştir. Bu amaç doğrultusunda benimsenen ilkeler ise, 2. maddede yer almakta olup, özellikle 2/3. fıkrada, üye

[71] Çelebi, **a.g.e.,** s. 336-339.
[72] Pazarcı, Uluslararası…, 2021, **a.g.e.,** s. 551.

devletlerin milletlerarası uyuşmazlıklarını barışçıl yollarla çözerek milletlerarası barış, güvenlik ve adaleti tehlikeye atmaktan kaçınacakları hükme bağlanmıştır. Madde 33 uyarınca, devletler arasındaki anlaşmazlıklar ya kendi aralarında ya da BM aracılığıyla barışçıl yöntemlerle çözüme kavuşturulmaya çalışılır; ancak bu çözümler gerçekleşmemişse, meşru müdafaa hakkı (md. 51) dışında kuvvet kullanımı yasaklanmıştır. BM Antlaşması, 2/4 maddesi ile kuvvet kullanımını genel olarak yasaklamakta olup, bu yasaklama milletlerarası teamül hukukunun da temel bir kuralını teşkil etmekte ve Antlaşma'nın en önemli hükümlerinden biridir.[73]

Devletlerin güç kullanımı bağlamında sıklıkla tartışılan konulardan biri, meşru savunma hakkının kapsamı ile bu hakkın hangi şartlarda kullanılabileceğidir. BM Şartı'nın 51. maddesine göre, bir devletin meşru savunma hakkını kullanabilmesi için öncelikle "silahlı saldırıya" maruz kalması gerekmektedir. 1974 yılında BM Genel Kurulu tarafından kabul edilen 3314 (XXIX) sayılı "Saldırının Tanımı" kararıdır. Bu karar, Güvenlik Konseyi'nin saldırı tanımı yaparken dikkate alması gereken kriterleri belirlemeye çalışmıştır. Karar, saldırıyı üç aşamalı bir biçimde ele almakta; ilk maddesinde BM Şartı'nın 2/4. maddesine paralel olarak, bir devletin diğerinin egemenliği, toprak bütünlüğü veya siyasal bağımsızlığına karşı ya da BM Şartı ile uyuşmayan biçimde silahlı güç kullanmasını saldırı olarak tanımlamaktadır. İkinci maddede ise, saldırının meşruiyeti konusunda ispat yükü ilk silahlı gücü kullanan devlete ait kılınmıştır. Yani, BM Şartı'na aykırı ilk silahlı eylem, otomatik olarak saldırı sayılacaktır. Ancak bu madde aynı zamanda Güvenlik Konseyi'ni, saldırı niteliği taşıyıp taşımadığına karar verirken olayın koşullarını ve sonuçlarının ağırlığını değerlendirmeye davet etmektedir. Üçüncü maddede ise, belirli eylemler (işgal, abluka, bombardıman, bir devletin topraklarını başka bir devlete kullandırmak suretiyle saldırı gerçekleştirilmesi, silahlı gruplar aracılığıyla güç kullanımı gibi) saldırı olarak kesin biçimde nitelendirilmiştir. İkinci tartışma konusu ise, meşru savunma hakkının kullanımı için fiili bir silahlı saldırının beklenip beklenmemesi gerektiğidir. Genel Kurul, ilk silahlı güç kullanımının saldırı olduğunu kabul etmekle birlikte, Güvenlik Konseyi'nin olayın ciddiyetini dikkate alarak değerlendirme yapması gerektiğini belirtmiştir. [74]

[73] Bozkurt, Poyraz ve Erdal, **a.g.e.,** s. 307.
[74] Nejat Doğan, Cenap Çakmak ve Halil Kürşad Aslan (der.), **Birleşmiş Milletler: BM Sistemi ve Reformu**, Ankara: Siyasal Kitabevi, Aralık 2014, s. 58-60.

Kavramın sınırlarının açık şekilde belirlenmemesi, hangi eylemlerin silahlı saldırı kapsamında değerlendirileceği hususunda yorum farklılıklarına ve belirsizliklere yol açmaktadır. Bu konuda referans alınan temel belge, BM Genel Kurulu'nun 14 Aralık 1974 tarihli ve A/3314 sayılı "Saldırının Tanımı" Kararıdır. Söz konusu karar, saldırı eylemlerinin nitelik ve kapsamını belirlemeye yönelik uluslararası düzeyde kabul görmüş en önemli düzenlemelerden biri olma özelliğini taşımaktadır. Kararda yer alan ilgili hüküm şu şekildedir:[75]

"Bir devletin başka bir devletin egemenliğine, toprak bütünlüğüne veya siyasal bağımsızlığına karşı herhangi bir biçimde BM Kurucu Antlaşmasına aykırı olarak silahlı kuvvet kullanımıdır".[76]

Bu bağlamda, bir devletin kendisine yönelik ciddi ve yakın bir tehdit durumunda önleyici veya önceden yapılan savunma hakkını kullanıp kullanamayacağı sorusu ortaya çıkmaktadır. Literatürde bu konu halen tartışmalıdır; ancak genel uygulamada ve BM Şartı'nın yorumunda meşru savunma hakkı dar kapsamda değerlendirilmekte, önleyici müdahaleler sınırlı kabul edilmektedir. Üçüncü önemli husus, bir devletin maruz kaldığı saldırıya karşı üçüncü bir devletin meşru savunma hakkını kullanıp kullanamayacağıdır. Örneğin, saldırıya uğrayan bir devlet kendisini savunamaz hale geldiğinde, başka bir devletin X devletinin çağrısı olmadan ve kolektif meşru müdafaa hakkına dayanarak saldırganlara karşı güç kullanıp kullanamayacağı tartışmalıdır. Son olarak, BM Şartı'nın 51. maddesinde belirtilen meşru müdafaa hakkının, Güvenlik Konseyi'nin milletlerarası barış ve güvenliği sağlamak amacıyla gerekli önlemleri almasına kadar süreceği kabul edilmiştir. Milletlerarası hukuk ve BM Şartı'nın genel yorumları, silahlı saldırı olmaksızın yapılan karşı eylemlerin, siyasi veya ekonomik gerekçelere dayanan faaliyetlerin ya da silahlı olmayan gruplara karşı girişilen eylemlerin meşru savunma kapsamına girmemesi gerektiğini vurgulamaktadır.[77]

---

[75] Ulaş Can Değdaş, "Uluslararası Hukukta Önleyici Meşru Müdafaa Hakkı", **Anadolu Üniversitesi Hukuk Fakültesi Dergisi**, C.1, S.6, 2018, s. 27.
[76] BM Genel Kurulu'nun 14 Aralık 1974 tarih ve A/3314 sayılı "Saldırının Tanımı" kararı, http://www.un-documents.net/a29r3314.htm, (Erişim Tarihi: 01.11.2025).
[77] Doğan, Çakma, Aslan, (der.), **a.g.e.,** s. 58–60.

BM Antlaşması'nda kuvvet kullanımına ilişkin genel yasaklamaya rağmen, dört belirgin istisnanın varlığı göze çarpmaktadır. Bunlar şunlardır:

a) Meşru müdafaa kapsamında kuvvet kullanımı (m. 51),
b) BM Güvenlik Konseyi'nin kararıyla kuvvet kullanımı (VII. Bölüm),
c) Güvenlik Konseyi faaliyete geçmeden önce beş daimî üyenin kuvvet kullanımı (m. 106),
d) II. Dünya Savaşı sırasında düşman devletlere karşı kuvvet kullanımı (m. 107).

Bu istisnalar arasında özellikle ilk iki maddeye odaklanmak gerekmektedir. BM Antlaşması'nın 51. maddesi, hem bireysel hem de kolektif meşru müdafaa hakkını düzenlemektedir. Buna göre, BM üyesi herhangi bir devlete yönelik silahlı bir saldırı gerçekleştiğinde, Güvenlik Konseyi milletlerarası barış ve güvenliği korumak üzere toplanıp gerekli önlemleri alana kadar, saldırıya uğrayan devlet tek başına veya diğer devletlerle birlikte meşru müdafaa hakkını kullanabilir. Bu bağlamda, meşru müdafaa hakkı, herhangi bir sınırlamaya tabi tutulmaksızın uygulanabilir.[78]

NATO üyesi devletlerin onayladığı 5. maddeye göre, bir NATO müttefikine yönelik gerçekleştirilen silahlı saldırı, tüm üyelere karşı yapılmış sayılmakta ve bu durumda diğer üyeler, saldırıya maruz kalan müttefike destek sağlamak amacıyla gerekli gördükleri önlemleri alma yükümlülüğünü üstlenmektedir.

Kuzey Atlantik Antlaşması madde 5

"Taraflar, Avrupa veya Kuzey Amerika'da bir veya daha fazlasına yönelik silahlı bir saldırının hepsine yönelik bir saldırı olarak değerlendirileceği konusunda anlaşmışlardır ve dolayısıyla, böyle bir silahlı saldırı meydana gelirse, her birinin, Birleşmiş Milletler Şartı'nın 51. maddesi'nde tanınan bireysel veya kolektif meşru müdafaa hakkını kullanarak, saldırıya uğrayan tarafa veya taraflara, derhal, bireysel olarak ve diğer taraflarla birlikte, silahlı kuvvet kullanımı da dahil olmak üzere,

[78] Bozkurt, Poyraz ve Erdal, **a.g.e.,** s. 308.

Kuzey Atlantik bölgesinin güvenliğini yeniden sağlamak ve sürdürmek için gerekli gördüğü eylemleri gerçekleştirerek yardım edeceklerini kabul etmişlerdir.

Bu tür silahlı saldırılar ve bunun sonucunda alınan tüm önlemler derhal Güvenlik Konseyi'ne bildirilecektir. Güvenlik Konseyi uluslararası barış ve güvenliği yeniden sağlamak ve sürdürmek için gerekli önlemleri aldığında bu tür önlemler sona erdirilecektir".[79]

2.2.2. Suçluyu Cezalandırma Yetkisi

TCK'nın 13. maddesi, devletin korunması ilkesine dayanarak, yabancı bir ülkede Türkiye'nin varlıklarına ve özellikle siyasal çıkarlarına yönelik işlenen suçların cezalandırılmasına imkân tanıyan hukuki düzenlemeleri içermektedir. Bu madde kapsamında, Türkiye'ye karşı yabancı bir ülkede işlenen belirli suçların failleri, Türk vatandaşı olup olmadıklarına bakılmaksızın, Türkiye'de yargılanabilmekte ve Türk yasalarına göre, cezalandırılabilmektedir.[80]

TCK kapsamında devletin korunmasına ilişkin suçlar şu şekilde sınıflandırılmaktadır: Birinci grup, devletin egemenlik simgelerine ve resmi organlarına yönelik suçları içermekte (md. 299-331); ikinci grup, devletin güvenliğine karşı işlenen suçları kapsamaktadır (md. 302-308). Üçüncü kategoride, anayasal düzene ve bu düzenin işleyişine yönelik suçlar yer almakta (md. 309-316), dördüncü grupta ise, milli savunmaya karşı suçlar ele alınmaktadır (md. 317-325). Beşinci sınıf, devlet sırlarının korunmasına ilişkin suçlar ve casusluk faaliyetlerini kapsamaktadır (md. 326-339). Son olarak, altıncı grup, yabancı devletlerle ilişkiler bağlamında işlenen suçları içermektedir (md. 340-343).

Devletlerin, evrensel değerler aleyhine işlenen suçları, failin kimliği veya suçun işlendiği yer gözetilmeksizin, bu değerleri koruma amacıyla yargılama ve cezalandırma

[79] Kuzey Atlantik Antlaşması, https://www.nato.int/cps/en/natohq/official_texts_17120.htm, (Erişim Tarihi: 28.06.2025).
[80] İçel, **a.g.e.,** s. 178.

yetkisini ifade eden tek taraflı evrensel yetki, TCK'nın 13. maddesinde hukuki düzenlemelerle güvence altına alınmıştır. [81]

TCK'ya göre tek yanlı evrensel yetkinin kapsamına aldığı suçlar şöyledir; 1- soykırım ve insanlığa karşı suçlar, göçmen kaçakçılığı ve insan ticareti (md76-80), 2- işkence (md.94,95), 3- çevrenin kasten kirletilmesi (md.181), 4- uyuşturucu veya uyarıcı madde imal ve ticareti (md.188), 5- uyuşturucu veya uyarıcı madde kullanılmasını kolaylaştırmak (md.190), 6- parada sahtecilik (md. 197), 7- para ve kıymetli damgaları imale yarayan araçların üretimi ve ticareti (md.200), 8- mühürde sahtecilik (md. 202), 9- fuhuş (mh.227), 9- deniz, demiryolu veya havayolu ulaşım araçlarının kaçırılması veya alıkonulması (md.223/2, 3), ve bu tür araçlara zarar verme suçları (md.152). Burada saymış olduğumuz suçlardan dolayı tek yanlı evrensellik yetkisinin kapsamında olan bu suçlardan dolayı Türkiye'de yargılama yapılabilesi için Adalet Bakanın istemi gereklidir. Soykırım ve insanlığa karşı suçlar ile göçmen kaçakçılığı ve insan ticareti suçlarından dolayı yabancı bir ülkede mahkûmiyet veya beraat kararı verilmiş olsa da Adalet Bakanının talebi üzerine Türkiye yeniden yargılama yapabilir. Diğer suçlarda ise, yabancı ülkede böyle bir mahkeme kararı var ise, artık Türkiye yargılama yapamayacaktır.

Bilgi ve iletişim teknolojilerinin küresel çapta yaygınlaşmasıyla birlikte, siber ortamı kullanan kişi sayısında önemli bir artış gözlemlenmiştir. Bu durum, internetin siyasi, askeri ve ekonomik alanlardaki etkilerinin giderek belirginleşmesine yol açmış ve devletler, kendi sınırları içinde bu alanı kontrol altına almayı öncelik haline getirmiştir. Devletler, siber alan üzerindeki denetimlerini siyasi, ekonomik, kültürel ve teknolojik araçlar aracılığıyla sağlamaya çalışmaktadır. Zira siber güvenlik açıkları, rakip devletler tarafından siyasi ve stratejik hedeflere ulaşmak amacıyla istismar edilme riski taşımaktadır. Bu duruma örnek olarak, İran'ın nükleer enerji programına yönelik olarak kullanılan Stuxnet solucanı ile internet üzerinden bilgi toplama faaliyetlerini yürüten PRISM programı gösterilebilir. Bahsi geçen olaylar, devletlerin siber uzaya ilişkin kaygılarını artırmış ve bu alanda kontrol sağlamak amacıyla politika geliştirmeye daha fazla önem vermelerine neden olmuştur.[82]

[81] İçel, **a.g.e.,** s. 179.
[82] Kıllıoğlu, **a.g.e.,** s. 134.

2.2.3. Geri Verilmesini Talep Hakkı

Bir devlet sınırları içinde suç işleyip ardından başka bir ülkeye kaçan suçluların, suçun işlendiği ülkede yargılanması veya önceden verilen cezanın infaz edilmesi amacıyla, devletler arası suçluların iadesi uygulamasına başvurulmaktadır. Tarih boyunca suç, işleniş yeri ve fail kim olursa olsun hem ilgili toplumun hem de milletlerarası toplumun zararına olan bir fiil olarak değerlendirilmiş ve toplumsal düzeni koruyan normlar çerçevesinde kınanmıştır. Bu bağlamda, suçluların iadesi mekanizması, "ya iade et ya da yargıla" (aut dedere aut judicare) prensibi üzerine kurulmuştur.[83] Esasen suç, nerede ve kim tarafından işlenirse işlensin geçmişten günümüze gerek suçun işlendiği topluluk gerekse milletlerarası toplumun zararına olan bir davranış olarak nitelendirilmiştir.[84]

Savaş hukuku ile milletlerarası hukukun gelişimi sürecinde, esir düşen askerlerin yanı sıra, bir devlet sınırları içinde suç işleyen yabancıların bulundukları ülkede yargılanıp yargılanamayacağı ve kendi ülkelerine iade edilip edilmeyeceği gibi hukuki sorunlar gündeme gelmiştir. Bu sorunlara çözüm arayışı kapsamında çeşitli kurumlar ortaya çıkmış; esir kavramı ile esirlerin iadesi ve takası gibi uygulamalar bu süreçte geliştirilmiştir. Özellikle iade mekanizması, milletlerarası hukukun evrimi ve devletler arasındaki adli yardımlaşma gereksinimleri doğrultusunda şekillenmiş bir kurumdur.[85] İade Kurumu, milletlerarası hukukun gelişiminin ve devletler arasındaki adli yardımlaşma ihtiyacının bir sonucu olarak ortaya çıkmıştır.[86]

Devletlerin kendi egemenlik alanları içinde suç işleyen bireyleri yargılama yetkisi söz konusu olduğunda, temel kabul genellikle suçun işlendiği ülkenin bu kişileri yargılama hakkına sahip olduğudur. Bu ilke, mülkilik prensibi olarak adlandırılmakta

[83] Kayıhan İçel, Suçluların Geri Verilmesi Üzerine Bir İnceleme, **İstanbul Hukuk Fakültesi Dergisi**, 30, (3-4), Temmuz 2011, s. 693.
[84] Ahmet Ulutaş, "Suçluların İadesine Dair Avrupa Sözleşmesi ve Türkiye", (Gazi Üniversitesi SBE Yayımlanmamış Doktora Tezi), Ankara, 2010, s. 1.
[85] Yusuf Yaşar ve Zafer İçer, "Tutuklu ve Hükümlülerin Takası ve İadesi", **Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi**, C.25, S.2, 2019, s. 1488.
[86] İzzet Özgenç, **Türk Ceza Hukuku Genel Hükümler**, 17. b, Ankara: Seçkin Yayıncılık, 2021, s. 1112.

olup, failin kim olduğu dikkate alınmaksızın, suçun gerçekleştiği devletin yargı yetkisinin bulunduğunu kabul eden evrensel bir ceza hukuku kuralıdır.[87]

Geniş bir perspektiften ele alındığında, geri verme kavramı, başka bir ülkeye kaçmış ya da o ülkede bulunan sanık veya hükümlünün, yargılama ve cezanın infazı amacıyla yetkili devlete iade edilmesini ifade etmektedir.[88] Kısacası, geri verme; bir devletin yargı yetkisine giren bir suçu işleyip, diğer bir devlete kaçan kişinin, yargılamaya yetkili olan devletin talebi üzerine, bu devlete teslim edilmesidir.[89]

Geri verme kurumu, Osmanlı döneminde "iade-i mücrimin" terimiyle anılmıştır. Türkiye Cumhuriyeti'nin 765 sayılı TCK'da bu kavram "suçluların iadesi" olarak yer alırken, günümüzde 5237 sayılı TCK'da ise, "geri verme" ifadesi kullanılmaktadır.[90]

Ceza hukukunun temel ilkelerinden biri olan mülkilik prensibi, suç işledikten sonra başka bir ülkeye kaçan şahısların takibine engel teşkil etmektedir. Adaletin sağlanması ve suçlunun işlediği fiil nedeniyle cezalandırılması gerekliliği kapsamında, suçlunun iadesi talebinde bulunan devlete teslim edilmesi zorunludur. Suçluların başka bir devlete kaçması durumunda, devletler arasındaki nezaket kuralları ve karşılıklı yardımlaşma yükümlülüğünün gereği olarak iade mekanizmasına başvurulmaktadır. Geri verme işlemi, devlet topraklarının suçlulara barınak sağlamaması ilkesine dayanmakta olup, temel amacı adaletin gerçekleştirilmesi ve kamu yararının korunmasıdır.[91] Suçlunun başka bir ülkeye kaçması durumunda devletlerarası nezaket kuralının ve yardımlaşma yükümlülüğünün bir gereği olarak iade kurumuna başvurulmaktadır.[92]

Mülkiyet ilkesinin ceza hukukundaki temel prensiplerden biri olması, suç işledikten sonra başka bir ülkeye kaçan şahısların takip edilmesini zorlaştırabilmektedir.

---

[87] Ahmet Can Yazgı, "6706 Sayılı Cezai Konularda Uluslararası Adli İş Birliği Kanunu Çerçevesinde İadenin Kabul Edilemeyeceği Haller", (İstanbul Üniversitesi SBE Yayımlanmamış Yüksek Lisans Tezi), İstanbul. 2019, s. 3.

[88] Süheyl Donay, "Suçluların İadesinde Yeni Gelişmeler", **İstanbul Hukuk Fakültesi Dergisi**, C.50, S.1-4, 1984, s. 239.

[89] Mustafa Cin, "Suçluların Geri Verilmesi ve Türk Hukuk", (İstanbul Üniversitesi SBE Yayımlanmamış Yüksek Lisans Tezi). 1996. s. 5.

[90] Mehmed Yerlikaya, "Türk Ceza Hukuku'nda Geri Verme Kurumu ve Avrupa Tutuklama-Yakalama Müzekkeresi", (İstanbul Üniversitesi SBE Yayımlanmamış Yüksek Lisans Tezi), İstanbul, 2010, s. 4.

[91] Ahmet Cemal Ruhi, Türk Hukukunda Suçluların İadesi, **Erzincan Binali Yıldırım Üniversitesi Hukuk Fakültesi Dergisi**, 7, (1-2), 2003, s. 498.

[92] İsmail Özkarcı, Ulusal ve Uluslararası Hukukta Terör Suçlularının İadesi, (Ankara Yıldırım Beyazıt Üniversitesi SBE Yayımlanmamış Doktora tezi), 2019, s. 49.

Ancak, işlenen suç nedeniyle adaletin tesisi amacıyla, suçlunun iade talebinde bulunan devlete teslim edilmesi gerekliliği ön plana çıkmaktadır. Suçlunun başka bir ülkeye sığınması durumunda, devletler arasındaki nezaket kuralları ve karşılıklı yardımlaşma yükümlülüğü doğrultusunda iade mekanizması devreye girmektedir. Geri verme işlemi, devlet topraklarının suçlulara sığınak olmaması ilkesine dayanmakta olup, bu süreçte adaletin sağlanması ve kamu yararının korunması temel hedefler arasında yer almaktadır. Hukuki açıdan geri verme kavramı, milletlerarası adli yardımlaşmanın bir türü olarak değerlendirilmektedir.[93] Geri verme işlemi, devlet toprağının suç işlemiş bir kişiye sığınak olmaması ilkesine dayanmaktadır. Bu çerçevede, geri verme işleminin özünde, aslında adaletin gerçekleştirilmesi ve kamusal yararın sağlanması amacı da bulunmaktadır.[94]

İade sürecinin işleyebilmesi için devletler arasında doğrudan bir ikili ilişki kurulması gerekmektedir. Milletlerarası hukuk çerçevesinde bu ilişkinin temel dayanağını ise, taraf devletler arasında yapılan anlaşmalar oluşturmaktadır. Bu bağlamda, iade işleminin hukuki zemini öncelikle bu tür milletlerarası antlaşmalarla şekillenmektedir. Pratikte, 19. yüzyıldan itibaren iade hukuku düzenlemeleri büyük ölçüde iki taraflı antlaşmalar aracılığıyla gerçekleştirilmiştir.[95] Geri verme devletler arasında ilişkiyi gerektirmekte ve bu sebeple kural olarak bir milletlerarası hukuk kurumudur. Bu nedenle iade kurumu konusunda antlaşma yapılması zorunludur. Geri verme ile ilgili olarak, her ülke kendi iç hukuk kurallarına göre, yöntemini tayin edeceğinden, iç mevzuatın da bu konuda hüküm içermesi gerekir. Zaten antlaşmalar da belirli bazı konularda zorunlu olarak iç hukuka atıfta bulunmaktadır.[96]

Milletlerarası alanda suçla ve suçlularla etkin mücadele, büyük ölçüde devletler arası iş birliğine dayanmaktadır. Bu iş birliği çoğunlukla milletlerarası antlaşmalar aracılığıyla kurumsallaşmakta olup, aynı zamanda milletlerarası teamül hukuku ve karşılıklılık ilkesi gibi geleneksel kaynaklara da dayanmaktadır. Türkiye açısından ise, Suçluların İadesine Dair Avrupa Sözleşmesi (SİDAS) ile bu sözleşmeye eklenen

[93] Ruhi, **a.g.m.,** s. 498.
[94] İçel, **a.g.e.,** s. 182.
[95] Özgenç, **a.g.e.,** s. 1113.
[96] Donay, **a.g.m.,** s. 240.

protokoller, suçluların iadesi sürecinde başvurulan başlıca hukuki metinler arasında yer almaktadır.

Kurumun milletlerarası kaynakları ise; milletlerarası antlaşmalar, teamül kuralları ile karşılıklılık ilkesidir.[97] Ayrıca Türkiye'nin de taraf olduğu SİDAS ve bu Sözleşmeye Ek Protokolleride kaynak olarak sayabiliriz.

İade işlemi, genel anlamda başka bir ülkede suç işlediği ya da işlemekle suçlanan kişilerin bulundukları ülkeden (talep edilen devlet) suçun işlendiği ülkeye (talep eden devlet) teslim edilmesi süreci olarak tanımlanır. Bu bağlamda, iade ilişkisine taraf olan devletler, durumlarına göre, bazen talep eden, bazen de talep edilen taraf konumunda olabilirler. Dolayısıyla, iade sürecinde taraf devletlerin statüsüne göre, geri verme koşulları ve prosedürleri farklılık gösterebilir.[98] İade sürecinde öncelikli olarak, suçlunun teslimi talebinde bulunan ülke ile talep edilen ülke arasında iade konusunu düzenleyen bir anlaşmanın bulunup bulunmadığı önemli bir kriterdir. Eğer taraflar arasında böyle bir anlaşma mevcutsa, iade işlemleri bu anlaşmanın hükümleri doğrultusunda yürütülür. Ancak, iade işleminin gerçekleşmesi için mutlaka taraflar arasında bir anlaşma olması zorunlu değildir. Anlaşma olmaması durumunda da devletler, karşılıklı anlayış ve kendi iç hukuk sistemlerindeki düzenlemeler çerçevesinde, suçlunun iadesi konusunda karar verebilir ve iade talebini kabul edip etmeme konusunda serbest iradelerini kullanabilirler.

Geri verme kurumu ile ilgili sözleşmeler arasında en fazla uygulanan SİDAS'tır. Türkiye Cumhuriyeti bu Sözleşmeyi 13.12.1957 tarihinde Paris'te imzalamıştır. Sözleşme 18.04.1960 tarihinden itibaren yürürlükte bulunmaktadır. SİDAS ile taraf devletlerin daha önceden kendi aralarında imzaladıkları iki taraflı sözleşmeleri geçersiz kılmıştır.[99] Türkiye, SİDAS'ın ikinci Ek Protokolü 1991 yılında onaylamış ve yürürlüğe koymuştur. Ayrıca SİDAS'ın 1. Ek Protokolü, 3. Ek Protokolü ve 4. Ek Protokolünü 2016 yılında onaylamış ve yürürlüğe koymuştur.[100]

[97] Berat Duman, "Türk Hukukunda Geri Verme Kurumu ve Usulü", **Türkiye Adalet Akademisi Dergisi**, S.24, 2016, s. 671.
[98] Yazgı, **a.g.t.,** s. 43.
[99] Saeed Bagheri, "Uluslararası Hukukta Suçluların İadesi ve Suçluları Kovuşturma Yükümlülüğü", **Ankara Üniversitesi Hukuk Fakültesi Dergisi**, S.1, 2013, s. 6.
[100] Özgenç, **a.g.e.,** s. 1115.

SİDAS'ın amacı yalnızca Avrupa kıtasıyla sınırlı kalmayıp, mümkün olduğunca daha geniş bir coğrafyada geri verme alanında milletlerarası hukuk normlarının oluşturulmasıdır. Bu doğrultuda, taraf devletlerin iç hukuk düzenlemeleri ile milletlerarası hukuk kurallarının uyumlaştırılması ve uygulamadaki farklılıkların en aza indirilmesi hedeflenmektedir. Bu sayede, Avrupa Konseyi üyesi olmayan ülkelerin de sözleşmeye katılımı mümkün hale gelmiştir.[101]Ayrıca Azerbaycan ve Ermenistan gibi bazı devletler de SİDAS'a taraf olmuşlardır.[102] SİDAS'a taraf olan devletler, sözleşmede belirlenen hüküm ve koşullar doğrultusunda, talepte bulunan devletin yetkili mercileri tarafından yürütülen yargılama süreci kapsamında ya da mahkûmiyet kararı ve emniyet tedbirlerinin uygulanması amacıyla istenen kişilerin iadesini karşılıklı olarak üstlenmektedir. Bu çerçevede, SİDAS aracılığıyla iade yükümlülüğünün, genel olarak milletlerarası bir sorumluluk niteliği taşıdığı ifade edilebilir.[103]

Cezai Konularda Uluslararası Adli iş Birliği Kanununda, her ülkenin iç mevzuatlarında, ülke içerisinde bulunan suçluların bir diğer ülkeye iadesi prosedürüne ilişkin düzenlemeler yer almaktadır. Hukukumuzda, suçluların iadesi prosedürü, 6706 sayılı Cezai Konularda Uluslararası Adli İş birliği Kanunu'nun 10 ila 22'nci maddelerinde düzenlenmiştir.[104] 6706 sayılı Kanun'da ister Türkiye'den ister Türkiye'ye yapılan iade taleplerinde, iade talebine konu olan fiilin yalnızca talepte bulunan devletin kanunlarında değil, aynı zamanda "Türk kanunlarına göre" de suç teşkil etmesi gerekmektedir. Geri verme hukukunda aranan bu temel şart, SİDAS'ta da öngörülen ve 1 yıl ile 4 aylık süreler gibi belirli zaman sınırlamalarıyla da desteklenmektedir.

Koşullarına bakıldığında, eyleme ilişkin koşullarda; eylem her iki devlet yasasına göre, suç sayılmalı ve yaptırım belirli bir ağırlıkta olmalıdır.[105] Avrupa Sözleşmesinin 7. maddesinde yer alan bu koşul, kendisinden talepte bulunulan devletin ülkesinde veya ülkesi sayılan bir yerde işlenen suçlardan dolayı faili geri vermeyebileceği anlamını taşımaktadır.

---

[101] Ahmet Ulutaş, **Avrupa İnsan Hakları Sözleşmesi Işığında Suçluların Geri Verilmesi**, Ankara: Türkiye Barolar Birliği Yayınları, 2012, s. 62.
[102] İçel, **a.g.e.,** s. 182.
[103] Gülin Güngör, "Suçluların İadesine Dair Avrupa Sözleşmesi (SİDAS)", **Milletlerarası Hukuk ve Milletlerarası Özel Hukuk Bülteni**, C.19, S.1-2, 1999, s. 361.
[104] Yaşar ve İçer, **a.g.m.,** s. 1490.
[105] Özgenç, **a.g.e.,** s. 1128.

Suç zamanaşımına veya affa uğramamış olmalıdır. Bu koşulun kabul edilmiş olmasının sebebi fiil, zamanaşımı ya da affa uğramış ise, artık devletin suç ve suçlu ile ilişkisini kesmiş olması anlamına gelmektedir.[106] Zamanaşımını bakımından göz önünde bulundurulacak husus sadece süreler olmamalıdır; zamanaşımını kesen ve durduran sebeplerde göz önünde bulundurulmalıdır.[107] Zamanaşımı ve af, dava ve ceza ilişkisini düşüren sebeplerdendir. Madde sadece zamanaşımından bahsedildiğinden, bunu dava ve ceza zamanaşımını kapsar şekilde düşünmek gerekmektedir. Af, genel affı kapsadığı gibi cezayı tamamen ortadan kaldıran bir özellik arz etmesi halinde özel affı da kapsar.[108] Geri verme talebinin konusu olan yargılanacak suç hakkında kesinleşmiş hüküm bulunmamalıdır. Avrupa Sözleşmesinin "non bis in idem" başlığını taşıyan 9. maddesi gereğince, yargılamak için geri verilmesi istenen kişi ile ilgili daha önce kesin hüküm niteliği taşıyan yargısal bir kararın bulunması durumunda geri verme talebi kabul edilmez.[109]

Suçun düşünce suçu veya siyasal suç ya da askeri suç niteliğinde olmaması gerekir. 6706 sayılı kanun 11/1-c/1 maddesi düşünce suçunu da geri verilmeyecek suçlar arasında göstermiştir. Bunun dışında geri verme sözleşmelerinde siyasal suçların geri verme engeli olarak öngörülmesine rağmen düşünce suçuna yer verilmemiştir. [110] Düşünce, ceza hukuku anlamında bir hareket olarak kabul edilemeyeceği için suç sayılarak cezalandırılmaz. Düşünce dünyaya yansımadığı ve bir suç tipinde düzenlenmiş olmadığı sürece cezalandırılamaz.[111]

Siyasal suçların tespitinde doktrin, genellikle objektif ve sübjektif teoriler arasında ayrım yapmaktadır. Ayrıca, siyasal suçlar tam siyasal suçlar ve nispi siyasal suçlar olmak üzere iki ana kategoriye ayrılmaktadır. Geri verme hukukunda, geri verilmemesi gereken suçlar arasında en çok siyasal suçlar öne çıkmaktadır. Ancak, hangi suçların siyasal suç olarak nitelendirileceğine ilişkin yasalar ve milletlerarası antlaşmalarda net tanımlamalar bulunmamaktadır; bu durum uygulamada da somut

[106] Özbek vd., **a.g.e.,** s. 157.
[107] Özgenç, **a.g.e.,** s. 1131.
[108] Mahmut Koca ve İlhan Üzülmez, **Türk Ceza Hukuku Genel Hükümler**, 14. b, Ankara: Seçkin Yayınevi, 2021, s. 848.
[109] İçel, **a.g.e.,** s. 190.
[110] İçel, **a.g.e.,** s. 191.
[111] Özbek vd., **a.g.e.,** s. 160.

olaylara bağlı olarak farklı değerlendirmelere yol açmaktadır.[112] Maddi ceza hukuku bağlamında "siyasal suç" kavramı yer almamakta olup, bu kavrama ilişkin evrensel ve kesin bir tanım henüz oluşturulamamıştır.[113] Siyasal suç kapsamında görülmeyen eylemler şöyledir; devlet başkanlarına yönelik suçlar buna örnek verilebilir (Sözleşme m.3/3). Belçika kuralı olarak da adlandırılan bu kural devlet başkanının görevde olduğu sırada kendisi veya yakınlarına yönelen kasten öldürme ve yaralama suçlarını kapsamaktadır.[114] Terör eylemeleri; siyasal suçların geri verilmezliği kuralına getirilen diğer sınırlamadır. Şiddetin araç olarak kullanıldığı terör eylemlerinin, toplumda sürekli baskı, korku, yılgınlık yaratarak siyasal saydıkları amaçlarına ulaşmak istemektedir.[115]

[112] İçel, **a.g.e.,** s. 192.
[113] Özgenç, **a.g.e.,** s. 1136.
[114] Özbek vd., **a.g.e.,** s. 161.
[115] İçel, **a.g.e.,** s. 194.

ÜÇÜNCÜ BÖLÜM

3.MİLLETLERARASI HUKUK ÇERÇEVESİNDE SİBER EGEMENLİK VE İLGİLİ ÇALIŞMALAR

Milletlerarası hukukun evrensel ölçekte kabul görmüş tek bir tanımı bulunmamaktadır. Bu durum, farklı yazarların tanımlarında çeşitli yaklaşımların benimsenmesine yol açmaktadır. Zira her yazarın milletlerarası hukuku tanımlama biçimi, onun genel hukuk anlayışı ile doğrudan ilişkilidir. Özellikle, bu hukuk dalının süjeleri konusundaki farklı görüşler, yapılan tanımlar üzerinde belirleyici bir etkiye sahiptir.[116] Milletlerarası hukukun zaman içerisinde gelişim göstermesi ve bu sürecin doğal bir uzantısı olarak küresel ölçekte yaygınlaşmasıyla birlikte, devletler arasında kabul gören "ortak hukuk normlarının" sayısında da paralel bir artış gözlemlenmektedir. Bu gelişimde en temel rolü oynayan unsurların başında ise, milletlerarası antlaşmalar yer almaktadır. Çünkü antlaşmalar, sadece devletlerarası iş birliğini teşvik etmekle kalmamakta, aynı zamanda milletlerarası ilişkilerde uygulanacak genel ilke ve kuralların çerçevesini de belirleyici niteliktedir.[117]

Son yirmi yıl içerisinde, klasik milletlerarası hukuk anlayışında merkezi bir yer tutan hukuk ile siyaset ayrımına karşı çıkan bazı yaklaşımlar gelişmiş olsa da milletlerarası hukukun bir hukuk düzeni olduğu gerçeği değişmemektedir. Çünkü milletlerarası hukuk, bir hukuk düzenine özgü temel unsurları bünyesinde barındırmaktadır. Genel olarak bir hukuk düzeni, iki temel niteliğe sahiptir: ilki, uyulması zorunlu normlardan oluşan bir sistem ortaya koyması; ikincisi ise, bu normların uygulanmasını sağlayan örgütlü bir toplumsal yapının varlığıdır. Bu çerçevede değerlendirildiğinde, milletlerarası hukukta, iç hukuk sistemlerinde olduğu gibi, bağlayıcılığı olan kurallar bütünü meydana getirmektedir. Bu bağlayıcılığın iki temel dayanağı bulunmaktadır. İlk olarak, hukuk kurallarını oluşturma yetkisiyle donatılmış bir toplumsal otoritenin varlığı söz konusudur. İkinci olarak ise, oluşturulan düzenin bir

[116] Çelebi, **a.g.e.,** s. 11.
[117] Akıl, **a.g.e.,** s. 213.

hukuk düzeni olarak kabul edilmesi için, bu kurallara uyma gerekliliğinin genel anlamda kabul görmesi gerekir. İlk koşul bağlamında, milletlerarası hukuk kurallarını ortaya koyan otoritenin esas itibarıyla devletler ve sınırlı ölçüde milletlerarası örgütler olduğu görülmektedir. Her ne kadar ulusal hukuk sistemlerinde olduğu gibi tek bir yasama organı bulunmasa da kuralların çok taraflı şekilde belirlenmesi yalnızca örgütlenme biçiminden kaynaklanan bir farklılıktır. Bu durum, milletlerarası hukukun normatif bir otoriteden yoksun olduğu anlamına gelmemektedir. İkinci koşul açısından ise, milletlerarası hukuk normlarının bağlayıcı olduğu, bu kurallara tabi olan devletler ve diğer milletlerarası aktörler tarafından genel olarak kabul edilmektedir. Bu durum, söz konusu normların yaptırım gücünü devletlerin kendi rızalarına dayandırmakta ve milletlerarası hukuk kurallarının geçerliliğini bu kabul üzerinden inşa etmektedir. Dolayısıyla, milletlerarası hukukta iç hukukta olduğu gibi merkezi bir yaptırım otoritesinin bulunmaması, onun hukuk düzeni niteliğini ortadan kaldırmamaktadır. Aksine, bu durum, kuralların bağlayıcılığının devletlerin rızasına dayalı olarak şekillendiğini göstermektedir.[118]

Uzun yıllar boyunca, milletlerarası toplumun temel ve hatta tek hukuki süjesi olarak yalnızca devletlerin kabul edildiği bir anlayış hâkim olmuştur. Ancak günümüzde, devlet dışındaki aktörlerin de milletlerarası hukuk süjesi olarak ortaya çıktığı gerçeği yadsınamaz hale gelmiştir. Bu değişim, özellikle BM'nin yapısı ve işlevleri ile devletlerle olan etkileşimi göz önünde bulundurulduğunda daha açık biçimde anlaşılmaktadır. Klasik milletlerarası hukuk anlayışı, esas olarak devletler arası diplomatik ilişkiler ile savaş durumlarını düzenleyen normatif bir çerçeve sunmaktaydı. Ancak günümüzde bu geleneksel yaklaşım geçerliliğini büyük ölçüde yitirmiştir. Devletlerin sayısındaki artış ve devlet destekli milletlerarası örgütlerin çoğalması, milletlerarası hukuk kavramının hem kapsamını hem de işlevini nitelik ve nicelik açısından dönüştürmüştür. Buna ek olarak, teknolojik gelişmelerin de etkisiyle toplumlar ve hukuk sistemleri arasındaki etkileşim artmış; bilgi, iletişim ve iş birliği olanaklarının genişlemesi, milletlerarası hukukun yalnızca savaş ve barış zamanlarına özgü ilişkileri düzenleyen bir hukuk alanı olarak tanımlanmasını yetersiz hale getirmiştir. Bu bağlamda, 20. yüzyıl boyunca yaşanan yapısal ve kavramsal değişimler, milletlerarası hukukun

[118] Pazarcı, Uluslararası…, 2021, **a.g.e.,** s. 6-7.

yeniden tanımlanması ihtiyacını doğurmuş ve bu ihtiyaç günümüze kadar süregelen bir dönüşüm sürecine işaret etmiştir.[119]

Martha Finnemore ve Kathryn Sikkink tarafından geliştirilen ve literatürde geniş kabul gören "normların yaşam döngüsü" modeli, milletlerarası normların kurumsallaşma sürecini üç aşamada ele almaktadır. Bu sürecin ilk aşamasında, "norm girişimcileri" ya da diğer adıyla "öncü aktörler" belirleyici bir rol üstlenir. Söz konusu aktörler, örgütsel yapılardan destek alarak ve sosyalleştirme, itibara dayalı referanslar, teknik danışmanlık, eğitim faaliyetleri, kapasite geliştirme, norm tanımlama ve ayıplama gibi çeşitli stratejiler aracılığıyla normun benimsenmesini teşvik ederler. Bu noktada, norm girişimcilerinin faaliyet gösterdiği kurumsal platformların bilgiye, uzmanlığa ve kaynaklara erişim kapasitesi, normun kabul görmesinde önemli bir etki yaratır. Girişimciler, yeterli sayıda devleti bu yeni normu kabul etmeye ikna ettiklerinde, norm yaşam döngüsünde kritik bir eşiği aşarak daha geniş bir alana yayılmaya başlar. İkinci aşamada, yani normların "yaygınlaşma" sürecinde, devletler bu normları; milletlerarası toplumda meşruiyet kazanma, siyasal kimliklerini pekiştirme, itibar elde etme ve milletlerarası sistemin parçası olma yönündeki motivasyonlarla benimserler. Bu doğrultuda, benimsenen normlar, devletlerin milletlerarası kimliğini biçimlendirme ve hangi küresel topluluk içerisinde yer aldıklarını belirleme açısından işlevseldir. Son aşamada ise, normlar geniş ölçüde içselleştirilerek evrensel bir niteliğe bürünür. Bu evrenselleşme; öğrenme, sosyalleşme, müzakere, ikna ve sosyal baskı gibi süreçlerle gerçekleşir. Milletlerarası normlar zamanla hukuki bağlayıcılık kazanabilirken, yasal bir statüye kavuşmasalar dahi özellikle hukukun üstünlüğünün güçlü olduğu sistemlerde aktörlerin davranış biçimlerini, tercihlerine yön veren normatif çerçeveler oluşturabilir. Buna karşın, yeterli düzeyde benimsenmeyen ya da paydaşlar arasında ortaklaşa kabul görmeyen normlar, yasallaşmış olsalar bile etkili olamayabilir.[120]

Milletlerarası hukuk, esas itibarıyla milletlerarası toplumun hukuki zeminini oluşturmaktadır. Ancak bu noktada temel mesele, milletlerarası toplumun hangi aktörler veya birimler temelinde tanımlanması gerektiğidir. Bir başka ifadeyle, "milletlerarası toplum" kavramı yalnızca devletlerden oluşan bir yapıyı mı ifade etmektedir, yoksa bu

[119] Bozkurt, Poyraz ve Erdal, **a.g.e.,** s. 8.
[120] Tuba Eldem, "Uluslararası Siber Güvenlik Normları ve Sorumlu Siber Egemenlik", **İstanbul Hukuk Mecmuası**, S.79, 2021, s. 356.

kavram devletlerin ötesine geçerek bireyleri ve insanlık bütününü kapsayan daha geniş bir yapıyı mı temsil etmektedir? Bu tartışmanın yanı sıra, milletlerarası toplumda gittikçe daha etkin hale gelen ve herhangi bir devletin iç hukuk sistemiyle doğrudan bağlantısı bulunmayan milletlerarası örgütlerin hukuki statüsünün nasıl ve nerede konumlandırılması gerektiği de ayrı bir hukuki mesele olarak karşımıza çıkmaktadır. Milletlerarası örgütlere dair kuralların, devlet merkezli geleneksel milletlerarası hukuk çerçevesine nasıl entegre edileceği sorusu, çağdaş milletlerarası hukuk tartışmalarının önemli bir parçasıdır. Öte yandan, belirli ölçüde siyasi ve kurumsal yapıya sahip olmakla birlikte henüz devlet olarak tanınmayan bazı toplulukların, örneğin vesayet altındaki halkların veya özerk bölgesel oluşumların, milletlerarası toplum içindeki hukuki konumları da belirsizlik arz eden alanlardan biridir. Bu tür aktörlerin milletlerarası hukuk içerisindeki yeri hem normatif hem de pratik düzeyde dikkatle ele alınması gereken bir meseledir.[121]

Milletlerarası hukukunun, milletlerarası toplumun üyeleri arasındaki ilişkileri düzenleyen bağımsız bir hukuk disiplini olduğu tarihi bir olgudur. Ancak bu hukuk dalının evrimine paralel olarak, milletlerarası toplumun kimlerden oluştuğu sorusu çeşitli kuramsal yaklaşımlar çerçevesinde farklı şekillerde yanıtlanmıştır. Bu çeşitlilik, milletlerarası hukuk tanımına dair farklı görüşlerin ortaya çıkmasına da zemin hazırlamıştır. Kimi hukukçular, milletlerarası toplumun yalnızca bağımsız ve egemen devletlerden oluştuğunu ve dolayısıyla milletlerarası hukukun yalnızca bu devletler arasındaki ilişkileri düzenleyen kurallar bütünü olduğunu savunmuşlardır. Bu yaklaşım, "geleneksel görüş" olarak adlandırılmakta ve devlet dışındaki aktörlerin hukuki süje olamayacağı tezine dayanmaktadır. Öte yandan, Leon Duguit ve Georges Scelle gibi bazı düşünürler ise, daha farklı bir perspektif benimseyerek, milletlerarası toplumun yalnızca bireylerden meydana geldiğini ileri sürmüşlerdir. Bu yaklaşıma göre, gerçek kişiler dışında hiçbir tüzel varlık, örneğin devletler, hukuki süje olarak kabul edilemez. 1920'li yıllarda yaygınlık kazanan bu düşünce, milletlerarası hukuku; farklı siyasal yapıların vatandaşları olan bireyler arasında gerçekleşen ilişkileri düzenleyen normatif bir sistem olarak tanımlar. Modern hukuk yaklaşımı ise, daha kapsayıcı bir bakış açısını benimseyerek, milletlerarası hukukun süjelerini yalnızca bağımsız devletlerle sınırlı tutmamaktadır. Bu güncel anlayışa göre; tam egemenliğe sahip devletlerin yanı sıra,

[121] Pazarcı, Uluslararası…, 2021, **a.g.e.,** s. 4.

milletlerarası örgütler, kısmi yetkilere sahip devlet benzeri yapılar, sui generis statüye sahip topluluklar ile belirli koşullarda gerçek kişiler de milletlerarası hukukun süjeleri arasında yer alır. Tüm bu değerlendirmelerin ışığında, milletlerarası hukuku; devletlerin ve diğer milletlerarası hukuk süjelerinin karşılıklı ilişkilerini düzenleyen kurallar bütünü olarak tanımlamak mümkündür. Bu tanım hem klasik hem de çağdaş yaklaşımları dikkate alarak disiplinin kapsamını daha geniş bir zemine oturtmaktadır.[122]

Avrupa merkezli olarak geliştirilen bu hukuk sisteminin hangi terimle ifade edilmesi gerektiği, tarihsel süreçte tartışma konusu olmuştur. Türkçede "milletlerarası hukuk" kavramının karşılığı olarak kullanılan terimlerin seçimi ise, hem dönemin hukuk anlayışına hem de dil kullanımındaki eğilimlere göre, değişiklik göstermiştir. Bu bağlamda, Türkçedeki ilk çalışmalardan biri olan Baron Schlechta Ottokar'ın 1847 yılında Viyana'da yayımlanan eserinde, Almanca "Völkerrecht" kavramının karşılığı olarak "Hukuk-u Milel" terimini tercih ettiği görülmektedir. Bu ifade, "uluslar hukuku" anlamına gelmekte ve dönemin Osmanlıca dil yapısına uygun düşmektedir. Daha sonraki dönemlerde ise, farklı yazarlar, "Devletler hukuku" anlamını taşıyan "Hukuk-u Düvel" ifadesini tercih etmişlerdir. Bu terminolojik farklılık, yalnızca çeviri tercihlerinden değil, aynı zamanda milletlerarası hukukun süjesi olarak devletlerin mi, yoksa ulusların mı esas alındığı yönündeki teorik tartışmalardan da beslenmiştir.[123]

Milletlerarası hukukunun aşamalı gelişimine ilişkin olarak, evrensel nitelikli milletlerarası örgütlerin çalışmalarından önce, akademisyenler ve bilimsel kuruluşlar tarafından yapılan araştırmalar dikkat çekmektedir. Milletlerarası hukukunun kodifikasyonu fikri, ilk kez 18. yüzyılın sonlarında gündeme gelmiş; 19. yüzyıl sürecinde bazı hukukçular, milletlerarası hukuka ilişkin kuralları maddeler halinde sistematik olarak derleyen eserler kaleme almıştır. Çok taraflı antlaşmalar yoluyla gerçekleştirilen kodifikasyonun ilk örnekleri, 1899 ve 1907 yıllarında Lahey'de düzenlenen konferanslarda imzalanan antlaşmalar olarak ortaya çıkmıştır. Bu belgeler, uyuşmazlıkların barışçıl yollarla çözümüne ilişkin prosedürlerin yanı sıra kara savaşları ve deniz savaşlarına dair kurallar gibi önemli hususları düzenlemiştir. Milletler Cemiyeti döneminde ise, bu konuda doğrudan bir kodifikasyon hükmü bulunmamakla birlikte, 22 Eylül 1924 tarihinde, kodifikasyon için uygun sorunları belirlemek amacıyla on yedi

[122] Bozkurt, Poyraz ve Erdal, **a.g.e.,** s. 7-8.
[123] Pazarcı, Uluslararası…, 2021, **a.g.e.,** s. 5.

uzmandan oluşan bir komite kurulmuştur. Söz konusu komite, özellikle tabiiyet, karasuları ve yabancılara karşı işlenen suçlardan devletin sorumluluğu gibi alanları kodifikasyon kapsamına almıştır. BM ise, önceki kodifikasyon girişimlerinin başarısızlıklarını dikkate alarak, Genel Kurul aracılığıyla milletlerarası hukukun gelişimi ve kodifikasyonunu teşvik etme görevini üstlenmiştir. Bu bağlamda, BM Genel Kurulu 11 Aralık 1946'da milletlerarası hukukun gelişimi ve kodifikasyon çalışmalarının alanında uzman bir grup tarafından yürütülmesini önererek bu süreci başlatmıştır. Takip eden süreçte, 21 Kasım 1947'de BM Genel Kurulu bünyesinde, "Devletler Hukuku Komisyonu" adıyla bir alt kurul oluşturulmuştur. Söz konusu komisyon, kuruluşundan itibaren çok sayıda konuyu ele almış ve pek çok konuda milletlerarası antlaşmanın hazırlanmasına önemli katkılar sağlamıştır. [124]

"Kaynak" terimi, genel anlamıyla bir olgunun ya da varlığın başlangıç noktası, doğduğu veya ortaya çıktığı yeri ifade eder.[125] Hukuk sistemlerinde ise, bu kavram, o düzen içerisindeki hukuk normlarını oluşturan ve geliştiren unsurları tanımlamak amacıyla kullanılmaktadır. [126] Hukukta "kaynak" kavramı farklı anlamlarda kullanılmakta olup, bu nedenle maddi kaynak ve şekli kaynak ayrımı yapılmaktadır. Hukukun maddi kaynağı, hukuk düzeninin temelini oluşturan tarihi, sosyolojik, felsefi ve ahlaki unsurları ifade eder. Örneğin, milletlerarası hukukun dayanaklarını inceleyen gerçekçi yaklaşımı benimseyenler için maddi kaynak, toplumsal olaylar ve sosyal dayanışma olarak görülmektedir. Öte yandan, milletlerarası hukukta şekli kaynakların kapsamı konusunda öğreti içinde tam bir görüş birliği bulunmamaktadır. Bu bağlamda en önemli düzenleme, Milletlerarası Adalet Divanı Statüsü'nün 38. maddesidir. Söz konusu maddenin birinci paragrafında, kaynaklar; a- antlaşmalar, b- teamüller, c- genel hukuk ilkeleri, d- mahkeme kararları ile doktrin olarak sıralanmıştır. İkinci paragraf ise, Divan'ın hak ve adalete uygun karar verme yetkisini düzenlemektedir. Ancak, Statü'nün bu maddesi hem kaynakların sıralanışı hem de kapsamı açısından çeşitli eleştirilere maruz kalmıştır. Ayrıca, daha önce de belirtildiği gibi, yazarlar şekli kaynakların sayısı ve niteliği konusunda farklı görüşler ortaya koymaktadır.[127]

[124] Bozkurt, Poyraz ve Erdal, **a.g.e.,** s. 23-26.
[125] Bozkurt, Poyraz ve Erdal, **a.g.e.,** s. 43-45.
[126] Pazarcı, Uluslararası…, 2021, **a.g.e.,** s. 38.
[127] Çelebi, **a.g.e.,** s. 85-86.

Milletlerarası düzeyde merkezi bir yasama organının bulunmaması nedeniyle, norm oluşturma işlevi doğrudan doğruya milletlerarası hukuk süjesi olan aktörler tarafından yerine getirilmektedir. Bu bağlamda, milletlerarası hukukta normatif düzenlemeler çoğunlukla taraflar arasında akdedilen antlaşmalar yoluyla gerçekleştirilmektedir. Milletlerarası antlaşmalar, milletlerarası hukukun tanıdığı süjeler arasında hukuki bağlayıcılığı bulunan ilişkiler kurmak, mevcut bir hukukî durumu değiştirmek veya sona erdirmek amacıyla yapılan irade beyanlarıdır. Bu tür belgeler, taraflar arasında doğrudan hak ve yükümlülük doğuran işlemler olup, yazılı biçimde düzenlenmeleri yaygın bir uygulamadır. Milletlerarası hukukta taraflar arasında imzalanan yazılı belgeler çeşitli adlarla anılmaktadır. Bunlar arasında en yaygın kullanılan terimler şunlardır: "antlaşma", "sözleşme", "protokol", "senet", "genel senet", "nihai senet", "misak", "şart", "modus vivendi" (özellikle ticaret alanında geçici nitelikte kısa süreli düzenlemeler için kullanılır), "statü", "tüzük", "tahkimname" (milletlerarası bir uyuşmazlığın yargısal bir mercie sunulmasına dair anlaşma), "konkorda" (dini içerikli meselelerde papalık tarafından akdedilen anlaşmalar) ve "mektup değişimi" (devletler arası mutabakatın karşılıklı yazışmalar yoluyla sağlandığı durumlar). Bu çeşitlilik, antlaşmaların içerik, kapsam ve hukuki etki bakımından farklı biçimlerde yapılandırılabileceğini göstermektedir. Ayrıca, bu belgeler milletlerarası ilişkilerin dinamik yapısı içerisinde hukuki güvenlik ve öngörülebilirliği sağlamak adına temel rol oynamaktadır.[128]

3.1.Siber Egemenlik Kavramının Ortaya Çıkışı ve Tanımı

Egemenlik kavramı, özellikle 20. yüzyılda hız kazanan teknolojik ilerlemelerle birlikte dönüşüme uğramış ve kendisini yeni toplumsal, siyasal ve teknolojik koşullara uyarlama çabasına girmiştir. Bu süreçte, ulus-devlet yapısının meşruiyeti ve sürdürülebilirliği üzerine yürütülen tartışmaların yoğunluk kazanması, egemenlik anlayışının da yeniden değerlendirilmesini beraberinde getirmiştir. Bu bağlamda, geleneksel egemenlik tanımları yetersiz kalmaya başlamış ve farklı bağlamlarda yeni egemenlik türleri ortaya çıkmıştır. Bu yeni egemenlik türlerinden biri de dijitalleşme ve küresel teknolojik etkileşimlerin bir sonucu olarak gündeme gelen "siber egemenlik" kavramıdır. Bu kavram, devletlerin dijital alan üzerindeki denetim ve kontrol yetkilerini,

[128] Çelebi, **a.g.e.,** s. 125-127.

bilgi akışını düzenleme gücünü ve ulusal güvenlik stratejilerini yeniden tanımlama ihtiyacını yansıtmaktadır.[129]

Milletlerarası hukukta devletlerin egemenlik haklarının bir sonucu olarak bazı temel ilkeler kabul edilmiştir. Bu ilkeler arasında en öne çıkanlar: 1- egemen eşitlik ilkesi, 2- devletlerin içişlerine müdahale etmeme ilkesi ve 3- doğal kaynaklar üzerinde sürekli egemenlik ilkesidir. Egemen Eşitlik İlkesi, devletlerin eşit egemen yapılar olması, milletlerarası hukukta tüm devletlerin hukuki açıdan aynı statüye sahip olması anlamına gelir. Bu eşitlik, her devletin aynı hak ve yükümlülüklere sahip olduğu ilkesine dayanır. Başka bir deyişle, gönüllü olarak kabul edilen istisnalar dışında, tüm devletler eşit hukuki konuma sahiptir. BM Antlaşması'nın 2. maddesinin 1. fıkrası bu ilkeyi açıkça desteklemektedir. Egemen eşitlik yalnızca hukuki bir norm değil, aynı zamanda milletlerarası ilişkilerde devletler arasında denge ve karşılıklı saygının temelidir. Devletlerin egemenliğinden türeyen bir diğer temel ilkede, diğer devletlerin iç işlerine müdahale etmeme yükümlülüğüdür. Bu ilke, ilk kez BM Genel Kurulu'nun 21 Aralık 1965 tarihli ve 2131 (XX) sayılı kararıyla sistematik bir şekilde kabul edilmiştir. Doğal kaynaklar üzerinde sürekli egemenlik ilkesi, egemenliğin ve halkların kendi kaderini tayin hakkının bir uzantısı olarak, özellikle sömürgecilikten kurtulan devletlerin katkısıyla, doğal kaynaklar üzerinde ekonomik egemenlik hakkı milletlerarası hukukta özel bir ilke olarak kabul edilmiştir.[130]

Milletlerarası hukuk bağlamında devletin yetkileri geniş bir perspektiften ele alındığında; ikili veya çok taraflı antlaşmalar dâhil olmak üzere tüm hukuki işlemleri, tek taraflı tasarrufları, hukuka uygun kararları ve eylemleri bu yetkinin kapsamına girmektedir. Ancak uygulamadaki milletlerarası hukuk anlayışı, devletin milletlerarası hukuk kurallarını yaratma ve devletler arası ilişkileri düzenleme yetkisini, teknik anlamda "yetki" kavramının dışında değerlendirmektedir. Bu nedenle, "devlet yetkisi" terimi dar ve teknik anlamıyla ele alındığında, devletin milletlerarası hukuka uygun biçimde gerçekleştirdiği işlemlerin, kararların ve faaliyetlerin hangi coğrafi sınırlar içerisinde, kimler üzerinde ve ne ölçüde geçerli olduğunun belirlenmesi anlamına gelmektedir. Devletin kurucu unsurlarından biri olan egemenlik hakkının incelenmesi sırasında da belirtildiği üzere, devletin kendi toprakları üzerinde temel ilke olarak münhasır bir

[129] Kıllıoğlu, **a.g.e.,** s. 133-134.
[130] Pazarcı, Uluslararası…, 2021, **a.g.e.,** s.154-156.

egemenlik yetkisi bulunmaktadır. Bu egemenlik, devlete ülkesel alanda yasama, yürütme ve yargı faaliyetlerini yürütme konusunda geniş kapsamlı yetkiler tanımaktadır. Başka bir ifadeyle, devletin ülkesel egemenliği, bu sınırlar içinde her türlü kamu gücü kullanımını mümkün kılmaktadır. Böylece, devletin ülkesel yetkileri yalnızca coğrafi değil, aynı zamanda kişisel ve maddi anlamda da geniş bir kapsama sahiptir.[131]

Alman hukukçu Carl Schmitt, "Nomos" kavramını modern siyaset teorisine kazandıran önemli isimlerden biridir. Bu terim, Antik Yunan'da hem yasa ve gelenek anlamında hem de idari-bölgesel bir yapılanmayı ifade eden "nome" yapılarıyla ilişkilendirilerek kullanılmıştır. Schmitt, bu kavramı belirli bir mekânın hukuki ve siyasal organizasyonunu tanımlamak amacıyla yeniden yorumlamıştır. Geleneksel anlamda egemenlik; kara, deniz ve hava sahaları gibi fiziksel sınırlara dayanmakla birlikte, teknolojinin baş döndürücü bir hızla gelişmesiyle birlikte bu anlayış dönüşüme uğramış ve siber uzay gibi fiziksel olmayan alanlar da egemenlik tartışmalarının konusu haline gelmiştir. Siber uzay, insan eliyle yaratılmış bir ortam olup, yapısı itibarıyla dinamik, değişken ve fiziksel sınırlardan yoksundur. Bu özellikleriyle klasik egemenlik tanımlarının dışında konumlanmakta, fakat tam da bu nedenlerle özgün bir inceleme alanı sunmaktadır. Siber alandaki egemenlik tartışmaları bağlamında, özellikle devletlerin bu yeni alanda yetki iddia etme girişimleri dikkat çekicidir. Her ne kadar siber uzayın teknik altyapısı, örneğin internet protokolleri ve sunucu sistemleri, üzerinden belirli kontrol mekanizmaları tanımlanabilir olsa da bu alanı doğrudan düzenleyen ve devletler arası uzlaşıya dayanan genel kabul görmüş bir milletlerarası hukuk normlar sistemi henüz oluşturulamamıştır. Bu durum, internetin ve siber ortamın mevcut hukuki statüsünü ve bu bağlamda yaşanan çatışmaları, belirsizlikleri ve egemenlik taleplerini anlamak açısından oldukça önemlidir.[132]

3.1.1. Milletlerarası Hukukta Siber Egemenlik

Milletlerarası hukuk bağlamında devletin ülkesel sınırları, devlet yetkilerinin kapsam ve sınırlarının belirlenmesinde temel bir referans noktasıdır. Bu kapsamda, milletlerarası hukuk düzeni, bir devletin yer ve kişi bakımından yetkisini belirlerken iki temel ilkeye dayanır. İlk ilke olan milletlerarası hukukun açıkça izin verdiği bir durum

[131] Pazarcı, Uluslararası…, 2021, **a.g.e.,** s.156-157.
[132] Kıllıoğlu, **a.g.e.,** s.143.

bulunmadıkça, bir devletin kendi ülke sınırları dışında yetki kullanması mümkün değildir. Bu prensip "yetkinin ülkeselliği" ilkesi olarak adlandırılır ve devlet yetkisinin coğrafi sınırlarını ifade eder. Bu ilke, Milletlerarası Daimî Adalet Divanı tarafından 1927 yılında karara bağlanan Lotus davası çerçevesinde açıklığa kavuşturulmuştur. Türkiye ile Fransa arasında geçen bu davada, 2 Ağustos 1926 gecesi Fransız gemisi Lotus ile Türk gemisi Bozkurt Midilli açıklarında çarpışmış ve Türk gemisi batmış, sekiz mürettebat hayatını kaybetmiştir. Olayın ardından Lotus İstanbul'a ulaştığında, Türk yetkililer olaya müdahale etmiş, gemi kaptanı Hasan Bey ile Fransız subayı Demons tutuklanmış ve haklarında yargı süreci başlatılmıştır. Fransa, Türkiye'nin açık denizde bir Fransız vatandaşına yönelik cezai işlem uygulamasının milletlerarası hukuka aykırı olduğunu ileri sürerek, Türkiye'nin bu yetkiyi ancak milletlerarası hukukun açıkça tanıdığı bir hükme dayanarak kullanabileceğini iddia etmiştir. Türkiye ise, Lozan Antlaşması'nın 15. maddesine atıfla, herhangi bir milletlerarası hukuk kuralına aykırılık olmadığı sürece milli yetkinin kullanılabileceğini savunmuştur. Divan, değerlendirmesinde Fransa'nın yaklaşımını reddetmiş ve şu temel gerekçeyi ortaya koymuştur. Milletlerarası hukukun devletlerin yetkileri üzerindeki en temel sınırlaması, aksi yönde açık bir izin olmadıkça, bir devletin kendi yetkilerini başka bir devletin topraklarında kullanamamasıdır. Bu bağlamda yetki ilkesel olarak ülkeseldir. Ancak bu durum, bir devletin ülke dışında gerçekleşen olaylara ilişkin olarak, kendi topraklarında yargı yetkisi uygulamasını mutlak biçimde yasaklayan bir ilke değildir. Dolayısıyla, yetkinin ülkeselliği ilkesi, devletlerin mutlak surette ülke dışı kişi, mal veya fiiller üzerinde düzenleme yapamayacağı anlamına gelmez. Temel kural olarak bu düzenlemelerin doğrudan ülke dışında uygulanması mümkün olmasa da bu kişi ve unsurlar herhangi bir biçimde devletin ülkesine girdiğinde, devletin bu yetkileri uygulaması mümkündür.[133]

İkinci ilkeye bakıldığında, devlet yetkisinin niteliğine ilişkin ilke ise, devletin egemenliğine dayanan ikinci temel ilke olup devletin kendi toprakları içerisindeki yetkisinin içeriğini ve kapsamını tanımlar. Bu ilkeye göre, bir devlet, kendi ülkesinde meydana gelen her türlü olgu, olay, kişi ve eşya üzerinde münhasır yetkiye sahiptir. Bu yetki, başka bir devletin müdahalesine kapalıdır ve yalnızca söz konusu devlet tarafından kullanılabilir. Ancak milletlerarası hukuk bu ilkeye birtakım sınırlamalar getirmektedir. Bazı durumlarda devlet, topraklarında bulunan belirli kişiler ya da nesneler üzerinde

[133] Toluner, **a.g.e.,** s. 2-4.

yetkisini ya kısıtlı biçimde kullanmak zorunda kalmakta ya da bu yetkiyi tamamen kullanmaktan kaçınmakla yükümlü kılınmaktadır. Aynı şekilde, eğer milletlerarası bir hukuk normu açıkça öngörüyorsa, bir devletin sınırları içinde başka bir devletin sınırlı da olsa yetki kullanmasına da olanak tanınabilmektedir. Bu gibi istisnalar, devlet egemenliğinin mutlak olmadığını, belirli durumlarda milletlerarası hukuk tarafından şekillendirildiğini göstermektedir. Bu noktada şu hususun altı çizilmelidir. Milletlerarası hukuk tarafından getirilen her sınırlama, otomatik olarak o devletin ülkesinde başka bir devletin yetkili olduğu anlamına gelmez. Yani, bir devletin egemen yetkilerini kullanmasının tamamen engellenmesi ya da sadece belirli şekilde kullanmasının zorunlu tutulması, her zaman bu yetkinin başka bir devlete devredildiği ya da paylaşıldığı sonucunu doğurmaz. Öte yandan, bir devletin kendi yasalarının uygulama alanını veya yargı yetkisini ülke dışında gerçekleşen olaylara veya ülke dışındaki kişi ve eşyalara teşmil edebilmesi, bu yetkinin ancak ülke içinde fiilen uygulanabileceği koşulunu değiştirmediği sürece, bu tür durumlar da söz konusu ilkenin bir istisnası olarak değerlendirilemeyebilir. Dolayısıyla, devlet yetkilerinin sınırlarının belirlenmesinde, yalnızca teorik değil, uygulamaya yönelik boyutların da dikkate alınması gereklidir.[134]

Günümüzde milletlerarası hukukun zorunlu bir yargı sistemine sahip olmadığı bir gerçektir. Adalet Divanı gibi milletlerarası yargı organları ya da hakemlik mekanizmaları, devletlerin ya da diğer milletlerarası aktörlerin bu organlara başvurmasını genel anlamda zorunlu kılmamaktadır. Başka bir ifadeyle, söz konusu yargı veya hakemlik organlarına başvuru, tarafların rızasına bağlıdır. Bununla birlikte, milletlerarası alanda gözlemlendiği üzere, devletler aralarındaki uyuşmazlıkların çözümünde bu tür mekanizmalara giderek daha fazla başvurma eğilimi göstermektedir. Ayrıca, devletler önceden yaptıkları antlaşmalarla yetki tanıyarak, zorunlu yargılama veya hakemlik usullerini kurmak suretiyle, milletlerarası hukukun bu alandaki zayıflığını kısmen gidermeye çalışmaktadırlar. Öte yandan, milletlerarası hukuk genel anlamda zorunlu yargılama mekanizması tesis edememiş olsa da milletlerarası sorumluluk ilkeleri vasıtasıyla, hukuka aykırı her türlü eylemin ilgili milletlerarası aktörler tarafından ileri sürülmesini mümkün kılan bir sistem geliştirmekten de geri kalmamıştır. Milletlerarası hukukun, kurallara uymayan taraflara yaptırım uygulayacak merkezi bir yürütme organına sahip olmaması da bilinen bir durumdur. Ancak bu durum, milletlerarası hukukun her tür yaptırım

[134] Toluner, **a.g.e.,** s. 2-4.

mekanizmasından yoksun olduğu anlamına gelmemektedir. Zira milletlerarası hukuk, kendi içinde yaptırımları uygulama gücüne sahip olmamakla birlikte, bu eksikliği devletlerin kendi ulusal mekanizmaları aracılığıyla yaptırımları uygulaması öngörüsüyle telafi etmeye çalışmaktadır. Ayrıca, milletlerarası toplumun örgütlenme düzeyinin artmasıyla birlikte, devletlerin zaman zaman kolektif yaptırımlar uygulama imkânı da ortaya çıkmıştır. Nitekim, Milletler Cemiyeti ve sonrasında BM'nin kurulmasıyla, gerektiğinde zorlayıcı tedbirler ve hatta kuvvet kullanımı dahil olmak üzere ortak yaptırımlar öngörülmüş ve pratikte uygulanmıştır.[135]

Egemenlik kavramı, bir devletin ekonomik, askerî ya da teknolojik alanlarda tam anlamıyla bağımsız olmasını gerektirmez. Günümüz dünyasında devletler, pek çok alanda karşılıklı bağımlılık ilişkisi içerisindedir. Özellikle ekonomik düzlemde birçok devlet, başka devletlerle iş birliğine ve desteğe ihtiyaç duymakta; bu durum ise, zaman zaman ulusal politika üretiminde sınırlamalara yol açabilmektedir. Ancak bu tür bağımlılık ilişkileri, bir devletin egemenliğini ortadan kaldırmaz. Zira, söz konusu devlet, kendi ülkesinde yasa koyma, uygulama ve yürütme yetkisini tek başına elinde bulundurmaya devam etmektedir. Bununla birlikte, egemenliğin mutlak bir serbesti anlamına gelmediği de açıktır. Devletlerin milletlerarası hukuk çerçevesinde çeşitli yükümlülükler üstlenmesi ve bu bağlamda bazı hareket alanlarının daralması, egemenlik ilkesine aykırılık teşkil etmez. Başka bir ifadeyle, bir devletin milletlerarası hukuk normlarına bağlılık göstermesi, yasa yapıcı ve yürütücü otorite olma vasfını yitirmediği sürece, egemenliğine halel getirmez.[136]

3.1.2. Siber Uzay Kavramı

Bu tanımlamalar ışığında, günümüz siber uzayın tek bir bileşenden ibaret olmadığı; aksine, farklı sayısal etkileşim ve iletişim yöntemlerini barındıran, birbirine iç içe geçmiş çoklu alanlardan oluşan karmaşık bir yapı olduğu söylenebilir. Bu bağlamda, hızla değişen ve homojen olmayan küresel bir sistemin varlığı gündeme gelmektedir. Siber uzayda, internete bağlı bilgisayarlar fiziksel konumlarından bağımsız olarak, zaman ve mekân kısıtlaması olmaksızın anlık veri iletimi ve iletişim imkânına sahiptir. Öte

[135] Pazarcı, Uluslararası…, 2021, **a.g.e.,** s. 7-8.
[136] Akıl, **a.g.e.,** s. 270.

yandan, bilgisayar güvenliği kavramı, artık salt fiziksel bir mesele olmaktan çıkarak, siber uzayın kendine özgü dinamikleri çerçevesinde ele alınan kritik bir alan haline gelmiştir.[137]

Transmission control protocol (TCP) ve Internet protocol address (IP) protokolünün kökenleri, 1960'ların sonları ile 1970'lerin başlarında, Amerikan Savunma Bakanlığı'na bağlı İleri Araştırma Projeleri Ajansı'nın yürüttüğü paket anahtarlamalı ağ deneylerine dayanmaktadır. Bu protokolün geliştirilmesini mümkün kılan proje, ABD'deki bilgisayar sistemlerinin olası felaket durumlarında bile işlevselliğini korumasını ve aralarındaki iletişimin kesintisiz devam etmesini hedeflemiştir. Günümüzde değerlendirildiğinde, bu hedeflerin büyük ölçüde gerçekleştiği ve projenin beklenmedik birçok başarıya da imza attığı görülmektedir. TCP/IP'nin tarihçesi, aynı zamanda İnternet'in gelişim tarihini de kapsamaktadır; zira TCP/IP ve İnternet, birbirinden ayrılmaz bir bütün oluşturur. TCP/IP, internetin temel iletişim protokolü olarak işlev görmektedir. İnternetin sahipliğiyle ilgili olarak ise, bu ağın belirli bir sahibi bulunmamaktadır; herkes internetin kullanıcısı olmakla birlikte, hiçbir kurum veya birey internetin münhasır sahibi değildir. Buna rağmen, internet tamamen kontrolsüz değildir; TCP/IP protokolünü yöneten ve düzenleyen çeşitli gönüllü kuruluşlar mevcuttur.[138]

İnternet, ABD Savunma Bakanlığı bünyesindeki Gelişmiş Araştırma Projeleri Dairesi Ağı'nın sivil kullanıma açılmasıyla birlikte küresel gündemin önemli bir unsuru haline gelmiştir. 1990'lı yılların başında, telefon hatları aracılığıyla modemlerle sağlanan sınırlı internet erişimi, 21. yüzyılın başlarında büyük ölçüde artarak yüksek hızlı ve geniş çaplı bağlantı olanaklarına ulaşmıştır. Kişisel bilgisayarlar, mobil telefonlar ve dijital algılayıcılar gibi yeni nesil teknolojik araçların yaygınlaşması, ağ kapasitesinin büyümesine ve günümüzün dijital dünyasının şekillenmesine katkıda bulunmuştur. Bu gelişmeler aynı zamanda bilgi üretimi ve depolama kapasitesinde önemli artışlara olanak sağlamıştır.[139] Özellikle internet teknolojilerinin gelişimiyle birlikte, devlet sınırları belirginliğini büyük ölçüde yitirmeye başlamıştır. Benzer biçimde, uzay ve uydu teknolojilerindeki ilerlemeler de coğrafi sınırları aşarak, devletlerin egemenlik alanları

[137] Mehmet Eren, **Avrupa Birliği'nin Siber Güvenlik Politikası**, 1. b, İstanbul: Beta Basım, 2017, s. 20.
[138] Murat Yıldırım, **Her Yönüyle İnternetin Altyapısı TCP/IP Hızla Genişleyen ve Taşınmaya Hazırlanan IP Ağları İçin Tek Kapsamlı Kaynak**, 10. b, İstanbul: Pusula Yayıncılık, 2009, s. 2.
[139] Ekonomi ve Dış Politikalar Araştırma Merkezi, **Türkiye'de Siber Güvenlik ve Nükleer Enerji**, 1. b, İstanbul: Edam, 2016, s. 101.

içerisindeki doğal kaynaklar ve güvenlik altyapılarına ilişkin doğrudan bilgi edinilmesine olanak tanımıştır.[140]

"Bilgisayar" kavramı, kişisel bilgisayarlar (desktop veya laptop), mobil cihazlar (örneğin tabletler, akıllı telefonlar) gibi programlanabilir bilgi işlem ve iletişim cihazlarının yanı sıra, iletişim içinde bulundukları sunucular ve ağ donanımlarını da kapsamaktadır. Sunucular; web sitelerini barındıran ön uç sunucuları, veri tabanlarına ev sahipliği yapan arka uç sunucuları ile e-posta, metin mesajları, ses ve video içerikleri gibi bilgilerin depolanması veya iletimi amacıyla kullanılan ara düğümleri içermektedir. Ağ bileşenleri arasında ise, güvenlik duvarları, yönlendiriciler ve anahtarlar (switch) yer almaktadır. İncelenen temel unsurlar arasında, bu cihazlarda çalışan yazılımlar, aralarındaki iletişim protokolleri, kullanıcıların bu sistemlerle kurduğu etkileşim biçimleri ile kötü niyetli tarafların sistemleri kötüye kullanma potansiyeli bulunmaktadır.[141]

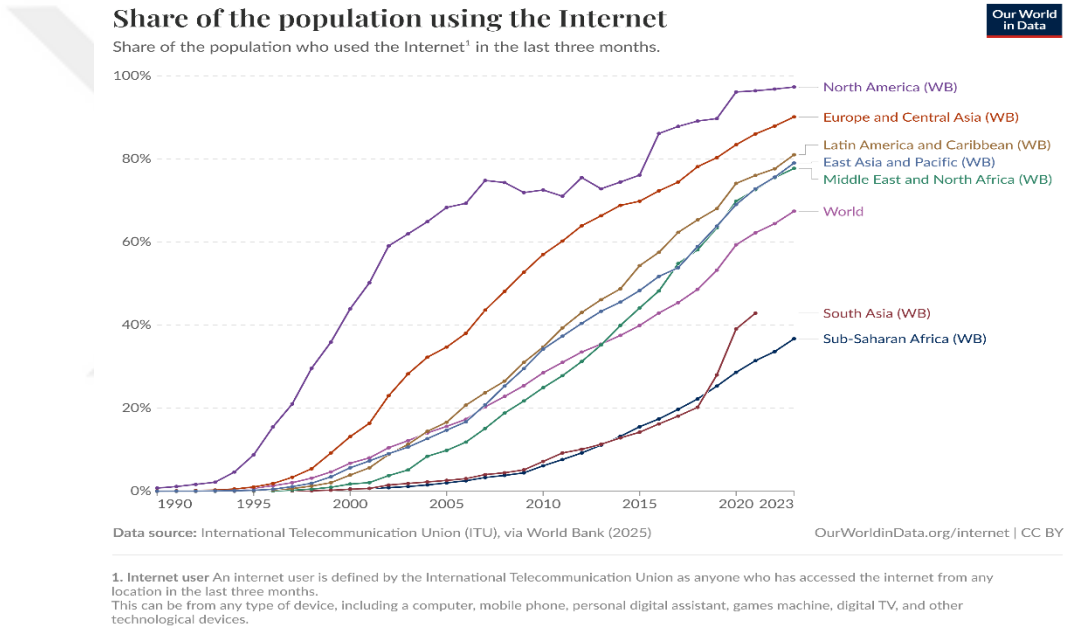
İnternetin ticari amaçlarla kullanılmaya başlandığı ilk dönemlerde, işletmeler uygulamaların güvenlik boyutlarına yeterince önem vermemiştir. Ancak zamanla, kaynaklarının kötü niyetli saldırganların saldırılarına karşı korunması gerekliliği ortaya çıkmış ve bu doğrultuda önlemler alma ihtiyacı doğmuştur. Bu kapsamda, çoğunlukla güvenlik duvarları gibi teknolojik çözümler tercih edilerek güvenlik ihtiyaçları karşılanmaya çalışılmıştır. Yeni teknolojilerin devreye girmesiyle birlikte benzer güvenlik riskleri ortaya çıkabilmekte, fakat edinilen deneyim sayesinde kullanıcılar ve kurumlar bu açıkları tespit edip gidermeye yönelik adımlar atmaktadır. Özellikle nispeten yeni sayılabilecek kablosuz ağ teknolojileri, kullanıcılar ve işletmeler açısından hâlâ bazı güvenlik zafiyetlerini barındırabilmektedir. Kablosuz erişim noktaları çeşitli güvenlik mekanizmaları içermekle birlikte, bu önlemler her zaman gerekli güvenlik düzeyini sağlamakta yetersiz kalabilmektedir.[142]

İnternetin sivil kullanıma açılmasıyla birlikte yaygınlaşması, iletişim olanaklarındaki ve kapasitesindeki önemli gelişmeler, küreselleşmenin etkisiyle günlük yaşam ve sosyal yapıda meydana gelen çeşitlilik, teknolojik yenilikler ve internet

[140] Akıl, **a.g.e.,** s. 28.
[141] Paul C. Van Oorschot, (Çev. Kemal Bıçakçı), **Siber Güvenliğe Giriş Bilgisayar Güvenliği ve İnternet Araçlar ve Mücevherler**, Ankara: Palme Yayınevi, 2002, s. 2.
[142] Can Okan Dirican, **Teori ve Uygulamalar ile TCP/IP ve Ağ Güvenliği**, 2. b, İstanbul: Açık Akademi Yayınları, Ağustos 2007, s. 473.

aracılığıyla yayılan zararlı yazılımların artışı, "siber uzay" ve "siber güvenlik" gibi yeni kavramların ortaya çıkmasına zemin hazırlamıştır. Ağ teknolojilerinin ticari, kültürel, askeri, siyasi ve finansal gibi kritik alanlarda kullanımı, küresel ölçekte hızlı bir şekilde yaygınlaşmıştır. Bu kadar önem taşımasına rağmen literatürde "siber uzay" kavramına ilişkin milletlerarası çapta kabul görmüş ortak bir tanım bulunmamaktadır.[143] İnternetin en önemli farklarından biri de diğer iletişim araçları gibi tek bir kişi, kurum ya da ülkenin tekelinde bulunmamasıdır. İnternet, bu teknolojiyi kullanan milyonlarca kişi, firma ve kuruluşun ortak sahipliğindedir.[144]

Şekil 1: Dünyada İnternet Kullanan Nüfusun Oranları (1990 ile 2023 arası)[145]



Yukarıdaki grafiğe bakıldığında, Kuzey Amerika nüfusunun; internetin kullanımının yaygınlaştığı tarih olan 1999 yılından itibaren dünyadaki internet kullanan nüfus ortalamasının hep üzerinde olduğu görülmektedir. Bununda aslında internet ve teknolojik atımların Amerika'da ortaya çıkmasından kaynaklandığı anlaşılmaktadır. Ayrıca Doğu Asya ve Sahra Altı Afrika bölgelerinde internet kullanan nüfusun, dünya

[143] Ali Burak Darıcılı, **Siber Uzay ve Siber Güvenlik ABD ve Rusya Federasyonu'nun Siber Güvenlik Stratejilerinin Karşılaştırmalı Analizi**, 1. b, Bursa: Dora Basım-Yayın, 2017, s. 64.
[144] Tülay Bektaş Şeker, **İnternet ve Bilgi Açığı**, Konya: Çizgi Kitabevi, 2025, s. 67.
[145] Uluslararası Telekomünikasyon Birliği, https://ourworldindata.org/grapher/share-of-individuals-using-the-internet?tab=chart, (Erişim Tarihi: 01.07.2025).

ortalamasının altında görülmektedir. Bu durumunda bölgenin ekonomik ve teknolojik altyapısı ile ilgili olabileceği akla gelmektedir.

İnternet, başlangıçta esas olarak araştırma ve eğitim amaçlı bir ağ olarak tasarlanmış olmasına rağmen, günümüzde kullanım alanı çok daha geniş ve farklı boyutlara ulaşmıştır. Günümüzde internet, kamu, özel ve ticari iletişim için temel bir altyapı haline gelmiş olup hızla büyümektedir. İnternet üzerindeki güvenlik açıkları hem kamu kurumları hem özel sektör kuruluşları ve bireyler için önemli riskler oluşturmaktadır. Kurumların kendi bünyelerindeki bilgisayarlar ve ağlar için geliştirdikleri güvenlik önlemleri, birbirine bağlı karmaşık bir ağ yapısı olan internet üzerinde aynı derecede etkili olamamaktadır. İnternetin temel yapısında güvenlik unsurlarının önceden tasarlanmamış olması, bilgi bütünlüğü, kullanılabilirlik ve mahremiyetin sağlanmasını zorlaştırmaktadır. Daha önce de belirtildiği üzere, internet, kullanıcılar arasında güven esasına dayanan açık bir sistem olarak geliştirilmiştir. Bu nedenle, kontrol merkezi bir yönetim yerine kullanıcılarda bulunmaktadır ve tek bir otorite tarafından yönetilememektedir. Ayrıca, internetin coğrafi bir sınırı veya fiziksel bir mekânı olmaması, ona geleneksel fiziksel kuralların uygulanmasını güç ya da imkânsız kılmaktadır. Bunun yanı sıra, internet güvenliği bağlamında dikkate alınması gereken önemli bir diğer husus, saldırganların teknik becerileri ile teknolojik olanaklardaki gelişmelerdir.[146]

Siber uzay, yalnızca kritik altyapılardaki güvenlik açıklarından kaynaklanabilecek fiziksel saldırılara müdahale edilmesini gerektirmekle kalmayıp, aynı zamanda iletişim kesintileri ve gecikmeler aracılığıyla fiziksel saldırıların gerçekleşmesini kolaylaştıran bir ortam da sunabilmektedir. Bir siber teröristin, bilgisayar başında bulunduğu konumdan bağımsız olarak, dünyanın herhangi bir noktasındaki başka bir bilgisayara eşit uzaklıkta olması bu alanın küresel doğasının somut bir örneğidir. Bilgi akışı, politik, etnik ve dini sınırları aşarak sürekli ve kesintisiz bir şekilde devam etmektedir. Ayrıca, siber uzayın temelini oluşturan yazılım ve donanım altyapısı da küresel ölçekli tasarım ve gelişim süreçlerinin ürünüdür. Bu küresel yapı nedeniyle, mevcut güvenlik açıkları evrensel düzeyde erişilebilir olup, tüm kullanıcılar için potansiyel risk teşkil etmektedir.[147]

---

[146] Sait Yılmaz ve Olcay Salcan, **Siber Uzay'da Güvenlik ve Türkiye**, 1. b, İstanbul: Milenyum Yayınları, 2008, s. 37-38.
[147] Yılmaz ve Salcan, **a.g.e.,** s. 49-50.

Siber uzayda zaman ve mekân kavramları, fiziksel dünyadaki simetrik yapıya tabi değildir. Bu farklılık, aktörlere fiziksel sınırların ötesinde stratejik anlamda belirgin asimetriler oluşturma olanağı tanımaktadır. Geleneksel simetrik çatışma ortamlarında taraflar birbirlerini görebilmekte ve rakibin belirli bir zaman ve mekândaki hareketlerini takip edebilmektedir. Buna karşın siber saldırılar durumunda, mağdur taraf saldırganın kimliği, konumu ve saldırının gerçek amacına ilişkin kesin bilgilere ulaşmakta zorlanmaktadır. Ayrıca, siber tehdit aktörleri mesai kavramına bağlı kalmaksızın faaliyet gösterebilmekte ve hedeflerinin çalışma saatlerine riayet etmeksizin saldırılar gerçekleştirebilmektedirler. Bu bağlamda, siber tehditlerin asimetrik ve dinamik yapısı, genellikle simetrik örgütlenmeye sahip devlet ve kamu kurumlarının hiyerarşik yapıları ile kültürel normları üzerinde olumsuz etkiler yaratmakta; özellikle nükleer enerji tesisleri ve kritik altyapı gibi hassas alanlarda dezavantajlı konumlara yol açmaktadır.[148]

Siber uzay, dört temel bileşenden meydana gelmektedir: kullanıcılar; çevrimiçi paylaşılan resimler, metinler, videolar ve sesler gibi bilgi içerikleri; programlar, kodlar ve protokoller gibi yazılımsal unsurlar; ayrıca bilgisayarlar, kablolar, sunucular, uydu sistemleri, anahtarlar ve modemler gibi fiziksel altyapıyı oluşturan donanımlar. Bu bağlamda, siber uzay ekosisteminin herhangi bir bileşenine yönelik gerçekleştirilen saldırılar, siber saldırı olarak tanımlanmalı ve bu şekilde değerlendirilmelidir; aksi takdirde yapılacak tanımlar eksik kalacaktır.[149]

Siber uzayla ilgili kavramlara ilişkin tanımlarda genel bir mutabakat sağlanamamış olsa da Soğuk Savaş sonrasındaki dönemde, özellikle 2000'li yılların başlarından itibaren devletlerin ordularını, istihbarat birimlerini, kurumsal yapıları ve vatandaşlarını siber tehditlere karşı korumak amacıyla kapsamlı siber güvenlik stratejileri geliştirmeye başladığı görülmektedir. Devletler, etkin bir siber güvenlik kapasitesi oluşturabilmek için, siber uzay alanındaki teknolojik üstünlüğe sahip olmaları ve bu alandan kaynaklanabilecek saldırılara karşı gerekli önlemleri almaları gerektiğinin bilincindedir. Günümüzde devlet güvenliğinin teknolojik gelişmelerle doğrudan ilişkili olduğu göz önüne alındığında, siber uzay teknolojilerine erişim eksikliğinin ciddi bir güvenlik açığı yaratacağı da açıktır. Ayrıca, devletlerin güvenlik stratejilerini etkili bir

[148] Ekonomi ve Dış Politikalar Araştırma Merkezi, **a.g.e.,** s. 94.
[149] Köksoy, **a.g.e.,** s. 11.

siber güvenlik ve savunma kapasitesi oluşturmak amacıyla, geleneksel güvenlik paradigmasına dayalı kurum ve stratejilerini yeniden yapılandırmaları gerekmektedir.[150]

Küresel siber alandaki çalışmalar, temelde yedi ana başlık altında toplanmaktadır:

1-Teknik Altyapı: Alan adı sistemi ve teknik standartların düzenlenmesi.

2-Suç: Siber suçlarla mücadele edilmesi.

3-Savaş ve Sabotaj: Yıkıcı siber saldırılar ve siber savaş faaliyetleri.

4-Casusluk: Siber ortamda yapılan istihbarat ve bilgi toplama eylemleri.

5-Gizlilik: Çevrimiçi mahremiyetin ve kişisel verilerin korunması.

6-İçerik Yönetimi: İnternet üzerindeki içeriklerin denetlenmesi ve kontrolü.

7-İnsan Hakları: Dijital dünyada temel insan haklarının gözetilmesi.[151]

Siber uzayın temel unsurlarından biri insan faktörüdür; zira siber saldırılar genellikle bireyler veya gruplar tarafından planlanmakta ve yürütülmektedir. Aynı zamanda bu saldırılar, hedef olarak da insanları veya insan topluluklarını seçebilir. Bu durum, kullanıcıların siber uzayın en savunmasız ve bilinçlendirilmesi gereken kesimi olduğunu göstermektedir. Öte yandan, siber güvenliğin güçlendirilmesinde en kritik aktörlerin de bireyler olduğu söylenebilir. Başka bir ifadeyle, siber güvenlikte en zayıf halka birey olduğundan, etkin bir güvenlik sağlamak için bireylerin eğitilmesi en doğrudan ve etkili yöntem olarak öne çıkmaktadır. Bu bağlamda, siber güvenlik konusu sadece teknik bir mesele olmayıp, sosyal ve siyasal boyutlarıyla da ele alınmalıdır. Gelişmiş güvenlik teknolojileri ne kadar etkin olursa olsun, bu teknolojilerin başarılı bir şekilde uygulanabilmesi, nitelikli insan kaynaklarına bağlıdır. Ayrıca, kapsayıcı bir siber güvenlik stratejisinde insan faktörünün yokluğu, süreçlerin etkin ve başarılı bir biçimde yürütülmesini güçleştirmektedir. Siber uzaydaki paydaşların çıkarlarının ve güvenliklerinin korunması, belirli sınırların ötesinde küresel iş birliği ve etkileşim gerektirir. Zira, küresel çabalar hem farkındalığı artırmakta hem de daha güçlü güvenlik standartlarının geliştirilmesi ile siber suçların araştırılması ve kovuşturulmasında etkinlik sağlamaktadır. Siber saldırıların doğası itibarıyla küresel olması, siber güvenliğin

[150] Darıcılı, **a.g.e.,** s. 33.
[151] Joseph S. Nye, "The Regime Complex for Managing Global Cyber Activities", **Global Commission on Internet Governance Paper Series**, 2014, s. 7.

sağlanmasının da ancak milletlerarası iş birliği ve yönetişimle mümkün olacağını göstermektedir.[152]

3.1.2.1. Siber Güvenliğin Tanımı ve Ortaya Çıkışı

Siber uzay, sunduğu yaşam kolaylıkları ile beraberinde getirdiği risk ve tehditler nedeniyle son dönemlerde birçok disiplinin yanı sıra milletlerarası ilişkiler alanında da merkezi bir tartışma konusu haline gelmiştir. Bu alandaki kavramların ve olguların eski paradigmalarla değerlendirilmesi, henüz sağlıklı ve kapsamlı bir yaklaşımın geliştirilmesini engellemiştir. Milletlerarası ilişkiler disiplini, disiplinler arası özellik taşımasına rağmen kuruluşundan itibaren realist ve güvenlik odaklı yaklaşımların etkisi altında kalmıştır. Bu durum, siber uzayın da öncelikle güvenlik perspektifiyle ele alınmasına neden olmaktadır. Siber uzay, milletlerarası ilişkileri derinden etkileyip şekillendirme kapasitesine sahip önemli bir araç olarak karşımıza çıkmaktadır. Bu alandaki kısa tarihsel süreçte bile birçok örnek ve vakıa, siber uzayın milletlerarası dinamiklerde oynayabileceği rolü ortaya koymaktadır. Ancak, siber uzayın gelecekte barışçıl ve refahı artırıcı bir platform mu, yoksa güvenlikçiliğin ve askerileştirmenin etkisiyle mevcut fiziksel milletlerarası sorunların yansıtıldığı bir ortam mı olacağı konusunda kesin bir yargıya varmak güçtür. Bu sorulara verilecek yanıtlar, büyük ölçüde bugün geliştirilecek politikalar ve uygulamalar doğrultusunda şekillenecektir. Güvenlik temelli bir yaklaşımın benimsenmesi durumunda, siber uzayın çatışmacı bir yapıya bürünmesi muhtemel iken; şeffaflık, özgürlük, iş birliği ve paylaşım temelli stratejiler ise, daha barışçıl ve istikrarlı bir milletlerarası siber ortamın oluşmasını sağlayacaktır. Burada temel belirleyici unsur, siber uzay aktörlerinin ve paydaşlarının inşa etmek istedikleri geleceğin niteliğidir. Ayrıca, siber uzay büyük veri kapasitesi sayesinde sosyal bilimlerde davranışsal analizlerin yapılmasını mümkün kılmıştır. Geçmişte erişilmesi güç olan istatistiksel verilere, günümüzde internet sayesinde kolaylıkla ulaşılabilmekte ve bu durum nicel veri kullanımını zorunlu kılmaktadır. Siber güvenlik ise, anarşik yapısı ile bilinen siber uzayın doğrudan bir ürünüdür. Bu bağlamda, siber güvenlik alanında farklı türde aktörlerin etkin olduğu gözlemlenirken, hiçbir aktörün tek başına hâkimiyet kurmadığı da dikkat çekmektedir.[153]

[152] Köksoy, **a.g.e.,** s. 23-24.
[153] Köksoy, **a.g.e.,** s. 3-5.

Siber alandaki hızlı gelişmeler, yeni güvenlik tehditlerinin ortaya çıkmasına yol açmıştır. Bu tehditlerle başa çıkma sürecinde devletlerin önemi giderek artmakla birlikte, devletlerin bu konuda etkin stratejiler geliştirmekte güçlük çektiği gözlemlenmektedir. Küçük gruplar ve bireylerin gerçekleştirdiği siber saldırıların etkisiyle, milletlerarası sistemin yapısı neo-realist paradigmaların öngördüğünden daha belirsiz ve anarşik bir niteliğe bürünmeye başlamıştır. Siber uzayın doğası gereği, tehditlerin kaynağının, zamanının ve yerinin önceden tahmin edilemez olması, milletlerarası sistemi Soğuk Savaş dönemine kıyasla daha karmaşık ve kontrolü zor bir hale getirmektedir. Ayrıca, siber uzayı düzenleyen kapsamlı ve evrensel bir milletlerarası hukuk rejiminin henüz oluşturulamamış olması; devletler arasındaki iş birliği yerine artan rekabetçi politikaların egemenliği ve bu rekabetin giderek şiddetlenmesi, milletlerarası sistemin eskiye göre, çok daha fazla belirsizlik ve güvensizlik içinde olduğunu göstermektedir.[154]

Terör örgütlerinin siber savaş kapasitesine sahip olup olmadıkları ya da bu kapasitenin düzeyi hakkında kesin bilgilere ulaşmak güçtür. Ancak son dönemlerde, bazı terörist grupların siber saldırıları stratejik bir silah olarak kullanmaya başladığı gözlemlenmektedir. Teröristlerin planlama yapmak, finansal işlemlerini yürütmek, propaganda faaliyetlerini sürdürmek ve güvenli iletişim sağlamak amacıyla bilgi teknolojileri ve interneti yoğun şekilde kullandığı bilinmektedir. Örneğin, 1993 yılında Dünya Ticaret Merkezi'ne yönelik ilk bombalama eyleminin planlayıcısı olarak hüküm giymiş olan Remzi Yusuf'un dizüstü bilgisayarında, Pasifik bölgesinde faaliyet gösteren 12 farklı havayolu şirketine yönelik bombalama planlarını içeren şifreli dosyalar bulunmuştur. Dünya Ticaret Merkezi'ne yönelik saldırılar, sadece can ve mal kaybına yol açmakla kalmamış, aynı zamanda pazarların kapanmasına ve New York'un finansal bilgi altyapısının tahrip olmasına neden olmuştur. Bu olaylar, teröristlerin bilgi teknolojisini kritik altyapılara karşı etkin bir saldırı aracı olarak kullanma eğilimlerini açıkça ortaya koymaktadır. Gelecekte ülkeler, sadece saldırgan birey ve grupların değil, aynı zamanda bilgi harbi olarak tanımlanan; "kendi bilgi ve bilgi sistemlerini korurken, düşmanın bilgi ve bilgi sistemlerini etkileyerek bilgi üstünlüğü sağlamaya yönelik" araç ve teknikleri kullanan devlet aktörlerinin siber saldırılarına maruz kalabileceklerdir. Gelişmiş siber saldırı teknikleri ve eğitimli personel ile donanmış ülkeler, bilgi harbi yürütme kapasitesine sahip olabilirler. Siber uzay savunmasında baştan itibaren güçlü bir konumda

[154] Darıcılı, **a.g.e.,** s. 128.

olan ve bu alanda hazırlıklarını tamamlamış devletler, söz konusu tehditlere karşı etkin bir direnç gösterebileceklerdir.[155]

Siber güvenlik, kısa sürede ve düşük maliyetle çeşitli sektörlere yönelik gerçekleştirilen siber saldırılar sonucunda, ülkelerin askeri ve siyasi yapılarına ilişkin gizli bilgilerin açığa çıkması, toplumsal yapılar ve kimliklerle ilgili algıların şekillenmesi, ulusal ekonomilerin zarar görmesi ile kritik altyapı sistemlerine yönelik saldırılar sonucu çevresel sorunların ortaya çıkması gibi pek çok alanda önemli bir güvenlik sorunu haline gelmiştir. Bu bağlamda, siber güvenlik aynı zamanda güvenlik sektörlerinin birbirine nasıl entegre olduğunu ve iç içe geçtiğini göstermesi bakımından da büyük önem taşımaktadır. Bu noktadan hareketle, siber güvenlik ve onun gelişim sürecini, genel anlamda bir güvenlikleştirme süreci çerçevesinde değerlendirmek anlamlı olacaktır.[156] Siber uzayda olduğu gibi, siber güvenlik kavramı da sürekli değişen ve gelişen dinamik bir yapıya sahiptir; bu nedenle tanımları da zaman içinde evrilmektedir. Hatta aynı kurumlar, farklı dönemlerde değişen teknolojik koşullar ve gelişmeler doğrultusunda, yeni kavram ve süreçleri içerecek şekilde farklı tanımlar yapmak zorunda kalmaktadırlar. Siber uzay ekosistemi hem derinliği hem genişliği ile oldukça kapsamlı ve değişken bir alan olduğundan, mevcut birçok kavrama ek olarak her geçen gün yeni kavramlar gündeme gelmektedir.[157]

Bilgisayarların taşınabilirlik kazanması, akıllı cep telefonu teknolojilerinin gelişimi ve internet erişiminin yaygınlaşması sonucunda, internetin sunduğu olanaklar ve sağladığı kolaylıklar yalnızca günlük yaşamı değil, aynı zamanda siyasal, askeri ve ekonomik alanlarda da yeni bir güç dinamiğinin ortaya çıkmasına zemin hazırlamıştır. Bu gelişmeler, güvenlik alanındaki tartışmaların ve analizlerin siber uzay ile siber güvenlik kavramları çerçevesinde şekillenmesine de önemli ölçüde katkı sağlamıştır.[158]

Profesyonel ve gizli yürütülen bilgisayar tabanlı istihbarat faaliyetleri ise, amaç ve yöntem açısından farklılık göstermektedir. Devletlerin resmî kurumları, özel sektör kuruluşları, araştırma enstitüleri, ticari organizasyonlar, sanayi firmaları ve bankalar gibi birçok aktör, bilgisayar ağlarından yararlanmaktadır. Bunların bir kısmı kendi

[155] Yılmaz ve Salcan, **a.g.e.,** s. 54-55.
[156] Eren, **a.g.e.,** s. 25.
[157] Köksoy, **a.g.e.,** s. 8.
[158] Darıcılı, **a.g.e.,** s. 30.

geliştirdikleri özel yazılımlar ile iç işleyişlerini sürdürmektedir; örneğin bir devletin üst düzey makamları, ülkenin en uzak noktalarındaki bireysel tüketim verilerini takip edebilmektedir. Dışarıdan bilgisayar istihbaratı gerçekleştiren aktörler için, bu durum birçok erişim kapısının açık olması anlamına gelmektedir. Yerel ağlar üzerinden merkezi yönetim noktalarına ve tersine ulaşım mümkündür. Ulusal ağların milletlerarası web bağlantıları olsa da dışarıdan erişim teorik olarak engellenmektedir. Elektronik ortamdaki tüm veri akışları dinlenmekte, manyetik bantlara kaydedilmekte ve ardından tercüme, analiz ve değerlendirme süreçleri için ilgili merkezlere iletilmektedir. İşlem sonrası veriler farklı depolama birimlerine aktarılmakta, özetlenmekte ve indekslenerek karar mercilerine sunulmaktadır. Bu süreçlerin tümü bilgisayar teknolojisinin kapsamındadır. Bilgisayar sistemlerinin içerikleri, kapasiteleri, uyumlulukları, esneklikleri ve uydular gibi iletişim altyapıları, teknik istihbaratın ayrılmaz parçasını oluşturmaktadır. Bilgi hırsızlığı ve sistemlere izinsiz erişim "hack" işlemleri, ileri düzey programlama bilgisine sahip uzman kişiler tarafından, hedef bilgisayarın işletim sistemi veya yazılımındaki güvenlik açıkları tespit edilerek gerçekleştirilmektedir. Hedef sistem şifre korumalı ise, şifreler özel olarak geliştirilen yazılımlar aracılığıyla ya da farklı yöntemlerle elde edilip kırılarak erişim sağlanmaktadır. Ayrıca bilgi toplama amaçlı dinleme istasyonları ve telefonlara yerleştirilen çipler gibi donanımlar da kullanılmakta ve tüm bu süreçlerde bilgisayar teknolojisi etkin biçimde destek sağlamaktadır.[159]

Ulusal siber güvenlik kavramı, hükümetlerin ulusal güvenlikle doğrudan ilişkili alanlarda kamu sektörü, özel sektör ve ilgili milletlerarası bilişim ve iletişim teknolojisi (BİT) sistemlerine bilgi akışını düzenleyen prensipler bütünü ve bu alandaki devlet aracılığıdır. Bu kavram beş temel yetki alanına dayanmaktadır: 1- askeri siber alan faaliyetleri, 2- siber suçlar konusunda hesap verebilirlik mekanizmaları, 3- istihbarat ve karşı istihbarat faaliyetleri, 4- kritik altyapının korunması ve kriz yönetimi, 5- siber diplomasi ile internet yönetimi.[160]

Siber uzayda tarafların çıkarları çatıştığında, taraflar meşru olmayan yöntemlere başvurabilmektedir. Ayrıca, çoğu zaman tarafların geliştirdiği siber silahlar ve teknolojiler, karşılıklı bir güç mücadelesinin ortaya çıkmasına yol açmaktadır. Siber saldırılara karşı geliştirilen politika ve araçlar da bu güç mücadelesini daha da

[159] Yılmaz ve Salcan, **a.g.e.,** s. 26-27.
[160] Köksoy, **a.g.e.,** s. 444.

derinleştirebilmektedir. Söz konusu mücadele, ekonomik, sosyal ve siyasi alanlarda önemli zararlara yol açabilecek siber savaşlara dönüşme potansiyeli taşımaktadır. Bu durum hem bireylerin hem de devletlerin farklı dönemlerde değişken tehdit algılarıyla karşı karşıya kalmasına neden olmaktadır. Siber uzay, milletlerarası ilişkilerin biçimlenmesinde ve aktörlerin pozisyon almalarında yeni bir alan olarak önem kazanmıştır. Bu alandaki üstünlük mücadelesi, devletleri zaman zaman karşı karşıya getirirken, bazen de ortak politikalar geliştirmek üzere iş birliğine sevk etmektedir. Milletlerarası aktörler, siber alanda etkinlik sağlamak ve potansiyel tehditleri önlemek amacıyla hızla büyüyen bilişim sektörüne odaklanmaktadırlar. Ayrıca, ekonomik ve sosyal düzenin sürekliliğini sağlamak için kritik sistemlere yönelik olası zararlı müdahalelere karşı önlemler almaya çalışmaktadırlar.[161]

Siber güvenlik, çağımızın bilgi teknolojileri ortamında elektronik cihazların ve dijital verilerin kötü niyetli siber saldırılara karşı korunması ile bu doğrultuda gerekli güvenlik tedbirlerinin uygulanmasını ifade etmektedir. Bu kavram, oldukça geniş kapsamlı olup yalnızca temel bir tanımla sınırlanamaz. Siber güvenlik bağlamında, "hack" terimini anlamadan önce bu kavramın açıklığa kavuşturulması gerekmektedir. Hack, bir sistemin güvenlik açıklarını tespit etmek ve izinsiz olarak belirli kişi veya kuruluşların dosyalarına ya da sistemlerine müdahale etmek anlamına gelmektedir. Hacker ise, bu teknik bilgi ve yöntemlere sahip olarak sistemi bu şekilde ele geçiren bireyi tanımlamaktadır.[162]

Siber güvenlik, bilişim sistemlerinin tüm bileşenlerini kapsayan kapsamlı bir güvenlik alanıdır ve sıklıkla bilgi güvenliği ile karıştırılmaktadır. Ancak siber güvenlik, bilgi güvenliğine kıyasla daha geniş bir çerçeveyi ifade etmektedir. Bu bağlamda, siber savaş ve siber ordu gibi kavramlarla birlikte değerlendirilir. Siber güvenlik sahasında birçok alt disiplin mevcuttur; web güvenliği, ağ güvenliği, yazılım, donanım ve fiziksel güvenlik kategorileri en yaygın olanlarıdır. Medyada "hack" terimi genellikle siber suç faaliyetleriyle ilişkilendirilse de bu tanım eksik ve yanıltıcıdır. Toplumda yanlış bir algıya yol açan bu kavram, aslında geniş bir yelpazede kullanılmaktadır; örneğin, bir kişinin yoğurt kabını saksıya dönüştürmesi veya bilgisayar grafiklerinde matematiksel formülleri

[161] Eren, **a.g.e.,** s. 2.
[162] İlker Ertuğrul, **Network, Linux, Kriptoloji, Deep Web, Sızma Testleri, Ofansif ve Defansif Siber Güvenlik**, 1. b, İstanbul: Dikeyeksen, 2020, s. 2.

optimize eden hızlı algoritmalar geliştirmesi de birer hack örneğidir. Siber güvenlik literatüründe ise, hack, sistemdeki bir açığın kullanılması anlamına gelir. Hacker terimi ise, yaygın kanının aksine yalnızca bilgisayar sistemlerine izinsiz giriş yapan ve hizmetlerin durmasına yol açabilen üstün yetenekli bireyler için değil, teknik bilgiye sahip ve sistem açıklarını kullanan kişiler için de kullanılmaktadır. Darknet, deepweb ve Tor gibi kavramlar ise, hackerların anonimlik ve internetten izole olma ihtiyaçlarından doğmuş olup, anonimlik bazen gizlilik, bazen ise, veri paylaşımı amacı taşımaktadır. Günümüzde bu platformlar, suç unsuru taşıyan faaliyetlerin ve bilgilerin paylaşıldığı, kolluk kuvvetlerinin de yoğun şekilde araştırmalar yürüttüğü alanlar haline gelmiştir. Bu nedenle, bu tür ortamlara "karanlık internet" denilmektedir. Örneğin, Temmuz 2015'te FBI tarafından kapatılan Darkode adlı platform, dünya çapında en büyük çalıntı veri satışlarının gerçekleştirildiği bir merkez olarak bilinmektedir. Uzun süreli takip sonucunda gerçekleştirilen operasyon neticesinde, 20 ülkeden 70 kişi tutuklanmış ve birçok kişi hakkında yakalama kararı çıkarılmıştır. Bu operasyonda FBI'ın çeşitli ulusal ve milletlerarası polis teşkilatları ile iş birliği yaptığı ifade edilmiştir.[163]

Derin internet, farklı perspektiflerden çeşitli şekillerde tanımlanmaktadır. Bazı görüşlere göre, kullanıcıların kimliklerinin izlenemediği ve anonimliklerinin korunduğu Tor Gizli Servisleri gibi şifreli bir alanı ifade eder. Diğer bir bakış açısı ise, bilinen arama motorlarının erişemediği, özel şifreleme yöntemleriyle korunmuş sayfalar, bağlantısız web siteleri ve yalnızca belirli kullanıcı gruplarının ulaşabildiği gizli içeriklerin yer aldığı görünmeyen bir boyutu işaret etmektedir. Ayrıca derin internet terimi, bazı çevrelerde yasa dışı faaliyetlerin ve çeşitli zararlı aktörlerin bulunduğu, internetin rahatsız edici ve tartışmalı yönlerini de kapsayan ortak bir kavram olarak kullanılmaktadır. Derin internet, yukarıda bahsedilen unsurları içermekle birlikte, aynı zamanda belirli bir fiziksel ortamdan ziyade bir düşünce biçimi olarak da değerlendirilebilir.[164]

Siber güvenlik, bilginin ve onun taşıdığı özelliklerin korunmasının yanı sıra, bilgisayar sistemlerinin güvenliğinin sağlanması ve bilişim sistemlerinden kaynaklanabilecek siber tehditler ile saldırıların yol açtığı güvenlik açıklarının en aza indirilmesini hedefleyen kapsamlı bir alandır. Her ne kadar bu tanım siber güvenliğin

[163] Mustafa Altınkaynak, **Uygulamalı Siber Güvenlik ve Hacking**, 3. b, İstanbul: Ezgi Matbaacılık, s. 1.
[164] Jamıe Bartlett, (Çev.Yasin Konyalı), **Dark Net İnternetin Yeraltı Dünyası**, 1. b. İstanbul: Timaş Yayınları. 2016. s. 12-13.

sağlanması sürecinde kullanılan çeşitli araç ve yöntemlere işaret etse de hukukî çerçeve ve insan hakları boyutuna değinmemesi önemli bir eksiklik olarak değerlendirilmektedir. Aslında, bu iki kritik unsuru ön plana çıkaran tanımlara literatürde nadiren rastlanmaktadır.[165] Siber güvenliğin temel amacı, tüm kullanıcılar ve paydaşlar için özgürlük ve güvenliğin sağlandığı bir siber ortam yaratmaktır. Bireylerden milletlerarası kuruluşlara kadar geniş bir yelpazeyi kapsayan siber uzay aktörlerinin farklı perspektiflere sahip olması doğaldır. Bireyler, özel sektör temsilcileri, sivil toplum kuruluşları, devletler ve milletlerarası örgütler gibi çeşitli yapıların ortak hedef ve süreçlerde birleşmesi zorluklar barındırsa da tüm bu aktörlerin siber uzayda birlikte var olma ve buradan faydalanma zorunluluğu bulunmaktadır. Bu bağlamda, paydaşların hak ve menfaatlerini koruyan kapsayıcı ve dengeli çözümler geliştirilmesi gereklidir.[166]

Siber güvenlik, temelde siber alanda gerçekleşen saldırılar, riskler ve tehditler nedeniyle ortaya çıkan güvensizlik durumunu ifade etmektedir. Bu güvensizliğin kaynakları teknik, sosyal veya fiziksel temelli siber saldırılardan oluşmaktadır. Genel olarak, siber güvenlik kavramı, bireyler veya şirketlere yönelik küçük ölçekli bilgisayar sistemi saldırılarıyla ilişkilendirilsede son yıllarda ulusal ve milletlerarası güvenliği derinden tehdit eden, büyük çaplı siber saldırıların da gerçekleştiği gözlemlenmektedir.[167]

Ağ protokolleri, işletim sistemleri ve yazılımlarda meydana gelen hatalar, deneyimli programcılar tarafından tespit edilmekte; kâr amacı güden veya sadece keyfi nedenlerle saldırı gerçekleştiren pek çok bilgisayar korsanı tarafından ise, istismar edilmektedir. Tam anlamıyla güvenli kodlama ve konfigürasyonlar yapılsa bile, kasıtlı saldırılar ile doğal afetlerin varlığı her zaman söz konusu olacaktır. Bu nedenle, yüzde yüz güvenlik sağlanmasının mümkün olmadığı söylenebilir. Risk, "bir varlıkta bulunan zayıflığın bir tehdit unsuru tarafından kullanılması ihtimali" olarak tanımlanabilir. Mutlak güvenliğin mevcut olmaması sebebiyle bilgi sistemlerinde her daim bir risk bulunmaktadır. Buradaki temel amaç, mevcut riski tamamen ortadan kaldırmak değildir; zira riskin sıfırlanmasına yönelik çabalar, teknolojik ve ekonomik açıdan çoğu zaman sürdürülebilir değildir. Ayrıca, bir bilgi sistemi için riskleri tamamen ortadan kaldırmak amacıyla, o sistemin değerinden daha fazla kaynak ayırmak mantıklı bir yaklaşım

[165] Köksoy, **a.g.e.,** s. 7.
[166] Köksoy, **a.g.e.,** s. 8.
[167] Köksoy, **a.g.e.,** s. 10.

değildir. Öte yandan, riskleri olduğu gibi kabul etmek de zararlı sonuçlar doğurabilir. Bu nedenle, risklerle birlikte yaşamayı öğrenmek daha etkin bir strateji olarak değerlendirilmektedir. Bu bağlamda, bilgi sistemindeki riskleri değerlendiren, risklerin yaratabileceği zararları tahmin eden, risk azaltma önlemlerinin maliyetini hesaplayan ve buna göre, riskleri minimize eden bir mekanizmaya ihtiyaç duyulmaktadır. Risk yönetimi bu işlevi yerine getiren temel araçtır. Mutlak güvenliğin sağlanamaması ve risklerin varlığı, güvenliği salt bir ürün olarak görme yaklaşımını geçersiz kılmaktadır. Günümüzde bilgi teknolojileri güvenliği, gerçek zamanlı risk yönetimi süreci haline gelmiştir. Bu süreçte risk yönetimi, bilgi teknolojileri güvenlik ürünlerinin seçimi ve geliştirilmesinde temel karar verme mekanizması olarak işlev görmektedir.[168]

Siber güvenlik, yalnızca ulusal güvenlik açısından değil, aynı zamanda küresel ekonomik yapı üzerinde de önemli etkiler yaratmaktadır. Nitekim 2004 yılında küresel siber güvenlik sektörünün piyasa değeri yaklaşık 3,5 milyar Amerikan doları olarak belirlenmişken, bu rakam 2017 yılına gelindiğinde yaklaşık 35 kat artarak 120 milyar dolara ulaşmıştır. Bu hızlı büyüme, siber güvenliğin ekonomik boyutunu gözler önüne sermektedir. Aynı yıl itibarıyla siber suçların küresel ekonomiye verdiği zararın yaklaşık 600 milyar dolar olduğu ve bu rakamın dünya gayrisafi yurt içi hasılasının yaklaşık %0,8'ine tekabül ettiği tespit edilmiştir. BİT'lerin ekonomik sistemlere katkısı değerlendirildiğinde, küresel düzeyde faaliyet gösteren ilk 500 siber güvenlik firmasının coğrafi dağılımı da dikkat çekicidir. Bu firmaların %75'i Kuzey ve Güney Amerika kıtalarında yer alırken, %14'ü Avrupa'da, %7'si İsrail'de ve %4'ü ise, Asya kıtasında konumlanmıştır. AB ülkeleri özelinde yürütülen analizlerde ise, BİT sektörünün ekonomik katkısı; yaratılan katma değer, sağlanan istihdam olanakları ve araştırma-geliştirme faaliyetleri bağlamında ele alınmış ve bu alanın ekonomik büyüme üzerindeki stratejik rolü açık biçimde ortaya konulmuştur.[169]

Bilgi çağının sunduğu gelişmiş teknolojiler, istihbarat örgütleri açısından hem yeni fırsatlar hem de çeşitli zorluklar yaratmaktadır. Bu bağlamda istihbarat kurumları, hem bilgi toplama ve analiz süreçlerini daha verimli hâle getirecek yöntemleri benimsemeye çalışmakta hem de elde edilen verilerin politika yapıcılara etkin biçimde aktarılması için yeni stratejiler geliştirmektedir. Günümüz istihbarat yapılanmalarında

[168] Yılmaz ve Salcan, **a.g.e.,** s. 73-74.
[169] Köksoy, **a.g.e.,** s. 456.

öncelikli hedeflerden biri, gizli verilerin güvenli biçimde aktarılabileceği özel dijital iletişim ağlarının oluşturulmasıdır. Bu doğrultuda, ABD örneğinde geliştirilen "intelink" adlı sistem, istihbarat personelinin gizli belgelerle etkileşimde bulunmasına olanak tanıyan, güvenlik duvarları ve özel ağ protokolleriyle korunmuş kapalı bir ağ yapısıdır. İntelink sistemi, görünüm açısından genel internet altyapısına benzemekle birlikte, sadece yetkili kullanıcıların erişebileceği ve güvenlik dereceli içeriklerin barındırıldığı sayfalardan oluşmaktadır. Bu sistemin kullanıcıları arasında savunma, dışişleri, enerji, adalet ve ulaştırma bakanlıkları gibi kamu kurumlarının temsilcilerinin yanı sıra askeri personel de yer almaktadır. Ancak pratikte, kullanıcıların bu platform yerine hâlâ brifingler, fiziki belgeler ve telekonferanslar gibi daha geleneksel yöntemleri tercih ettikleri gözlemlenmektedir. Öte yandan, internetin küresel ölçekteki yaygınlığı ve erişilebilirliği, bilgisayar teknolojisinin tek başına elektronik istihbarat üretimini mümkün kılan bir temel unsur hâline gelmesini sağlamıştır. Günümüzde Yahoo, Google, Bing gibi popüler arama motorları, internetin devasa boyutunun yalnızca sınırlı bir bölümünü tarayabilmektedir. Bu durum, sanal ortamın istihbarat faaliyetleri için ne denli geniş ve zengin bir kaynak sunduğunun bir göstergesidir.[170]

Günümüzde bilgiye erişim araçlarının hem teknolojik hem de elektronik düzeyde büyük bir çeşitlilik ve gelişim göstermesi, özellikle bilgi savaşı ortamında koruyucu güvenlik tedbirlerinin önemini artırmıştır. Koruyucu güvenlik kavramı; güvenlik, istihbarata karşı koyma ve casusluğa karşı koyma olmak üzere üç temel bileşenden oluşmaktadır. Güvenlik terimi, bir devletin ulusal politikaları, diplomatik kararları, askerî faaliyetleri ve genel güvenlik stratejilerine ilişkin hassas bilgilerin korunmasına yönelik çabaları ve bu kapsamda alınan tedbirleri ifade etmektedir. Bu kapsamda koruyucu güvenlik; iletişim güvenliği, fiziksel güvenlik, personel güvenliği, donanım güvenliği ve yazılım güvenliği gibi alt başlıklarla istihbarat ve güvenlik birimlerinin temel sorumluluk alanlarını belirlemektedir. Bilgi sistemlerinde yer alan kritik içerikler ve elektronik bileşenler, yetkisiz erişime ve bozulmaya karşı son derece hassas olup, bunların yerine yenilerinin konulması ekonomik ve teknik açıdan yüksek maliyetlidir. Bu durum, söz konusu sistemleri casusluk ve sabotaj faaliyetleri için cazip hedefler hâline getirmektedir. Bu nedenle gelişmiş ülkeler, bilgi güvenliğini sağlamak amacıyla çok katmanlı güvenlik politikaları geliştirmekte; güçlü şifreleme teknolojileri üretmekte, ulusal yazılım

[170] Yılmaz ve Salcan, **a.g.e.,** s. 17-18.

merkezleri kurmakta ve ileri düzey izleme sistemleri ile desteklenmiş donanım altyapılarını geliştirmektedir. Donanım güvenliği; başta bilgisayar sistemleri olmak üzere, kurum içi donanımların düzenli bakımının yalnızca yetkili personel tarafından gerçekleştirilmesini, yüksek gizlilik derecesine sahip veri taşıyıcılarının (örneğin hard disk, CD, disket) kurum dışına çıkarılmasının engellenmesini kapsamaktadır. Yazılım güvenliği ise, dış kaynaklardan temin edilen uygulamaların içeriğinde gizlenmiş olası kötü amaçlı yazılımların tespiti ve sistemlere zarar verebilecek programların yüklenmesinin önlenmesi gibi önlemleri içermektedir. Ulusal güvenlik bağlamında, devletler kullandıkları elektronik sistemlerde yer alan hassas verilerin, çoğunlukla yabancı üreticiler tarafından geliştirilen ve sınırlı denetim imkânı sunan yazılımlarla işlenmesinden dolayı kaygı duymaktadır. Bu nedenle, izinsiz giriş tespit sistemlerinin, virüs koruma yazılımları ve güvenlik duvarları gibi çözümlerle entegre biçimde geliştirilmesi, gelecekte daha etkin bir yazılım güvenliği altyapısı oluşturulması açısından kritik görülmektedir.[171]

Bu çerçevede, siber uzaydaki kritik sistemleri hedef alabilecek mevcut açıklıkların etkin bir biçimde analiz edilmesi ve bu açıklar için teknik çözümler üretilmesi gerekmektedir. Aynı zamanda, daha güvenli bilişim altyapılarının oluşturulması adına, daha az zafiyet içeren yeni teknolojilerin geliştirilmesi ve mevcut teknolojik eğilimlerin güvenlik açısından değerlendirilmesi yönündeki çabaların kesintisiz şekilde sürdürülmesi büyük önem arz etmektedir.[172]

3.1.2.2. Siber Saldırı Kavramı

Milletlerarası hukuk bağlamında bir siber operasyonun 'saldırı' statüsünde değerlendirilebilmesi için, söz konusu eylemin fiziksel dünyada etkilere yol açması gerekmektedir. Bu çerçevede, insan yaşamına zarar veren, yaralanmalara neden olan veya maddi unsurlar üzerinde fiziki tahribat yaratma potansiyeli taşıyan eylemler siber saldırı olarak nitelendirilmektedir. [173]

[171] Yılmaz ve Salcan, **a.g.e.,** s. 17-18.
[172] Yılmaz ve Salcan, **a.g.e.,** s. 17-18.
[173] Michael N. Schmitt (ed.), **Tallinn Manual on the International Law Applicable to Cyber Warfare**, Cambridge: Cambridge University Press, 2013, s. 106.

Siber saldırı, siber güvenlik, siber caydırıcılık ve siber siyaset gibi kavramlar, tıpkı siber uzayın kendisi gibi belirsizlik içeren, tanımlanması güç ve çok boyutlu olgular arasında yer almaktadır. Bu kavramların sınırları açık şekilde çizilemediğinden, kuramsal çerçeveler içinde ele alınmaları ve uygulamaya yönelik politikaların oluşturulması da çeşitli zorluklar barındırmaktadır. Siber saldırılar yalnızca teknik yöntemlerle gerçekleştirilen dijital müdahalelerden ibaret değildir. Bu tür saldırılar; sosyal mühendislik, kimlik avı (phishing), dolandırıcılık gibi insan temelli yöntemlerle ya da dijital altyapılara yönelik fiziki sabotajlarla da gerçekleştirilebilmektedir. Ancak, mevcut literatürde siber saldırıların tanımlanmasında ve bunlara karşı geliştirilen güvenlik stratejilerinde ağırlıklı olarak teknik temelli yaklaşımlara odaklanıldığı gözlemlenmektedir. Bu durum, siber uzayın doğasının yalnızca teknik bir yapıdan ibaret olmadığı gerçeğini göz ardı eden dar bir perspektifi yansıtmaktadır. Oysa siber uzay, sadece dijital ağlar ve yazılımlar gibi teknik bileşenlerden değil; aynı zamanda bu ağları kullanan bireyler, kurumlar ve sosyal yapıların etkileşiminden oluşan çok katmanlı bir ekosistemdir. Dolayısıyla, siber güvenliğin sağlanmasına yönelik yaklaşımların, bu alanın sosyal, psikolojik ve fiziksel boyutlarını da içerecek şekilde bütüncül bir anlayışla yeniden ele alınması gerekmektedir.[174]

Siber uzayda devletler arasında artan rekabet, 21. yüzyılın en güncel ve karmaşık güvenlik tehditlerinden biri olarak ortaya çıkmaktadır. Günümüzde siber teknolojiler yalnızca savunma amacıyla değil, aynı zamanda saldırı aracı olarak da devletlerin dış politika ve güvenlik stratejilerinde yer edinmiştir. Bu durum, teknolojik gelişmelerin milletlerarası ilişkiler üzerindeki etkisinin giderek daha belirgin hale geldiğini göstermektedir. Siber saldırılar, doğaları gereği geleneksel güvenlik anlayışlarını dönüştürmüş, tehdit algılarını daha çok boyutlu ve asimetrik bir yapıya evrilmiştir. Böylece, klasik anlamda yalnızca devletler arası gerçekleşen güvenlik tehditleri yerini; bireyler, küçük gruplar ve terörist örgütler gibi devlet dışı aktörlerin de etkin olduğu, çok katmanlı bir güvenlik ortamına bırakmıştır. Bu çeşitlilik, yalnızca devletlerin değil, aynı zamanda milletlerarası örgütlerin de (örneğin NATO ve AB) bu yeni tehdide karşı kapsamlı tedbirler geliştirmelerini zorunlu kılmıştır. ABD, Çin Halk Cumhuriyeti ve Rusya Federasyonu (RF) gibi küresel güçler ise, siber uzaydaki potansiyel tehditleri dikkate alarak stratejik yatırımlar yapmakta, saldırı ve savunma temelli siber güvenlik

[174] Köksoy, **a.g.e.,** s. 10-11.

yapılanmalarını güçlendirmekte ve bu bağlamda kurumsal altyapılar oluşturmaktadır. Siber ortamda gerçekleştirilen faaliyetlerin düşük maliyetli, iz bırakmadan yürütülebilir ve kolay uygulanabilir olması, milletlerarası ilişkilerde güvenlik, tehdit ve caydırıcılık kavramlarının yeniden tanımlanmasını gündeme getirmiştir. Bazı devletlerin siber saldırı ve siber savaşı, geleneksel silahlı güçlerin yerine geçebilecek bir stratejik araç olarak değerlendirmeye başlaması, bu alandaki rekabeti daha da derinleştirmiştir. Bu gelişmeler, hem yeni güvenlik tehditlerini beraberinde getirmekte hem de devletlerin bu tehditleri bertaraf edebilmek için politika ve strateji üretme zorunluluğunu artırmaktadır. Ayrıca bireylerin ve küçük çaplı grupların dahi siber saldırılar düzenleyebilme kapasitesi, milletlerarası sistemin daha önce hiç olmadığı kadar belirsiz ve düzensiz bir yapıya dönüşmesine yol açmaktadır.[175]

Siber saldırılarda kullanılan araç ve yöntemler, teknolojik gelişmeler doğrultusunda sürekli evrim geçirmekte, daha erişilebilir ve kullanıcı dostu hale gelmektedir. Bu araçların yaygın şekilde dolaşıma girmesiyle, teknik bilgi ve deneyimi sınırlı bireyler dahi bu araçları kolaylıkla temin ederek kullanabilmektedir. Saldırganlar, çevrim içi sistemlerdeki güvenlik açıklarını tespit etmeye yönelik yeni teknikler geliştirerek, özellikle dağıtık sistem saldırı araçları sayesinde, aynı anda çok sayıda hedefe saldırıda bulunabilmekte ya da belirli ağlara yönelik odaklanmış tehditler gerçekleştirebilmektedir. Bu bağlamda, karmaşık saldırı yazılımlarının sadeleştirilip kolay kullanıma sunulması, düşük teknik kapasiteye sahip bireylerin dahi etkili saldırılar gerçekleştirmesine olanak sağlamaktadır. Nitekim geçmişte yaşanan örnekler, bazı siber saldırıların yüksek düzeyde teknik uzmanlık gerektirmesine karşın, pek çok başarılı saldırının bilgi ve beceri seviyesi düşük kullanıcılar tarafından gerçekleştirildiğini ortaya koymuştur. İnternet temelli saldırılarda fiziksel mevcudiyet gereksiniminin olmaması, saldırganların kimliğinin tespit edilmesini zorlaştırmakta ve güvenlik önlemlerinin etkisini sınırlamaktadır. Mevcut internet altyapısı ve kullanılan iletişim protokolleri, çoğu zaman dış kaynaklı saldırılara karşı yeterli güvenlik sağlayamamakta, dahili tehditlere karşı ise, daha da kırılgan bir yapı sergilemektedir. Dolayısıyla siber güvenlik, çok disiplinli bir yaklaşımı, bilgi paylaşımını ve ortak çözüm üretimini zorunlu kılmaktadır. Etkin bir güvenlik stratejisinin oluşturulabilmesi için siber tehditlerin dinamik doğasının ve hızla gelişen teknolojik altyapının sürekli izlenmesi, açıklıkların ve eğilimlerin analiz

[175] Darıcılı, **a.g.e.,** s. 39-40.

edilmesi büyük önem arz etmektedir. Ne var ki yazılım geliştiricileri, üreticiler, sistem yöneticileri ve son kullanıcılar arasında güvenlik konularına gereken önemin verilmemesi, bu süreci daha da karmaşık hale getirmektedir. İnternet ile siber güvenlik arasındaki ilişki değerlendirildiğinde, iletişim maliyetlerinin düşüklüğü ve internet erişiminin yaygınlığı, bu ortamın diğer elektronik iletişim biçimlerinin yerine geçmesine neden olmuştur. Kritik altyapıların internetle entegrasyonu, siber uzay ile fiziksel dünyanın iç içe geçmesine ve güvenlik açıklarının daha da belirginleşmesine yol açmıştır. Bilgisayar kontrollü altyapıların sayısındaki artış, bu sistemleri saldırılara karşı daha hassas hale getirmiştir. Bu nedenle, saldırganlar açısından bilgisayar tabanlı kontrol sistemleri ve bu sistemlere bağlı fiziksel yapılar cazip hedefler olarak öne çıkmaktadır. Sonuç olarak, siber güvenliğin sağlanması amacıyla hem mevcut sistem açıklıklarının giderilmesi hem de daha güvenli teknolojilerin geliştirilmesine yönelik çabaların süreklilik arz etmesi gerekmektedir. Siber tehditlerin izlenmesi, saldırı eğilimlerinin analiz edilmesi ve bu bilgilere dayalı politikaların üretilmesi, dijital dünyanın sürdürülebilir güvenliği açısından kaçınılmaz bir zorunluluktur.[176]

2001 yılında gerçekleşen ve Dünya Ticaret Merkezi'ni hedef alan 11 Eylül terör saldırıları, ulusal düzeyde kritik altyapılara yönelik saldırıların yaratabileceği yıkıcı etkiler konusunda küresel çapta ciddi endişelere yol açmıştır. Bu saldırılar sonrasında, El-Kaide bağlantılı terörist unsurların eylemi gerçekleştirmeden önce dijital haberleşme ve planlama araçlarını kullanmış olmaları, siber uzayın yalnızca devlet aktörleri arasında değil, aynı zamanda asimetrik tehdit unsurları ile devletler arasında da yeni bir mücadele alanı haline geldiğine ilişkin genel kanaati güçlendirmiştir. Dolayısıyla siber uzay, güvenlik paradigmasında klasik yaklaşımların ötesine geçerek, farklı aktörlerin faaliyet gösterebildiği çok boyutlu ve dinamik bir çatışma zemini olarak değerlendirilmeye başlanmıştır.[177]

Siber tehditlerin kaynakları, bireylerden devlet destekli örgütlü yapılara kadar oldukça geniş bir spektrumda yer almaktadır. Bu aktörler arasındaki sınırların çoğu zaman belirsiz olması, gerçekleştirilen eylemlerin arkasındaki asıl faillerin tespitini güçleştirmektedir. Örneğin, bireysel bir saldırı gibi görünen bir eylem, gerçekte bir devletin istihbarat teşkilatı tarafından gerçekleştirilmiş olabilir. Bu bağlamda, teknolojik

[176] Yılmaz ve Salcan, **a.g.e.,** s. 38-40.
[177] Ekonomi ve Dış Politikalar Araştırma Merkezi, **a.g.e.,** s. 94.

gelişmeleri yakından takip eden, yetkinliklerini sürekli olarak güncelleyen ve faaliyetlerinin kaynağını gizlemekte başarılı olan siber tehdit unsurları, günümüz dijital ortamında ciddi bir güvenlik problemi oluşturmaktadır. Bilgi teknolojilerine olan bağımlılığın giderek arttığı günümüzde, bilgilerin güvenli biçimde işlenmesi, saklanması ve iletilmesinin yanı sıra, kritik altyapıların siber saldırılara karşı korunması da oldukça karmaşık bir hal almıştır. Özellikle internetin yaygınlaşmasıyla birlikte siber güvenliğe yönelik tehditler hızla artmış, bu durum ulusal güvenlik kavramının yeniden ele alınmasını zorunlu kılmıştır. İnternet yoluyla yayılan zararlı yazılımların sıklığında meydana gelen artış bu durumu somut biçimde gözler önüne sermektedir. Örneğin; 1999 yılında her 1400 elektronik postadan biri zararlı yazılım içerirken, bu oran 2001 yılında her 370 mesajda bire yükselmiştir. Bu istatistik, yalnızca kurumsal bilgi sistemlerinin değil, aynı zamanda bireysel kullanıcıların da tehdit altında olduğunu açıkça ortaya koymaktadır. Bu bağlamda dikkat çeken örneklerden biri, 2005 yılında Kaliforniya'da yaşayan 21 yaşındaki Robert Lyttle'ın, çeşitli Amerikan federal kurumlarının bilgisayar sistemlerine izinsiz erişim sağlayarak gerçekleştirdiği saldırılardır. Lyttle'ın, Savunma Bakanlığı'na bağlı Savunma Lojistik Bilgi Sistemleri, Sağlık İşleri Ofisi ve NASA'nın Ames Araştırma Merkezi gibi kurumların sistemlerine sızdığı ve elde ettiği bilgileri bazı web sitelerini sabote etmek amacıyla kullandığı tespit edilmiştir. Bu örnek, yeterli bir donanıma sahip olmayan birinin dahi az bile olsa teknik bilgiye ve motivasyona sahip olduklarında, yüksek güvenlikli sistemlere zarar verebilecek kapasitede olduklarını ortaya koymaktadır. Dolayısıyla siber uzaydaki güvenlik açıkları yalnızca maddi zararlarla sınırlı kalmamakta, aynı zamanda kamu kurumlarının işleyişini ve ulusal güvenlik yapısını da tehdit edebilmektedir.[178]

"Hacker" terimi, köken itibarıyla bilgisayar teknolojileri alanında uzmanlık sahibi bireyleri tanımlamak amacıyla kullanılmaktadır. Ancak zamanla bu kavram, özellikle medyada ve popüler söylemlerde, kötü niyetli yazılım faaliyetlerinde bulunan bireyleri ifade etmek üzere kullanılmaya başlanmış ve bu bağlamda içeriksel bir dönüşüm geçirmiştir. Bugün günlük dilde, hacker kavramı yaygın biçimde kötü niyetli siber saldırganlar için kullanılmakta olup, bu kullanım biçimi akademik literatürde de giderek yer bulmaktadır. Hackerlar, bireysel olarak hareket edebildikleri gibi örgütlü yapılar hâlinde de faaliyet gösterebilmektedirler. Gerçekleştirdikleri siber saldırılar, teknik

[178] Yılmaz ve Salcan, **a.g.e.,** s. 49-51.

düzeyde çeşitlilik göstermekte olup, bu eylemlerin ardındaki motivasyonlar da farklılık arz etmektedir. Söz konusu motivasyonlar kimi zaman teknik merak ya da kişisel tatmin amaçlı iken, kimi zaman belirli ideolojik ya da politik hedefleri gerçekleştirmeye yönelik olabilmektedir. Siber güvenlik literatüründe hackerlar, etik yaklaşımlarına ve davranış biçimlerine göre, çeşitli alt gruplara ayrılmaktadır. En yaygın sınıflandırma; beyaz şapkalı (etik hackerlar), siyah şapkalı (kötü niyetli hackerlar) ve gri şapkalı (hem etik hem etik dışı yöntemleri kullanabilen) olmak üzere üç ana kategoridir. Bazı kaynaklarda ise, bu gruplara kırmızı ve mavi şapkalı hackerlar gibi daha özel nitelikler de eklenmektedir. Tüm bu gruplar arasında, özellikle sistem açıklarını tespit eden ve bu açıkların kapatılmasına dolaylı olarak katkı sağlayan hackerların, bilgi güvenliğinin gelişimine katkı sunduğu söylenebilir. Zira hackerlar tarafından keşfedilen sistemsel zafiyetler, bilgi güvenliği uzmanları tarafından analiz edilerek ortadan kaldırıldığında, ilgili sistemlerin daha sağlam ve güvenli bir yapıya kavuşması sağlanmaktadır. Dolayısıyla, her ne kadar bazı hacker faaliyetleri yasa dışı nitelik taşısa da bu durum siber güvenlik sistemlerinin evrimsel gelişiminde rol oynamaktadır.[179]

Dünya genelinde yaygın olarak gözlemlenen ve sıkça başvurulan siber saldırı teknikleri arasında oltalama (phishing), kötücül yazılımlar (malware), botnetler, hizmet engelleme saldırıları, Denial of service (DoS), DDoS ve sosyal mühendislik saldırıları bulunmaktadır. Ayrıca, kötücül yazılım türleri arasında yer alan Truva atı (trojan), virüsler, solucanlar ile reklam amaçlı ve casus yazılımlar da dikkat çekmektedir.[180] Siber silahlar ile ilgili bir diğer önemli tartışma, bu araçların stratejik silahlar sınıfına dâhil edilip edilmeyeceği meselesidir. Siber silahların yapısal özelliklerinin ve işleyiş biçimlerinin kapsamlı biçimde kavranması, devletler açısından kritik bir öneme sahiptir. Stratejik silahlar, yüksek yıkıcı güçleri, psikolojik terör ve korku unsurları ile dengede dehşet yaratma potansiyeline sahip karmaşık niteliklerle tanımlanmaktadır. Kritik ulusal altyapılar, finans ve bankacılık sistemleri, hassas iletişim ağları ile internet kullanımını kapsayan geniş bir hedef yelpazesinin bulunması, siber silahları geleneksel silahlara kıyasla daha tehditkâr ve korkutucu hale getirmektedir.[181]

[179] Köksoy, **a.g.e.,** s. 11-12.
[180] Eren, **a.g.e.,** s. 33.
[181] Ekonomi ve Dış Politikalar Araştırma Merkezi, **a.g.e.,** s. 12.

Askerî açıdan değerlendirildiğinde, yüksek profilli bir siber silahın, nükleer silah, biyolojik silah, zaman ayarlı bomba, anti-radyasyon füzesi, özel kuvvetler operasyonları ve hatta Orta Çağ kılıcının belirgin özelliklerini bir arada taşıdığı ifade edilebilir. Bu tür bir siber silah, nükleer silah benzeri bir özellik göstererek, kritik ulusal altyapıya önemli zararlar verebilecek kapasiteye sahiptir. Aynı zamanda biyolojik silahların doğasına benzer şekilde, saldırının tespiti ve saldırganın kimliğinin ortaya çıkarılması için özel istihbarat faaliyetleri gerektirir. Ayrıca, anti-radyasyon füzeleri gibi sinyal izleme yoluyla hedefe ulaşabilir ve ileride yapılacak saldırılar için zemin hazırlayabilir. Zaman ayarlı bombalara benzer biçimde, saldırının gerçekleşme zamanı ve etkisinin ortaya çıkması arasındaki süre, saldırgan tarafından planlanabilir. Gizli ve özel operasyonlara özgü unsurlara sahip olması nedeniyle, siber silahlar özel kuvvetler harekâtlarına da paralellik göstermektedir. Son olarak, caydırıcılık bağlamında değerlendirildiğinde, siber silahların Orta Çağ şövalyesinin kılıcına benzetilmesi mümkündür; zira bu kılıcın etkisi, kalkanla engellenememektedir.[182]

Günümüzde, bireyler savaşın gerçek yüzünü ve beraberinde getirdiği duygusal yükleri doğrudan deneyimleyememekte, dolayısıyla vicdani bir sorgulama yapma imkânından yoksun kalmaktadırlar. Buna ek olarak, gelişen askeri teknolojiler karşısında toplumların eskisine nazaran daha savunmasız ve korunmasız duruma düşmesi, savaşların daha sinsi ve örtülü biçimlerde ilan edilip yürütülmesine olanak tanımaktadır. 21. yüzyıl orduları, bilgi temelli askeri kapasitenin artırılması amacıyla bilimsel araştırmalar gerçekleştirmekte ve elde edilen bulguları silah sistemleri ile operasyonel konseptlere entegre etmeye çalışmaktadır. Bu doğrultuda, komuta, kontrol, komünikasyon, bilgisayar hesaplama, keşif, gözetleme ve istihbarat sistemleri, askeri bilgi üstünlüğünü stratejik bir avantaj haline getirerek, savaşların sonucunu belirlemede kritik bir rol oynamaktadır.[183]

3.1.2.3. Siber Saldırılar ile İnsan Haklarının İhlali

Siber güvenlik, hem yatay hem de dikey düzeyde temel haklarla yakından ilişkili bir kavramdır. Siber ortamda, bireyler ve topluluklar arasında karşılıklı olarak gerçekleşen siber tehditler önemli bir yer tutmaktadır. Ayrıca, bireyler veya gruplar tarafından kamu kurumlarına yönlendirilen saldırılar da siber güvenlik kapsamı içinde ele

[182] Ekonomi ve Dış Politikalar Araştırma Merkezi, **a.g.e.,** s. 20.
[183] Yılmaz ve Salcan, **a.g.e.,** s. 21.

alınmaktadır. Siber güvenlik, milletlerarası insan hakları belgeleri ve anayasal düzenlemelerce korunan bireysel özgürlüklerle doğrudan bağlantılıdır. Özellikle özel hayatın gizliliği, kişilik haklarının korunması, basın özgürlüğü, mülkiyet hakkı, ekonomik özgürlükler, din ve vicdan özgürlüğü, ifade özgürlüğü ile seçme ve seçilme hakkı gibi temel haklar ile siber güvenlik arasında güçlü ve nitelikli ilişkilere rastlanmaktadır.[184]

İnsan hakları alanında gelinen mevcut düzey, haklar bakımından nihai bir nokta olarak değerlendirilmemelidir. İnsan hakları, tarihsel süreç içinde gelişen, günümüzde de devam eden ve muhtemelen gelecekte de gelişmeye devam edecek dinamik bir süreçtir. Devletlerin anayasalarında yer alan insan hakları, devletin yetkilerinin kullanımında belirli doğal sınırlar oluşturmaktadır. Bu özellikleri nedeniyle insan hakları, birçok araştırmacıya göre, felsefi ve ahlaki temellere dayanmakla birlikte, ortaya çıkış sürecinde ve günümüzde de siyasi bir nitelik taşımaktadır. Hak, hukuk tarafından korunan menfaatler bütünü ve hukuk düzenince tanınan bir yetki olarak tanımlanabilir. Her hakkın beraberinde belirli unsurlar gelir; bu unsurlar, hakkın anlam kazanması için zorunludur. Bunlar arasında yetki, talep hakkı ve saygı gösterilme zorunluluğu yer almaktadır. Yetki, hakkın özünü oluşturan bir şeyi yapabilme kapasitesidir; elbette kişi bu hakkını kullanıp kullanmamakta özgürdür. Talep unsuru ise, hak sahibine olumlu ya da olumsuz taleplerde bulunma yetkisi verir. Son olarak saygı gösterme unsuru, hakkın genel veya belirli bir kişiye tanınmasını talep etmeyi ve bu hakkın meşru bir şekilde korunmasını gerektirir. Ayrıca, kazanılan her hak, beraberinde bir yükümlülüğü de getirir; bu yükümlülükler de hak sahibine aittir ve hakkın doğasına göre, olumlu (pozitif) ya da olumsuz (negatif) nitelikte olabilir. Yani birey, bir hakkı kullanırken belirli davranışları yapmakla yükümlü olabileceği gibi, bazı davranışlardan kaçınmakla da yükümlü olabilir. [185]

Siber güvenlik, bireylerden gruplara ve kamusal yapılara kadar geniş bir yelpazede etkili olan karmaşık bir tehdit alanını temsil etmektedir. Kamu kurumları ile kolektif yapıların veri güvenliğinin sağlanması ve ekonomik manipülasyonlara karşı korunması önemli bir konu olmakla birlikte, bireysel hakların siber tehditlere karşı korunması daha kapsamlı ve titiz bir yaklaşımı zorunlu kılmaktadır. Bu bağlamda, kişisel verilerin korunması, ekonomik bilişim suçlarından korunma ve siber ortamda bireysel

[184] Köksoy, **a.g.e.,** s. 381.
[185] Bozkurt, Poyraz ve Erdal, **a.g.e.,** s. 182-183.

özgürlüklerin korunması, insan hakları çerçevesinde değerlendirilmesi gereken temel unsurlardır. Kişisel verilerin korunması ve bilişim suçları alanında önemli akademik çalışmalar ve projeler geliştirilmiş olmakla beraber, siber güvenlik ile insan hakları arasındaki ilişkinin daha derinlemesine incelenmesi gerekmektedir. Bu inceleme, bireyin siber uzaydaki konumunun belirlenmesi, korunması gereken menfaatlerin tespiti, bu menfaatlerin sınırlandırılması ve birey üzerinde uygulanabilecek kısıtlayıcı düzenlemelerin kapsamının belirlenmesini içermelidir. Konunun disiplinler arası niteliği göz önünde bulundurulduğunda, farklı akademik disiplinlerden uzmanların katkılarıyla siber özgürlükler ve ilgili hakların kavramsal çerçevesinin gerçeklere uygun olarak oluşturulması, gelecekteki hukuki uygulamaların meşruiyetinin sağlanması açısından kritik öneme sahiptir.[186]

ABD'nin 1997 yılında gerçekleştirdiği tatbikatta, Ulusal Güvenlik Teşkilatı (NSA) tarafından görevlendirilen 35 saldırgan, devletin bilgi sistemlerine yönelik saldırılar düzenlemiştir. Tatbikat süresince uygulanan tüm savunma önlemlerine rağmen, saldırılar günler boyunca tespit edilememiştir. Saldırganlar, Savunma Bakanlığı'nın kritik bilgisayarlarındaki yüksek standarttaki erişim kontrol mekanizmalarına rağmen, internette halka açık bulunan teknikleri kullanarak büyük başarı elde etmişlerdir. Ayrıca, askeri ağların büyük bir kısmında üst düzey erişim sağlamış, elektronik posta ve telefon iletişimlerini kesintiye uğratmışlardır. Tatbikat sonucunda elde edilen veriler, bu yöntemlerle saldırganların gerçek hayatta Los Angeles, Chicago, Washington ve New York gibi büyük şehirlerin elektrik altyapısını kesebilecekleri; Savunma Bakanlığı'nın iletişim sistemlerini devre dışı bırakabilecekleri ve Deniz Kuvvetleri'ne ait gemilerdeki bilgisayarlara erişim sağlayabilecekleri sonucunu ortaya koymuştur. Bu bulgular, mevcut tehdit ortamının ciddiyetini ve endişe verici boyutlarını açıkça göstermektedir.[187]

Milyarlarca kullanıcısı bulunan sosyal medya platformlarına üye bireylerin temel haklarının, bu platformların ticari yönetişimi kapsamında güvence altına alınması güçleşmektedir. Sosyal medya şirketlerinin kendi iç denetimleri ve bağlı oldukları devletlerin bireysel hakların korunması yönündeki düzenleyici mekanizmaları yetersiz kalmakta; zira bu platformların milletlerarası şirketler olarak bağlı bulundukları ülkeler, ticaret ve vatandaşlık hukuku çerçevesinde denetim yapabilmekte, ancak tüm

[186] Köksoy, **a.g.e.,** s. 389.
[187] Yılmaz ve Salcan, **a.g.e.,** s. 52.

kullanıcıların haklarını eksiksiz şekilde korumakta başarısız olmaktadır. Bu bağlamda, milletlerarası çok kullanıcılı sosyal medya platformlarına ilişkin uluslar üstü denetim mekanizmalarının oluşturulması, temel hakların bireysel düzeyde korunmasında önemli bir gereklilik olarak ortaya çıkmaktadır. Ulusal egemenlik uygulamaları, fiziksel ortamda kara, deniz ve hava sahası sınırları dahilinde belirlenmiş olmakla birlikte, siber uzay olarak adlandırılan hukuksal uygulama alanı, fiziksel sınırları temel alan klasik egemenlik kuramlarının ötesinde yeni teorik yaklaşımlar gerektirmektedir. Bu nedenle, ulusal ve milletlerarası alanların sınırlarının tanımlanması, çağdaş normatif çerçevede yeniden ele alınmaktadır. Siber uzayın sınırlarının net olarak belirlenmemesi ve meşru bir otorite tarafından kontrol edilmemesi, bireysel insan hakları açısından farklı ve karmaşık sonuçlara yol açmaktadır. Ayrıca, siber ortamda bireylerin özel konumları, medeni hukukta düzenlenen komşuluk hukuku ve sınır ihtilafları esaslarına göre, çözümlenememektedir. Siber alanda bireyler arasında sözleşmesel bir ilişki bulunmadığından, borçlar hukukundaki sorumluluk ilkelerinin siber uyuşmazlıklarda etkili çözümler sunması da güç görünmektedir. Ayrıca, bireye yönelik saldırıların ceza hukuku kapsamında suç olarak tanımlanmaması durumunda, kabahatler hukuku ya da maddi ve manevi zararların tazmini konusunda yeni normatif düzenlemelere ihtiyaç duyulmaktadır. Bu karmaşık yapının hukuki olarak korunması zor olmakla birlikte, bireyin sanal ortamda korunması doğrudan kamu düzeninin korunmasıyla bağlantılıdır. Bireyin cep telefonundaki veriler yalnızca özel nitelikte olmayıp, aynı zamanda kamusal içerikler de barındırmaktadır.[188]

İnsan haklarının korunması, BM'nin temel amaçlarından biri olarak ön plana çıkmaktadır. BM Şartı'nın giriş bölümünde ve örgütün amaç ve ilkelerini belirleyen 1. maddesinde bu konu açıkça ifade edilmiştir. Şart'ın giriş kısmında "Biz BM halkları, temel insan haklarına, insan kişiliğinin onur ve değerine, erkeklerle kadınların ve büyük uluslarla küçük ulusların hak eşitliğine olan inancımızı yeniden ilan etmeye karar verdik" ifadesi yer alırken, 1. maddede BM'nin amaçlarından biri olarak "ekonomik, sosyal, kültürel ve insancıl nitelikteki milletlerarası sorunların çözümünde ve ırk, cinsiyet, dil veya din ayrımı gözetmeksizin herkesin insan hakları ve temel özgürlüklerine saygının artırılması ve güçlendirilmesi için milletlerarası iş birliğini sağlamak" gösterilmiştir. Bu hedef doğrultusunda, BM bünyesinde insan haklarının korunmasına yönelik geliştirilen

[188] Köksoy, **a.g.e.,** s. 389-390.

denetim mekanizması ikili bir yapıya sahiptir. Bunlardan ilki, antlaşma temelli usuller olup, hukuki dayanaklarını BM Genel Kurulu tarafından çeşitli tarihlerde kabul edilen antlaşmalardan almaktadır. Söz konusu antlaşmalar, ilgili hak ve özgürlüklerin korunmasını ve geliştirilmesini denetlemek amacıyla bağımsız komiteler oluşturmuştur; günümüzde dokuz komite ve bir alt komite bu usuller çerçevesinde faaliyet göstermektedir. İkincisi ise, BM Şartı'ndan kaynaklanan usullerdir; bunlar, herhangi bir antlaşmayla düzenlenmeyen, doğrudan BM Şartı'na dayanan mekanizmalardır. Bu kapsamda şikâyet usulleri, özel prosedürler ve 2006 yılında İnsan Hakları Komisyonu'nun yerini alan İnsan Hakları Konseyi ile Konsey'in kuruluşuyla uygulamaya konulan evrensel periyodik gözden geçirme mekanizması bulunmaktadır.[189]

İnsan Hakları Evrensel Beyannamesi (İHEB), insan hakları tarihindeki önemli bir dönüm noktası olarak kabul edilmektedir. Farklı hukuki ve kültürel geçmişlere sahip temsilcilerin katkılarıyla hazırlanmış olan bu belge, 10 Aralık 1948 tarihinde Paris'te BM Genel Kurulu tarafından (Genel Kurul Kararı 217 A) tüm halklar ve uluslar için ortak bir başarı standardı olarak ilan edilmiştir. İHEB, temel insan haklarının evrensel düzeyde korunmasını ilk kez sistematik bir biçimde ortaya koymuş ve 500'den fazla dile çevrilerek geniş bir küresel erişim sağlamıştır. Günümüzde, İHEB'nin, milletlerarası ve bölgesel ölçekte geçerli olan yetmişten fazla insan hakları antlaşmasının kabulüne öncülük ettiği ve bu antlaşmaların oluşumuna zemin hazırladığı yaygın bir şekilde kabul görmektedir. Bu yönüyle, Beyanname insan hakları geleneğinin gelişiminde belirleyici bir rol oynamış; ardından gelen insan hakları düzenlemeleri için temel teşkil etmiştir.[190]

Hazırlanan bu belge, BM Genel Kurulu tarafından 10 Aralık 1948 tarihinde kabul edilip ilan edilmiştir. Toplamda 30 maddeden oluşan bu Bildirge'de yer alan hak ve özgürlükler, dört ana kategori altında sınıflandırılmaktadır. Birinci kategori, 1789 Fransız Devrimi'nden itibaren gelenekleşmiş olan klasik bireysel hak ve özgürlükleri kapsamaktadır. İkinci kategoride sosyal haklar yer alırken, üçüncü kategori siyasal haklar ve kamu özgürlüklerini içermektedir. Son olarak, dördüncü kategori ekonomik ve sosyal hakları teşkil etmektedir. Evrensel İnsan Hakları Bildirgesi'nin içeriğinden çok, hukuksal statüsü uzun süredir tartışma konusu olmuştur. Elimizdeki metin, bağlayıcı bir antlaşma veya misak niteliği taşımamakta; BM Genel Kurulu tarafından kabul edilmiş bir bildiri

[189] Doğan, Çakmak ve Aslan (der.), **a.g.e.,** s. 151-152.
[190] Bozkurt, Poyraz ve Erdal, **a.g.e.,** s. 190.

olup, üye devletlerin anayasal onay süreçlerinden geçmemiştir. Bu durum, Bildirgenin üye devletler açısından bağlayıcı bir değer taşıyıp taşımadığı sorusunu gündeme getirmiştir. Hukuksal statüsüyle ilgili tartışmalar sürse de bildirgenin evrensel insan hakları açısından taşıdığı önemin tartışılmaz olduğu kabul edilmektedir. [191]

İnsanlık ailesinin tüm bireylerinin doğuştan sahip olduğu onur ve devredilemez hakların tanınması, özgürlük, adalet ve barışın temel taşıdır. İnsan haklarına yönelik saygısızlık ve küçümseme, insan vicdanında büyük tepkilere yol açmakta ve zulüm ile vahşetin yayılmasına neden olmaktadır. Tüm insanların korku ve yoksulluktan uzak, ifade ve inanç özgürlüğüne sahip bir dünyada yaşama arzusu, insanlığın en yüce ideali olarak kabul edilmektedir. Bu bağlamda, bireylerin zulüm ve baskıya karşı direnmek zorunda kalmamaları için insan haklarının hukukun üstünlüğü ilkesi çerçevesinde korunması zorunludur. Ayrıca milletler arasında dostane ilişkilerin geliştirilmesi teşvik edilmelidir. Bu anlayış doğrultusunda, BM halkları, Antlaşma'da temel insan haklarına, insan kişiliğinin onur ve değerine ve kadınlarla erkeğin eşit haklarına olan inançlarını yenilemiş ve daha geniş bir özgürlük içinde toplumsal ilerleme ile yaşam standartlarının iyileştirilmesini destekleme kararı almıştır. Üye devletler ise, BM ile iş birliği içerisinde, insan haklarına ve temel özgürlüklere evrensel saygının sağlanmasını ve korunmasını taahhüt etmişlerdir. Bu hak ve özgürlüklerin ortak bir anlayışla benimsenmesi, bu taahhüdün tam anlamıyla hayata geçirilmesi açısından büyük önem taşımaktadır. Bu nedenle Genel Kurul, İHEB'yi, toplumun her bireyinin ve organının bu bildiriyi sürekli göz önünde tutarak, eğitim ve öğretim yoluyla bu hak ve özgürlüklere saygıyı teşvik etmeleri; ulusal ve milletlerarası düzeyde ilerici önlemler alarak, hem üye devletlerin halkları arasında hem de bu devletlerin yargı yetkisi altındaki topraklardaki halklar arasında evrensel ve etkili bir şekilde tanınması ve uygulanması için çaba göstermeleri amacıyla, bütün halklar ve milletler için ortak bir başarı standardı olarak ilan etmiştir.[192]

Avrupa İnsan Hakları Sözleşmesi (AİHS), Avrupa Konseyi tarafından hazırlanmış bir milletlerarası belgedir. İnsan haklarına saygıyı temel ilke olarak benimseyen Avrupa Konseyi, bu sözleşmeyi 4 Kasım 1950 tarihinde Roma'da düzenlenen bir toplantıda, üye devletlerin dışişleri bakanları aracılığıyla imzalamıştır. Sözleşmenin yürürlüğe

[191] Çelebi, **a.g.e.,** s. 470-471.
[192] İnsan Hakları Evrensel Beyannamesi, https://www.un.org/en/about-us/universal-declaration-of-human-rights, (Erişim Tarihi: 28.06.2025).

girebilmesi için en az on üye devletin onay belgelerini Avrupa Konseyi Genel Sekreterliği'ne teslim etmesi şart koşulmuştur. Bu şart, 3 Eylül 1953 tarihinde sağlanmış ve sözleşme aynı tarihte yürürlüğe girmiştir. Türkiye ise, sözleşmeyi 10 Mart 1954'te, 6366 sayılı kanunla kabul etmiştir. AİHS'te yer alan hak ve özgürlükler, esasen Evrensel İnsan Hakları Bildirisi'nde belirtilenlerle paralellik göstermektedir. Ancak sözleşme, bildiri kapsamındaki tüm hakları değil, üye devletlerin hiçbir çekince koymaksızın benimseyebileceği ve uygulayabileceği hak ve özgürlükleri düzenleyip koruma altına almayı amaçlamıştır. Evrensel İnsan Hakları Bildirisi ile AİHS arasındaki temel fark, hukuki nitelik ve bağlayıcılık düzeyinde ortaya çıkar. Bildirge, bağlayıcı olmayan bir deklarasyon niteliğinde iken, sözleşme imzalayan ve onaylayan devletler için bağlayıcı bir sözleşme mahiyetindedir. Sözleşmenin birinci maddesi, yüksek akit taraf devletlerin kendi yargı yetkileri altındaki herkes için sözleşmede tanımlanan hak ve özgürlükleri tanıdığını hükme bağlamaktadır. Başvuru hakkı başlangıçta yalnızca taraf devletlere tanınmışken, zamanla gerçek kişiler, hükümet dışı kuruluşlar ve belirli koşullar altında topluluklar da bu hakkı elde etmiştir.[193] Bu çerçevede sözleşmeye taraf bir devletin yetki alanı içinde bulunan hakkı ihlal edilen ve açtığı davada hukuki yarara sahip herkes sözleşmenin kapsamı dahilindedir.[194]

AİHS kapsamında oluşturulan denetim mekanizması, yalnızca Avrupa İnsan Hakları Mahkemesine yapılan başvurular sonucunda devreye girmektedir. Sözleşme, mahkemeye başvuru için iki ayrı yol öngörmektedir. AİHS'nin 33. maddesine göre, her bir taraf devlet, sözleşme ve protokollerinin ihlal edildiğine dair diğer taraflarca ileri sürülen herhangi bir iddiayı gerekçe göstererek mahkemeye başvuruda bulunabilir.[195] Buna devlet başvurusu denilmektedir. Ayrıca bizzat sözleşmeci tarafların vatandaşları da mahkemeye başvuru yapabilmektedir. Buna da bireysel başvuru denilmektedir. Bireysel başvuru hakkını sözleşmeyle düzenlenen hak ve hürriyetlerin ilhak edildiği iddiasıyla sözleşmeci devletin yargı yetkisi içinde bulunan herkes kullanabilir. Yabancılar ve sözleşmeye taraf olmayan bir devletin vatandaşları da bu hakkı kullanabilmektedir. Önemli olan sözleşmeye aykırılık iddiasının sözleşmeye taraf herhangi bir devletin eylem veya işlemlerinden kaynaklanmasıdır.

[193] Çelebi, **a.g.e.,** s. 471-472.
[194] Bozkurt, Poyraz ve Erdal, **a.g.e.,** s. 203.
[195] Bozkurt, Poyraz ve Erdal, **a.g.e.,** s. 204.

Normatif ve maddi koşullar kapsamında, AİHS'in 8. ve 10. maddeleri ile diğer milletlerarası insan hakları belgeleri, örneğin İHEB'nin 12. ve 19. maddeleri, BM Siyasi ve Medeni Haklar Sözleşmesi'nin 17. ve 19. maddeleri ve daha yakın tarihli Avrupa Birliği Temel Haklar Bildirgesi'nin 7., 8. ve 11. maddeleri çerçevesinde tanınan ve koruma altına alınan haklar; ifade özgürlüğü, bilgiye erişim hakkı ve iletişim mahremiyetine dair haklar olarak sıralanabilir. Bu belgelerin, mahremiyet ve ifade özgürlüğünü sınırlandırmadan açıkça güvence altına alması, özellikle küresel iletişim ağı olan internetin temel prensipleriyle uyumlu bir yaklaşımı yansıtmaktadır.[196]

Ulusal ve milletlerarası insan hakları belgelerinde yer alan güvencelerin, bireylerin siber güvenlik alanında etkin biçimde korunabilmesi için ilk olarak sanal anarşinin sona erdirilerek meşru bir otoritenin tesis edilmesi gerekmektedir. Milletlerarası toplum tarafından tanınacak ve meşruiyet kazanacak böyle bir siber güvenlik mekanizması, bireylerin siber saldırılara karşı korunmasını sağlayacaktır. Teknik donanım ve kaynaklar açısından sınırlı kalan bireylerin, geniş ve karmaşık siber ortamda yalnızca bireysel önlemlerle korunması mümkün değildir. Bu nedenle, bireylerin siber uzayın sınırsız alanlarında temel insan hakları çerçevesinde korunmasını temin edecek meşru bir otoritenin BM bünyesinde oluşturulması büyük önem taşımaktadır. Siber güvenlik ile insan haklarının korunması alanında yeni uygulama modelleri ve düzenleyici çerçevelerin geliştirilmesi zorunlu hale gelmiştir. Çünkü bireyler sadece siber saldırganların değil, aynı zamanda aşırı denetim uygulayan kamu kurumlarının hak kısıtlamalarına da maruz kalma riskiyle karşı karşıyadır. Kişisel veriler, banka bilgileri, iletişim gizliliği, sağlık kayıtları, fikri mülkiyet hakları ve bireylerin sanal ortamda gerçekleştirdiği davranışlar hem bireysel hem de örgütsel yapılar tarafından hedef alınmaktadır. Buna ek olarak, ticari kuruluşlar da kişisel verileri rekabet hukukuna aykırı biçimde pazarlama amacıyla kullanabilmektedir. Yerel, ulusal ve bölgesel düzeyde yürütülen iş birlikleri, siber ortamda insan haklarının korunmasında yetersiz kalmaktadır. Devlet ve kurumların yanı sıra, bireylerin temel hakları da siber saldırıların odağı haline gelmiştir. Bu bağlamda, milletlerarası geçerliliğe sahip normatif düzenlemelerin insan hakları kavramsal içeriğine uygun şekilde hazırlanması zorunluluğu doğmuştur. Bu normların demokratik ilkelere uygun biçimde uygulanması ve temel haklara dayalı

[196] Yaman Akdeniz, **Beyaz Kitap**, 1. b, İstanbul: Papatya Yayıncılık, 2003, s. 15-16.

yargısal denetimin bağımsız mekanizmalar aracılığıyla gerçekleştirilmesi gerekmektedir.[197]

3.1.2.4. Siber Saldırılar ve Milletlerarası Güvenlik Sorunu

Son yirmi yıl içerisinde internetin beklenenden çok daha hızlı bir şekilde hayatın her alanında yaygınlaşması, dünya üzerindeki mesafeleri önemli ölçüde kısaltmış ve küresel etkileşimi artırmıştır. Bu gelişme, coğrafi sınırların önemini azaltarak, bilginin neredeyse anlık olarak dünyanın herhangi bir noktasına ulaşmasını mümkün kılmıştır. Başlangıçta siber alanı geç fark eden devletler, günümüzde bu alanın önemini kabul etmekte ve onun ihmal edilemeyecek bir unsur olduğunu açıkça ifade etmektedirler. Savunma, ulaşım, sağlık, istihbarat ve diğer kritik devlet hizmetleri artık büyük ölçüde bilgi ve iletişim teknolojileri aracılığıyla siber ortama taşınmış bulunmaktadır. Siber alanda yaşanan tehditlerin ve güvenlik ihlallerinin artışı, devletleri bu alanda kapsamlı politikalar ve savunma mekanizmaları geliştirmeye yönlendirmiştir. Günümüzde birçok ülke, kritik altyapılarının güvenliğini sağlamak adına ulaşım, sağlık ve istihbarat gibi hizmetlerini dijital platformlara taşımakta ve bu alanlarda koruma stratejileri oluşturmaktadır. [198] Bu alandaki tehditlerin boyutunu gösteren en çarpıcı tarihsel örneklerden biri Nisan 2007 Estonya siber saldırılarıdır. Söz konusu olayda, küresel ölçekte ele geçirilmiş milyonlarca cihazdan oluşan devasa bir botnet ağı kullanılmıştır. Saldırganlar, bu ağ üzerinden eşzamanlı ve koordine bir saldırısı başlatarak ülkenin devlet daireleri, telekomünikasyon altyapısı ve bankacılık sistemi gibi kritik fonksiyonlarını hedef almış ve sistemi işlevsiz hale getirmişlerdir.[199]

Küreselleşmenin etkisiyle ekonomi, sosyal politikalar, siyaset, ideolojik eğilimler, radikal dini hareketler, terörizm, çevresel meseleler, internetin yaygınlaşması ve bilimsel gelişmeler gibi alanlarda yaşanan değişimler dikkate alındığında, güvenlik anlayışlarının köklü bir dönüşüm geçirdiği söylenebilir. Soğuk Savaş sonrası dönemde, küresel ekonomik krizler, yasa dışı göç, etnik ve milliyetçi çatışmaların artışı, salgın hastalıklar ve siber güvenlik alanındaki sorunlar, güvenlik tehditleri arasında yeni odak noktaları olarak öne çıkmıştır. Ayrıca, birey güvenliği özellikle devlet karşısında önem kazanmış,

[197] Köksoy, **a.g.e.,** s. 97.
[198] Köksoy, **a.g.e.,** s. 36-37.
[199] Stephen Herzog, "Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses", **Journal of Strategic Security**, C.4, S.2, 2011, s. 50-51.

toplumsal güvenlik ve çevre güvenliği gibi kavramlar da güvenlik çerçevesine dahil edilmiştir. Geleneksel güvenlik tehditleri olan terörizm, savaş ve organize suçlar ise, dönüşerek yeni biçimlerde ortaya çıkmaya devam etmiştir. Teknolojik gelişmeler de bu dönemde büyük bir ivme kazanmış, özellikle 1980'lerden itibaren BİT'lerle hızla ilerlemiş ve 2000'li yıllarda dünya genelinde yaygınlaşmıştır. Kamu ve özel sektörün elektronik ortamda faaliyetlerini artırmasıyla birlikte yaşamın birçok alanı BİT'lere bağımlı hale gelmiştir. Siber ortam, insanlık için önemli faydalar sağlamakla birlikte, tehdit ve saldırıların hedefi haline gelmiş; can ve mal güvenliğini tehdit eden siber saldırılar nedeniyle zararlar büyük boyutlara ulaşmıştır. Bu gelişmeler, güvenlik anlayışında ciddi değişikliklere neden olmuş ve siber güvenlik konusu, bireylerin, kurumların, devletlerin ve milletlerarası kuruluşların öncelikli gündem maddelerinden biri haline gelmiştir. Bu bağlamda, siber uzay merkezli güvenlik sorunlarının, güvenlik uygulamalarına getirdiği yeni perspektifler ve devletlerin askeri kapasitelerini artırmaya yönelik imkanlar ışığında kapsamlı bir şekilde incelenmesi gerekmektedir.[200]

Bankacılık, perakende, e-ticaret, bilgi teknolojileri, savunma ve imalat gibi çeşitli sektörler, yeni iş olanakları yaratmanın yanı sıra otomasyon sayesinde çalışma ortamlarında önemli kolaylıklar sağlamıştır. Ancak, bilgi teknolojilerinin gelişimi, otomasyonun yaygınlaşması ve dijital hizmetlerin artması, iş süreçlerinde verimliliği artırmakla birlikte, küresel düzeyde çeşitli tehdit ve riskleri de beraberinde getirmiştir. Günümüzde dijitalleşmenin hız kazanmasıyla birlikte siber suç faaliyetlerinde de belirgin bir artış gözlenmektedir.[201] Siber uzay, kötü niyetli aktörlerin artan sıklıkta kötü niyetli siber faaliyetler ve operasyonlar yoluyla ittifakların istikrarını bozma çabaları nedeniyle sürekli bir tartışma konusu olmuştur. Potansiyel düşmanlar, kritik altyapılara zarar vermek, devlet hizmetlerine müdahale etmek, istihbarat elde etmek, fikri mülkiyet haklarını ihlal etmek ve askeri operasyonları engellemek gibi amaçlarla faaliyet göstermektedirler. [202] Bakıldığında siber saldırıların amacı aslında bu hedeflere ulaşmaktır.

Dünya genelinde internet kullanıcılarının bölgesel dağılımına ilişkin değerlendirme yapıldığında, toplam nüfus oranına göre, Asya bölgesi %55,1 ile en yüksek

[200] Darıcılı, **a.g.e.,** s. 28-29.
[201] Köksoy, **a.g.e.,** s. 455.
[202] NATO, https://www.nato.int/cps/en/natohq/topics_78170.htm, (Erişim Tarihi: 28.06.2025).

kullanıcı oranına sahiptir. Bunun %17,2 ile Afrika, %10,7 ile Avrupa ve %8,5 ile Latin Amerika ve Karayipler izlemektedir. Daha düşük oranlarla ise, Kuzey Amerika %4,7, Orta Doğu %3,3 ve Okyanusya/Avustralya %0,5 seviyelerinde yer almaktadır. 2000 ile 2020 yılları arasındaki internet kullanıcılarındaki büyüme oranları incelendiğinde, Afrika %11.567 gibi olağanüstü bir artışla en yüksek büyümeyi kaydetmiş, ardından %5.477 ile Orta Doğu, %2.411 ile Latin Amerika ve Karayipler, %1.970 ile Asya, %592 ile Avrupa, %279 ile Okyanusya ve Avustralya ve %223 ile Kuzey Amerika gelmektedir.[203]

Siber uzayda yaşanan teknolojik yenilikler, milletlerarası aktörlerin saldırı ve savaş stratejilerini doğrudan şekillendirmiştir. Son yıllarda bu alandaki hızlı teknolojik gelişmeler ve gelecekte bu ivmenin artarak devam edeceği beklentisi, büyük güçlerin kendi çıkarlarını koruma amaçlı tedbirlerini hızlandırmalarına yol açmıştır. Ayrıca, siber uzayın askeri güç artırımı için yeni bir fırsat olarak görülmesi, devletler arasındaki siber rekabeti yoğunlaştırmakta ve milletlerarası sistemdeki güvensizliği derinleştirmektedir. Bu bağlamda, askeri ve ekonomik açıdan güçlü devletler, siber alanda kendilerini savunmasız hissetmekte ve siber kapasitelerini geliştirmeye odaklanmaktadır. Devletler, güvenliği "kazanılmış değerlerine yönelik tehditlerin ortadan kalkması hali" olarak algılayarak, bu değerleri koruma amacıyla askeri güçlerini artırma gerekliliğini rasyonel bir yaklaşımla benimsemektedirler. Bu durum, siber uzaya yönelik artan ilgiyi ve alandaki yatırımları beraberinde getirmektedir. Öte yandan, siber uzaydaki gelişmelerin milletlerarası sistemi daha kaotik ve anarşik bir yapıya dönüştürdüğü; tehditlerin kaynağının belirsizleşmesi, yapısının, zamanının ve şeklinin tahmin edilemez hale gelmesi gibi boyutları, önceki bölümlerde ayrıntılı biçimde ele alınmıştır. Bu karmaşık ortamda devletler, güç toplamaya ve ulusal çıkarları doğrultusunda kullanmaya devam etmektedir. Bu anarşik yapıda, devletler kendilerini askeri güçlerine güvenmek ve bu gücü yeterli düzeyde tutmak zorunda hissetmektedir. Dolayısıyla, askeri kapasitenin artırılmasına olan ilginin yükselmesinde siber uzayın sunduğu yeni fırsatlar önemli bir rol oynamaktadır.[204]

2010 yılında İran'ın nükleer tesislerine yönelik olarak Stuxnet adlı gelişmiş bir zararlı yazılımın fiziksel hasara yol açtığı olay dikkate değerdir. Sonraki analiz ve değerlendirmeler, bu operasyonun İsrail ve ABD istihbarat birimleri tarafından

[203] Köksoy, **a.g.e.,** s. 444.
[204] Darıcılı, **a.g.e.,** s. 57-58.

planlanmış, hibrit nitelikte yıkıcı bir saldırı olduğunu göstermiştir. Stuxnet virüsünün geliştirilmesi, doğası gereği gizlilik içinde yürütülen bir faaliyettir. Virüs, gizli iletişim yöntemleriyle yürütülen kapsamlı keşif süreçlerinin ardından, önceden belirlenmiş istihbarat elemanları aracılığıyla, muhtemelen taşınabilir bir depolama aygıtı kullanılarak hedef nükleer tesislere bulaştırılmıştır. Bu operasyon, hem klasik istihbarat teknikleriyle personel teminini hem de siber kabiliyetleri kullanarak sabotaj gerçekleştiren elemanların yönetimini içermesi bakımından hibrit bir yapıya sahiptir. Operasyonun planlama ve uygulama aşamalarındaki sofistike ve hibrit karakteri göz önünde bulundurulduğunda, elde edilen başarı ve yarattığı etki açısından ilgili istihbarat servisleri açısından yüksek düzeyde etkili olduğu söylenebilir.[205]

Siber güvenlik, son dönemde ulusal ve milletlerarası güvenlik ile istikrarın temel unsurlarından biri haline gelmiştir. Günümüzde birçok devletin ulusal güvenlik stratejilerinde siber güvenlik önemli bir yer tutmakta, aynı zamanda milletlerarası çatışma ve savaş analizlerinde de siber çatışma ve siber savaş örneklerine sıkça rastlanmaktadır. Siber saldırılar, düşük maliyetleri, yüksek etkinlikleri ve faillerinin tespitinin zorluğu nedeniyle milletlerarası ilişkilerde yaygın olarak tercih edilen bir yöntem halini almıştır. Bu tür saldırılar, yol açtıkları zarar ve tahribat ile milletlerarası arenada caydırıcılık işlevini giderek artırmaktadır. Örneğin, 2007 yılında Estonya'ya yönelik gerçekleştirilen DDoS saldırıları, 2010'da İran'a uygulanan Stuxnet virüsü, İsrail'in Suriye'ye düzenlediği siber operasyonlar ve 2016 ABD seçimlerine Rusya'nın müdahalesi iddiaları, siber güvenliğin milletlerarası ilişkiler açısından ne denli kritik bir konu olduğunu göstermektedir. Bu saldırılar ayrıntılı olarak incelenmekten ziyade, milletlerarası ilişkiler üzerindeki etkilerini ortaya koymak amacıyla kısaca ele alınacaktır. Özellikle Estonya'ya yönelik saldırı, siber güvenlik alanında milletlerarası ilişkilerde ilk önemli uyarı niteliği taşıyan olaylardan biridir ve hatta ilk örnek olarak kabul edilebilir. Yaklaşık bir ay süren bu saldırı, dünyanın en dijitalleşmiş ülkelerinden birinde günlük yaşamı felç etmiştir. Bu olay, özellikle Batı dünyasında (Avrupa ve ABD) siber güvenliğin ulusal güvenlik açısından önemini artırmış ve bu konuda farkındalık yaratılmasına katkıda bulunmuştur.[206]

[205] Darıcılı, **a.g.e.,** s. 231.
[206] Köksoy, **a.g.e.,** s. 14-15.

Hizmet engelleme (DoS ve DDoS) saldırıları, sistemlerin işleyişini engellemeyi hedefleyen siber saldırı türleridir. DoS saldırısında amaç, hedef sistemin kapasitesini aşarak hizmetin aksamasına veya tamamen durmasına neden olmaktır. Bu saldırı genellikle iki aşamada gerçekleşir: İlk aşamada sistem içine yerleştirilen zararlı programlar kullanılırken, ikinci aşamada hazır araçlar devreye sokulur. Buna karşılık, DDoS saldırısı, birçok farklı kaynaktan eş zamanlı olarak yapılan koordineli saldırılardır. Her iki saldırı türünün ortak amacı, hedef sistemde sunulan hizmetin kesintiye uğraması ya da tamamen devre dışı kalmasıdır. Hizmet engelleme saldırıları, teknik olarak birer hacking yöntemi olmamakla birlikte, etkili uygulandıklarında hedef sistemler üzerinde ciddi zararlar verebilirler. Örneğin, 2016 yılında Facebook, WhatsApp, Instagram, Twitter ve Reddit gibi popüler sosyal medya platformlarında yaşanan erişim problemleri, DDoS saldırılarının ne kadar etkili olabileceğinin somut göstergelerindendir. Aynı şekilde, 2017 yılında Türkiye'de banka ve kurumların web sitelerine yönelik DDoS saldırıları sonucunda bu platformların hizmetlerinde yavaşlama ve geçici erişim kesintileri meydana gelmiştir. Bu saldırıların etkisini daha iyi anlamak için şöyle bir örnek verilebilir: Bir sunucu, aynı anda 7000 isteğe cevap verebilecek kapasiteye sahipse, bu sınır aşıldığında, örneğin 7001. istekle beraber sistemin kapasitesi zorlanır ve sonraki her talep sistemin performansını düşürür veya tamamen hizmet dışı kalmasına yol açar. DoS saldırılarında bu aşırı yük tek bir kaynaktan gelirken, DDoS saldırılarında çok sayıda farklı noktadan eş zamanlı olarak gerçekleştirilir. Böylece DDoS saldırıları, çok daha karmaşık ve zorlu bir müdahale süreci gerektirir.[207]

Hizmet engelleme saldırıları, günümüzde bilişim sistemlerinin erişilebilirliğini hedef alan en yaygın siber tehditlerden biri olarak öne çıkmaktadır. Bu saldırı türlerinde temel amaç, hedef alınan resmi kurum veya şirketlerin bilgi iletişim altyapılarını işlevsiz hale getirerek sunulan hizmetlerin kesintiye uğramasını sağlamaktır. DoS ve DDoS yöntemleri, sistemlerin normal işleyişini bozmak ve kullanıcıların hizmetlere erişimini engellemek üzere farklı tekniklerle uygulanmaktadır.[208]

Edward Snowden, 2004 yılında NSA'da güvenlik uzmanı olarak görev yapmaya başlamıştır. Daha sonra CIA ile bağlantılı olarak bilişim uzmanı pozisyonunda çalışmış, 2007 yılında diplomatik bir görevle Cenevre'ye gönderilmiş ve burada 2009 yılına kadar

[207] Ertuğrul, **a.g.e.,** s. 292-293.
[208] Eren, **a.g.e.,** s. 51.

görevini sürdürmüştür. 2009'da CIA ile olan ilişkisini sonlandıran Snowden, NSA'ya bağlı özel şirketlerde çalışmaya devam etmiş ve bu şirketlerden biri olan Booz Allen Hamilton'un Hawaii ofisinde görev yaparken, The Guardian gazetesi muhabiri Glenn Greenwald'a, ABD istihbaratının yöntemlerine ilişkin gizli bilgileri ifşa etmeye başlamıştır. ABD'nin NSA aracılığıyla geliştirdiği siber kapasite sayesinde, yasal bir dayanak olmaksızın hem kendi vatandaşlarının hem de müttefikleri ile düşman olarak görülen ülkelerin vatandaşları, politikacıları ve önemli şahsiyetlerinin internet, cep telefonu ve diğer dijital iletişim kanallarındaki bilgileri izlenmekte ve kayda alınmaktadır.[209]

Julian Assange tarafından yayımlanan Wikileaks belgeleri, iletişim teknolojilerindeki hızlı gelişmenin hem bireylerin hem de devletlerin (özellikle ABD'nin) gizli bilgilerini ifşa etmek amacıyla kullanılabileceğini göstermiştir. Bu belgeler, milletlerarası ilişkiler ve devlet-toplum etkileşimleri açısından ciddi sonuçlar doğurmuştur. Belgelerdeki iddiaların belirli coğrafyalarda yoğunlaşması, içeriklerin belirli amaçlarla seçilerek yayımlandığı izlenimini uyandırmaktadır. Örneğin, Irak Savaşı, Türkiye ve Ortadoğu'ya ilişkin ciddi iddialar yer alırken, İsrail'i zor durumda bırakacak ifadelerin belgelerde yer almaması dikkat çekicidir. Ayrıca, yalnızca "gizli" seviyedeki belgelerin yayımlanması ve "çok gizli" belgelerin bulunmaması da şüphe uyandırmaktadır. Wikileaks olayı, siber güvenlik literatüründe önemli tartışmalar başlatmıştır. Bu skandal, dijital ortamda saklanan bilgilerin gizliliğinin hiçbir zaman tamamen garanti edilemeyeceğini ve sistemdeki insan faktörünün bilgi sızıntılarına yol açabileceğini ortaya koymuştur. Wikileaks, "iletişim teknolojilerinin gelişimi ile devlet-toplum ilişkileri üzerindeki etkisi" ile "devletlerin gizlilik ilkesi" arasındaki ilişkiyi tartışmaya açması bakımından büyük önem taşımaktadır. İnternet tabanlı gazetecilik alanında yeni bir model olarak kabul edilen Wikileaks, günümüzde "savaş, cinayet, tutukluluk, ticaret, şeffaflık, ifade ve basın özgürlüğüne yönelik baskılar, diplomasi, istihbarat, çevre, yolsuzluk, finans, sansür, dini örgütler, şiddet ve suistimal" gibi birçok alana odaklanan "sızıntı gazeteciliğinin en etkili örneğini teşkil etmektedir. Bu yaklaşımı benimseyen yeni nesil gazeteciler, kâr amacı gütmediklerini ve geleneksel medya kuruluşları ile rekabet içinde olmadıklarını savunsalar da söz konusu gazeteciliğin istihbarat servislerinin bilgi akışı ve manipülasyonu olmadan varlığını sürdüremeyeceği

[209] Darıcılı, **a.g.e.,** s. 114-115.

de açıktır. Wikileaks, bilginin bir güç kaynağı olduğunu ve bir devletin elindeki bilgilerin herkes tarafından bilinmesinin o devletin gücünü zayıflatacağını göstermiştir. Bu bağlamda, ABD gibi küresel teknolojik bir gücün, sahip olduğu bilgileri korumakta zorlanması, siber güvenliğin devletlerin varlığını sürdürmesi açısından ne denli kritik olduğunu ortaya koymaktadır. Dolayısıyla, Wikileaks skandalı sırasında ABD'nin dijital sırlarını korumada yaşadığı güçlük, küresel hegemonyasına yönelik bir meydan okuma olarak da yorumlanabilir.[210]

1986 yılında Münih'teki LaBella diskotekinde meydana gelen ve birkaç Amerikalının hayatını kaybettiği bombalama olayı önemli bir güvenlik vakasıdır. Buehler'e göre, NSA Doğu Berlin'deki Libya Halk Bürosu ile Trablus arasındaki şifreli iletişimleri dinlemiş ve saldırının Libya Hükümeti'nin bilgisi ve talimatıyla gerçekleştirildiğini tespit etmiştir. Bu bilgi üzerine Libya'ya yönelik hava saldırıları düzenlenmiştir. İkinci önemli olay ise, İran devrimi sonrası Paris'e kaçan eski İran Başbakanı Şahpur Bahtiyar'ın 1991 yılında Paris'te öldürülmesiyle ilgilidir. NSA, Tahran ile çeşitli Avrupa başkentleri arasındaki şifreli haberleşmeleri dinleyerek İran Hükümeti'nin bu suikastta doğrudan rolü olduğunu açık şekilde ortaya koymuştur. Libya'nın bombalanması ve Bahtiyar suikastının ardından İran'a yönelik uygulanan diplomatik yaptırımlar, İran İstihbarat Servisi'nin NSA tarafından izlendiği gerçeğini kabul etmesine neden olmuştur. Bunun üzerine CRYPTO AG şirketinden bir mühendis, bakım gerekçesiyle İran'a davet edilmiş; Tahran'a varan Hans Buehler tutuklanmış ve uzun süre sonra 3 milyon İsviçre Frangı kefaletle serbest bırakılmıştır. Ülkesine döndükten sonra işinden çıkarılan Buehler, kefalet bedelini ödemek zorunda kalmış ve sonrasında bahsi geçen kitabını yayımlayarak, şifreleme cihazlarının nasıl manipüle edildiğine dair bilgileri ifşa etmiştir.[211]

21. yüzyılda siber uzaydaki gelişmeler ve yenilikler, farklı düzeydeki aktörlere önemli iletişim imkânları sağlarken, aynı zamanda bu paydaşları çeşitli risk ve tehditlerle de karşı karşıya bırakmaktadır. Siber uzay, sunduğu avantajlarla kullanıcılarını bu ortama bağımlı hale getirirken, kötü niyetli aktörlerin de aynı olanaklardan faydalanmasına olanak tanımaktadır. Çünkü bu ortamda, saldırı gerçekleştirmek isteyen bireylerin ihtiyaç duyduğu teknolojik araçlar hem kolay erişilebilir hem de ekonomik açıdan ulaşılabilirdir.

[210] Darıcılı, **a.g.e.,** s. 125-127.
[211] Yılmaz ve Salcan, **a.g.e.,** s. 114.

Siber güvenlik kavramı ise, siyasi ve sosyal bağlamlarda sınırlarının net olarak belirlenememesi sebebiyle oldukça karmaşık ve dinamik bir yapıya sahiptir. Geleneksel güvenlik anlayışının bu alandaki eksiklikleri de bu karmaşıklığı teyit etmektedir. Başlangıçta kişisel cihazlardaki bilgi güvenliği ile özdeşleşen siber güvenlik, günümüzde bireysel düzeyden küresel ölçeğe kadar genişleyen çok boyutlu bir kavram halini almıştır.[212]

Milletlerarası hukuk, esasen anlaşmalar ve milletlerarası teamül gibi temel kaynaklara dayanan, ancak klasik hukuk geleneklerine sıkı sıkıya bağlı kalmak zorunda olan görece genç bir hukuk dalıdır. Bu durum, milletlerarası hukukta meydana gelen değişim ve dönüşümlerin ağır ve uzun soluklu bir süreçte gerçekleşmesine neden olurken, teknolojik gelişmelerin hızla ilerlemesi karşısında esnekliğini sınırlamaktadır. Özellikle 21. yüzyılın ilk çeyreğinde teknolojinin hızlı gelişimi ve küresel ölçekte yaygın kullanımı, milletlerarası hukuk sisteminin siber güvenlik alanında etkin çözümler üretmesini zorlaştırmıştır. Teknolojideki hızlı değişimlere karşın, milletlerarası hukuktaki dönüşümler görece yavaş ilerlemektedir. Bu bağlamda, milletlerarası hukukun teknolojik yeniliklere uyum sağlama yolları, günümüzde bu alanda çalışan akademisyenler tarafından üzerinde durulan önemli araştırma konularından biri olmuştur. Siber güvenlik, hem ulusal hem de milletlerarası düzeyde, yeni kamu düzeninin şekillendirilmesinde kritik bir kavram olarak ön plana çıkmaktadır.[213]

3.2. Siber Egemenlik ve Milletlerarası Düzenlemeler

Siber güvenlik alanında temel sorun, "güvenliği kimin sağladığı" sorusudur. Geleneksel milletlerarası ilişkilerde güvenlik kavramı genellikle devlet güvenliği ile özdeşleştirilirken, siber uzay çok paydaşlı yapısı nedeniyle devlet merkezli olmaktan uzaktır. Bu alanda farklı aktörlerin birbirlerine zarar verme kapasitelerini tespit etmek, ölçmek ve değerlendirmek güçtür; dolayısıyla belirli bir denklikten söz etmek mümkündür. Sonuç olarak, siber uzaydaki güvenlik çeşitli düzeylerde birbirine bağlı ve etkileşim içerisindedir. Bireysel güvenlik kimi zaman bir ulusun güvenliğini etkileyebildiği gibi, bir şirketin güvenliği de küresel güvenlik ortamını şekillendirebilir. Bu sebeple, siber güvenlik konusuna bütüncül bir perspektiften yaklaşmak esastır. Hukuk

[212] Köksoy, **a.g.e.,** s. 18.
[213] Köksoy, **a.g.e.,** s. 382.

ve insan hakları alanlarında diğer paydaşların önceliklendirdiği hususlar, milletlerarası örgütlerin siber yönetişim çalışmalarında daha az vurgulanmaktadır. Ayrıca, bu örgütler tüm paydaşların katılımını teşvik ettiklerini ifade etseler de uygulamada devletlerin karar alma mekanizmalarında öncelikli rol oynamasını; diğer aktörlerin ise, daha çok danışmanlık pozisyonunda kalmasını tercih etmektedirler.[214]

Küresel ölçekte siber güvenlik alanında etkin rol oynayan kurumlar arasında Uluslararası Telekomünikasyon Birliği (ITU) ön plana çıkmaktadır. 1865 yılında kurulan ITU, siber güvenliğe ilişkin yaklaşımını hem aktör hem de çözüm düzeyinde çok boyutlu olarak geliştirmiş; ancak genel olarak teknik altyapının güçlendirilmesine odaklanmıştır. Buna karşın, NATO siber güvenliği, bilgisayarlar ve bilgisayar ağlarının oluşturduğu dijital ortamın korunması ve bu ortamda gerçekleşen çevrimiçi faaliyetlerin sürekliliğinin sağlanması olarak tanımlamaktadır. Bu anlayış doğrultusunda, NATO Güçlendirilmiş Siber Savunma Politikası gibi stratejik adımlar atmış; üye devletlerin öncelikle kendi politika ve stratejilerini oluşturmasını, ardından karşılıklı iş birliğini artırmasını teşvik etmiştir. Ayrıca, hukuki boşlukları gidermek amacıyla iletişim ve koordinasyon mekanizmalarının kurulmasını destekleyerek, siber güvenlik alanında faaliyet gösteren özel sektörle iş birliklerini geliştirmeyi hedeflemiştir.[215] Bunların dışında ayrıca OECD de siber güvenliğe dair birtakım çalışmalar yürütmüştür. OECD kendi içerisinde siber güvenliğe ilişkin bilgi, bilgisayar ve iletişim politikaları komitesi kurmuştur. Komite, bütün ülkeleri kapsayan şekilde siber güvenlik ile ilgili politikalar geliştirmek, istatistikler hazırlamak ve yayınlamak amacı gütmektedir.

3.2.1. Birleşmiş Milletler, Avrupa Birliği, Kuzey Atlantik Antlaşması Teşkilatı gibi Milletlerarası Kurumların Rolü

Milletlerarası örgüt kavramı, en geniş anlamıyla, milletlerarası arenada faaliyet gösteren, ticari amaç gütmeyen ve üç ya da daha fazla devleti kapsayan ancak devlet statüsüne sahip olmayan tüm iş birliği ya da birleşmeleri ifade etmektedir. [216] Milletlerarası ilişkilerin karmaşıklığı ve ortak ihtiyaçların etkili biçimde karşılanma gerekliliği, milletlerarası düzeyde örgütlenmeyi zorunlu kılmıştır. İlk milletlerarası örgütlenmeler, devletlerin egemenlik haklarına müdahale etmeyen ve daha çok teknik

[214] Köksoy, **a.g.e.,** s. 19.
[215] Köksoy, **a.g.e.,** s. 20.
[216] Pazarcı, Uluslararası…, 2021, **a.g.e.,** s. 192.

ihtiyaçlara yönelik alanlarda şekillenmiştir. Devletlerarası örgütlenme düşüncesinin temelleri, fikirsel olarak ilkçağlara kadar uzanmakla birlikte, somut adımların atılması 19. yüzyıla rastlamaktadır. Başlangıçta insani amaçlarla ortaya çıkan örgütlenme çabaları, I. Dünya Savaşı sonrasında insanlığın evrensel barış özlemi doğrultusunda bir dünya devleti idealine yönelmiş ve bu süreçte Milletler Cemiyeti 1919 yılında devletler arasında siyasi bir örgütlenme modeli olarak ortaya çıkmıştır. Ancak, Cemiyetin kuvvet kullanımı konusundaki açık yasaklamalardan kaçınması ve bu yetkinin belirli şartlara bağlanması, yapının en zayıf yönleri arasında yer almıştır. Milletlerarası örgütler, devletlerden bağımsız bir hukuki kişiliğe sahip olmakla birlikte, devletlerden farklı olarak belirli bir coğrafi ülkeye ya da vatandaşlık bağıyla bağlı insan topluluğuna sahip değildirler. Milletlerarası örgütler çeşitli şekillerde sınıflandırılabilir; evrensel, bölgesel, siyasal veya teknik nitelikli örgütler bunlar arasında sayılabilir. Genel olarak milletlerarası örgütlerde üyeler, devletlerin gönderdiği temsilciler aracılığıyla temsil edilmektedir.[217]

Milletlerarası örgütler, faaliyetlerinin kapsamı ve küresel etkileri açısından günümüzde devletlerden sonra en önemli aktörler arasında yer almaktadır. Özellikle milletlerarası ilişkiler disiplininde incelenen bu birimlerin yapısı ve yetkileri, büyük ölçüde milletlerarası hukukun kapsamında değerlendirilir. Her bir milletlerarası örgüt, amaçları, örgütlenme biçimi, yetki alanları ve üyelik yapısı gibi çeşitli faktörlere bağlı olarak özgün bir hukuki karaktere sahiptir. Bununla birlikte, tüm milletlerarası örgütlere ortak olan bazı genel nitelikli milletlerarası hukuk kuralları da mevcuttur. Bu kurallar, özellikle milletlerarası örgütlerin devletlerle, birbirleriyle ve diğer milletlerarası aktörlerle olan ilişkilerini düzenlemeye yöneliktir.[218] Milletlerarası örgütler, genel olarak hükümetler arası ve hükümet dışı olmak üzere iki ana kategoriye ayrılmaktadır. Burada milletlerarası örgüt ifadesi ile daha çok hükümetler arası örgütler kastedilmektedir. Hükümet dışı örgütlerin kuruluşu ve ilişkileri daha çok özel hukuka dayandığından, bu tür örgütlerin milletlerarası hukuk kapsamında resmi bir kişiliğe sahip olmadığı kabul edilmektedir. Öncelikle, bir milletlerarası örgütün milletlerarası kişiliğe sahip olup olmadığının belirlenmesi gerekmektedir. Her ne kadar milletlerarası örgütler milletlerarası hukukta tam bir tüzel kişilik olarak kabul edilse de devletler gibi gerçek ve egemen varlıklar değildirler. Bu tür örgütlerin milletlerarası kişilik kazanmalarında belirli

[217] Bozkurt, Poyraz ve Erdal, **a.g.e.,** s. 35-36.
[218] Pazarcı, Uluslararası Hukuk Dersleri…, 1989, **a.g.e.,** s. 104.

unsurlar rol oynar. Özellikle, devletlere benzer şekilde, milletlerarası örgütler de süreklilik gösteren yapılar olarak ortaya çıkarlar. Bu süreklilik ve kurumsallaşma ise, örgütlerin organları aracılığıyla sağlanmaktadır. [219]

1945 sonrası dönemde ve küreselleşmenin ivme kazanmasıyla birlikte, mevcut kaotik yapı yerini küresel çapta kalıcı ve istikrarlı bir barış ve güven ortamına bırakma amacı taşıyan girişimlere bırakmıştır. BM gibi milletlerarası organizasyonlar, bu bağlamda milletlerarası iş birliğini teşvik eden yapılar olarak ortaya çıkmıştır. Ancak aynı süreçte, milletlerarası iş birliğinin ötesine geçerek ekonomik ve siyasi entegrasyonu hedefleyen ulus üstü yapılar da gelişmiştir. Örneğin, BM mevcut devletler arası ilişkiler çerçevesinde dünya sisteminin yapısallaşmasını amaçlarken, ulus üstü oluşumlar bu sınırları aşarak yeni bir modeli inşa etmeyi hedeflemiştir. 1945 sonrası dönemde özellikle ekonomik temelli faaliyetler yürüten birçok ulus üstü yapı, ulus-devletlerin egemenliklerini belirli ölçülerde sınırlamak suretiyle işlev göstermiştir. Bu tür oluşumların en gelişmiş örneği olan AB, siyasal anlamda da ulus üstü bir model olarak öne çıkmış ve egemenlik kavramının geleneksel anlayışını önemli ölçüde dönüştürmüştür. Böylece, ulus-devlet egemenliği kavramı, ilk ortaya konduğu teorik çerçeveden oldukça farklı ve daha karmaşık bir nitelik kazanmıştır.[220]

Bilgisayar ve telekomünikasyon alanlarında yaşanan teknolojik gelişmelerin bilgi akışını küresel ölçekte yaygınlaştırması, önemli dönüşümlere yol açmıştır. Bu tür dolaylı etkiler, milletlerarası ilişkiler alanında da belirgin yapısal değişimlere neden olmuştur. Bu bağlamda hem gerçek hem de tüzel kişilikler, giderek artan bir şekilde milletlerarası hukukun öznesi hâline gelme eğilimi göstermektedir. Milletlerarası düzeydeki bu dinamik gelişmeler sonucunda ise, yeni milletlerarası örgütlenmelere ve bu örgütlenmeleri düzenleyecek hukuki normlara olan ihtiyaç her geçen gün daha da belirginleşmektedir.[221]

3.2.1.1. Birleşmiş Milletler (BM)

BM'nin milletlerarası güvenlik bağlamında enformasyon ve telekomünikasyon alanlarındaki gelişmeleri değerlendirmek üzere kurduğu Hükümet Uzmanları Grubu

[219] Bozkurt, Poyraz ve Erdal, **a.g.e.,** s. 137-138.
[220] Beriş, **a.g.e.,** s. 200-201.
[221] Akıl, **a.g.e.,** s. 73.

(HUG), BM Genel Kurulu'nun Birinci Komitesi altında faaliyet göstermektedir. 1956 yılından itibaren daimî statüye sahip olan Birinci Komite, BM Genel Kurulu bünyesindeki altı temel komiteden biridir ve Genel Kurul'un tek sözlü kayıt tutan ana komitesi olma özelliğini taşımaktadır. Birinci Komite, silahsızlanma ile milletlerarası güvenlik konularında gündem oluşturma yetkisine sahiptir. Nükleer, kimyasal, biyolojik ve kitle imha silahlarının yayılmasının engellenmesi, uzayın silahsızlandırılması ve uzaydaki silahlanma yarışının önüne geçilmesi gibi kritik alanlarda kayda değer başarılar elde etmiştir. Aynı zamanda, milletlerarası siber güvenlik tehditlerinin tartışıldığı en üst düzey forum olarak da işlev görmektedir. Son yirmi yılda, Birinci Komite; devletlerin siber alanda sorumlulukları, güven artırıcı önlemler ve kapasite geliştirme için gerekli norm, kural ve ilkeleri dikkate alarak siber güvenlik konusunu kapsamlı bir biçimde ele almış ve bu alanda özel çalışmalar yapmak üzere HUG'un kurulmasına zemin hazırlamıştır.[222]

BM Genel Kurulu'nun 73/266 sayılı kararı doğrultusunda, Genel Sekreter'e, milletlerarası güvenlik bağlamında devletlerin siber uzaydaki sorumlu davranışlarının geliştirilmesini ele almak üzere bir HUG oluşturulması yönünde çağrıda bulunulmuştur. Söz konusu grup, farklı coğrafi bölgeleri temsil eden 25 üye devletten gelen uzmanlardan teşkil edilmektedir. Bu uzmanlar görevlerini bireysel kapasiteleriyle yürütmekte olup, çalışmalarını teknik bilgi ve deneyimleri çerçevesinde sürdürmektedir. Grubun faaliyet alanı yalnızca teknik değerlendirmelerle sınırlı olmayıp, aynı zamanda Afrika Birliği, AB, Amerikan Devletleri Örgütü, Avrupa Güvenlik ve İş Birliği Teşkilatı ile Güneydoğu Asya Ulusları Birliği Bölgesel Forumu gibi bölgesel örgütlerle iş birliği ve istişare süreçlerini de kapsamaktadır. Bu bağlamda HUG, milletlerarası siber güvenlik mimarisinin güçlendirilmesine katkı sunmak ve devlet davranışlarını milletlerarası normlara uygun hale getirmek amacıyla çok aktörlü bir yaklaşımla çalışmalar yürütmektedir.[223]

Gücün yalnızca devletler arasında ve düzenli savaşlar çerçevesinde değil, aynı zamanda çeşitli aktörler (örgütler, topluluklar gibi) arasında farklı amaçlarla kullanılması, bu konuyu düzenleyen milletlerarası hukukun zaman içerisinde değişim geçirmesine,

[222] Eldem, **a.g.m.,** s. 360.
[223] United Nations, Hükümet Uzmanları Grubu, https://disarmament.unoda.org/group-of-governmental-experts/, (Erişim Tarihi: 28.06.2025).

kapsamının genişlemesine ve farklı şekillerde yorumlanmasına yol açmıştır. Burada "güç kullanımı" veya "silahlı kuvvet kullanımı" kavramları, esas olarak klasik (konvansiyonel) silahlarla gerçekleştirilen faaliyetleri ifade etmektedir.[224]

BM Şartı'nın 2. maddesinin 4. fıkrası, milletlerarası ilişkilerde güç kullanımını düzenleyen temel hukuki ilkeyi teşkil etmektedir. Bu hükme göre, tüm üye devletler, diğer devletlerin toprak bütünlüğüne veya siyasal bağımsızlığına yönelik doğrudan ya da dolaylı herhangi bir güç kullanma tehdidinde bulunmaktan veya kuvvet uygulamaktan kaçınmakla yükümlüdür. Ayrıca, bu yasak, BM'nin amaçlarıyla çelişen herhangi bir biçimde kuvvet kullanılmasını da kapsamaktadır.

BM Şartı Madde 2

"Birleşmiş Milletler örgüt ve üyeleri, 1. maddede belirtilen amaçlara ulaşmak üzere aşağıdaki ilkelere uygun biçimde hareket edeceklerdir:

1. Örgüt, tüm üyelerinin egemen eşitliği ilkesi üzerine kurulmuştur.

2. Tüm üyeler, üyelik sıfatından doğan hak ve çıkarlardan tümünün yararlanmasını sağlamak için işbu Antlaşmaya uygun olarak üstlendikleri yükümlülükleri iyi niyetle yerine getirirler.

3. Tüm üyeler, uluslararası nitelikteki uyuşmazlıklarını, uluslararası barış ve güvenliği ve adaleti tehlikeye düşürmeyecek biçimde, barışçı yollarla çözerler.

4. Tüm üyeler, uluslararası ilişkilerinde gerek herhangi bir başka devletin toprak bütünlüğüne ya da siyasal bağımsızlığa karşı, gerek Birleşmiş Milletlerin amaçları ile bağdaşmayacak herhangi bir biçimde kuvvet kullanma tehdidine ya da kuvvet kullanılmasına başvurmaktan kaçınırlar.

5. Tüm üyeler, örgütün işbu Antlaşma gereği giriştiği tüm eylemlerde örgüte her türlü yardımı yaparlar ve Birleşmiş Milletler tarafından aleyhinde önleme ya da zorlama eylemine girişilen herhangi bir devlete yardım etmekten kaçınırlar.

[224] Doğan, Çakmak ve Aslan (der.), **a.g.e.,** s. 55.

6. Örgüt, Birleşmiş Milletler üyesi olmayan devletlerin de, uluslararası barış ve güvenliğin korunmasının gerektirdiği ölçüde bu ilkelere uygun biçimde hareket etmesini sağlar.

7. İşbu Antlaşmanın hiçbir hükmü, Birleşmiş Milletlere herhangi bir devletin kendi iç yetki alanına giren konulara müdahale yetkisi vermediği gibi üyeleri de bu türden konuları işbu Antlaşma uyarınca bir çözüme bağlamaya zorlayamaz; ancak, bu ilke VII. Bölümde öngörülmüş olan zorlayıcı önlemlerin uygulanmasını hiçbir biçimde engellemez."[225]

BM Genel Kurulu, 1990 yılında kabul ettiği 45/121 sayılı "Suçların Önlenmesi ve Suçluların Değerlendirilmesi" kararında, Sekizinci BM Suçların Önlenmesi Kongresi'nin önerilerini onaylamıştır. Bu öneriler arasında özellikle bilgi akışının düzenlenmesi ve toplanması, ayrıca devletlerin bilgisayar teknolojilerinin istismarıyla etkin biçimde mücadele etme çağrısı öne çıkmaktadır. 2000'li yıllara gelindiğinde, siber suçlarla mücadele kapsamında çeşitli resmî girişimlerin artış gösterdiği görülmektedir. Bu doğrultuda, 1998 yılında RF tarafından sunulan bir karar taslağının ardından, 2000 yılında düzenlenen BM 55. Genel Kurulu oturumunda kabul edilen 55/63 sayılı karar önemli bir adım teşkil etmiştir. Bu kararda, bilgi ve iletişim teknolojilerinin suç amacıyla kullanılmasının önlenmesine yönelik birtakım önlemler ortaya konmuştur. Söz konusu önlemler arasında; devletlerin bilgi teknolojilerinin suistimaline karşı etkili yasal düzenlemeler ve uygulamalar geliştirmesi, milletlerarası soruşturmalarda adli iş birliğinin sağlanması, siber suçlarla mücadelede koordinasyonun artırılması, ilgili personelin eğitimi, bilgi sistemlerinin gizliliği, bütünlüğü ve erişilebilirliğinin korunması ile bu sistemlerin kötüye kullanımının cezai yaptırımlara tabi tutulması gibi hükümler yer almaktadır. Ayrıca, kamuoyunun bu tehditlere karşı bilinçlendirilmesi ve bireysel özgürlüklerin korunması gerekliliği de vurgulanmıştır. Devamında, 2001 yılında düzenlenen 56. Genel Kurul oturumunda kabul edilen 56/121 sayılı karar, bilgi teknolojilerinin suç amaçlı kullanımının önlenmesine ilişkin süregelen çabaların bir parçası olarak ortaya çıkmıştır. Bu kararda, siber tehditlerle mücadelede yalnızca BM'nin

[225] Birleşmiş Milletler Antlaşması, https://inhak.adalet.gov.tr/Resimler/SayfaDokuman/2212020141836bm_01.pdf, (Erişim Tarihi: 28.06.2025).

değil, aynı zamanda milletlerarası ve bölgesel örgütlerin de önemli roller üstlenmesi gerektiği ifade edilmiştir. [226]

BM Genel Kurulu'nun 2002 yılında gerçekleştirdiği 57. Oturumu sonucunda kabul edilen 57/239 sayılı kararla birlikte, küresel düzeyde bir siber güvenlik kültürünün inşası hedeflenmiştir. Kararda, yalnızca hükümetlerin değil, aynı zamanda özel sektör temsilcilerinin ve bireysel kullanıcıların da bilgi teknolojilerine artan derecede bağımlı hâle geldiği vurgulanmıştır. Bu doğrultuda, siber güvenliğin yalnızca teknik çözümlerle sağlanamayacağı, toplumun tüm kesimlerini kapsayan bütüncül bir güvenlik yaklaşımına ihtiyaç duyulduğu belirtilmiştir. Alınan kararda; milletlerarası kuruluşlar, özel sektör ve bireylerin, bilgi ve iletişim teknolojilerinin kötüye kullanımının önlenmesinde aktif rol üstlenmeleri gerektiği ifade edilmiştir. Ayrıca söz konusu kararda, küresel bir siber güvenlik kültürünün oluşturulmasına katkı sağlayacak dokuz temel unsur belirlenmiştir. Bu unsurlar; farkındalık yaratma, sorumluluk bilinci, etkili müdahale, etik değerler, demokratik ilkeler, risk analizleri, güvenlik odaklı tasarım ve uygulamalar, güvenlik yönetimi ve düzenli değerlendirme süreçleridir. Karar kapsamında, üye devletler 2003 yılında Cenevre'de ve 2005 yılında Tunus'ta gerçekleştirilecek Dünya Bilgi Toplumu Zirvesi'ne katılmaya davet edilmiş ve siber güvenlik kültürünün geliştirilmesine destek vermeleri talep edilmiştir. Bir yıl sonra, 2003 yılında gerçekleştirilen 58. Oturum neticesinde kabul edilen 58/199 sayılı karar, "Küresel Siber Güvenlik Kültürünün Geliştirilmesi ve Kritik Bilgi Altyapılarının Korunması" başlığını taşımakta ve önceki kararların devamı niteliğindedir. Bu kararda, bilgi ve iletişim teknolojilerindeki hızlı gelişmelerin yalnızca teknik değil, aynı zamanda ekonomik ve siyasi yapılar üzerinde de dönüştürücü etkiler yarattığı vurgulanmıştır. Özellikle enerji üretimi, iletimi ve dağıtımı, bankacılık ve finansal hizmetler, elektronik ticaret, su temini, gıda dağıtımı ve kamu hizmetleri gibi hayati öneme sahip sektörlerin, bilgi sistemlerine olan bağımlılıklarının arttığı ve bu durumun beraberinde yeni güvenlik tehditlerini doğurduğu ifade edilmiştir. Kararda ayrıca, kritik bilgi altyapılarının maruz kalabileceği olası hasar ya da saldırı durumlarında, zararın boyutunu sınırlayacak ve sistemlerin en kısa sürede işler hâle gelmesini sağlayacak önleyici tedbirlerin alınması gerekliliği vurgulanmıştır. Tehditlerin

[226] Köksoy, **a.g.e.,** s. 402-403.

tanımlanması, güvenlik açıklarının azaltılması ve risklerin yönetilmesine yönelik kapsamlı stratejilere duyulan ihtiyaç açıkça ortaya konmuştur.[227]

2004 yılında gerçekleştirilen BM Genel Kurulu'nun 59. Oturumunda kabul edilen "Uluslararası Güvenlik Bağlamında Bilgi ve Telekomünikasyon Alanındaki Gelişmeler" başlıklı 59/61 sayılı karar, bilgi teknolojilerinin ve bunlara ilişkin araçların yaygınlaşmasının, milletlerarası toplumun ortak çıkarları üzerinde önemli etkiler doğurduğunu ortaya koymuştur. Kararda, bu alandaki bilimsel ve teknolojik ilerlemelerin hem askerî hem de sivil alanlarda dikkate değer sonuçlar doğurduğu vurgulanmakta; özellikle sivil amaçlı kullanımın teşvik edilmesinin önemine işaret edilmektedir. Karar, milletlerarası bilgi güvenliğinin güçlendirilmesinde çok taraflı iş birliğinin ve eş güdümün artırılması gerektiğini ortaya koymuştur. Aynı yıl alınan 58/32 sayılı kararla, hükümet temsilcilerinden oluşan bir uzman grubunun kurulması ve bu grubun, milletlerarası bilgi güvenliği bağlamında bilim ve teknolojinin rolünü, özellikle askerî ve sivil uygulamaların teşvikine ilişkin hususları ele alan bir rapor hazırlayarak 60. Oturumda sunması öngörülmüştür. Ancak, bu grup üyeleri arasında görüş birliği sağlanamadığından dolayı sadece prosedürel nitelikte bir rapor sunulabilmiştir. Bu gelişmelerin ardından, 2008 yılında düzenlenen 63. Oturumda kabul edilen 63/37 sayılı kararla birlikte, bilgi ve telekomünikasyon teknolojilerinin milletlerarası güvenliğe etkisi yeniden gündeme alınmıştır. Bu karar doğrultusunda, 2009 yılında coğrafi temsil adaletine dikkat edilerek yeniden yapılandırılacak bir Hükümetler arası Uzmanlar Grubu oluşturulması kararlaştırılmıştır. Bu grubun temel görevleri arasında, mevcut ve muhtemel bilgi güvenliği tehditlerine karşı iş birliği yapılabilecek alanları değerlendirmek; bilgi güvenliği alanında bilimsel ve teknolojik gelişmeler ışığında mevcut kavramsal çerçeveleri gözden geçirmek ve tüm bu çalışmaları temel alarak hazırlayacakları raporu 65. Oturuma sunmak yer almıştır.[228]

BM Genel Kurulu, 2010 yılında gerçekleştirdiği 65. Oturumda kabul edilen 65/201 sayılı karar kapsamında, Hükümetler arası Uzmanlar Grubu tarafından hazırlanan raporu değerlendirmiştir. Raporda, BİT'lerin milletlerarası güvenlik üzerindeki etkileri kapsamlı biçimde ele alınmış; özellikle bu teknolojilerin kullanımındaki artışın, kritik altyapılar açısından yeni güvenlik açıkları ve olası kesintilere zemin hazırlayabileceği

[227] Köksoy, **a.g.e.,** s. 403-404.
[228] Köksoy, **a.g.e.,** s. 404.

belirtilmiştir. Telekomünikasyon sistemleri ile internet arasındaki karmaşık ilişkilerin, BİT araçlarının kötüye kullanım açısından hem kaynak hem de hedef haline gelmelerine neden olabileceği vurgulanmıştır. 21. yüzyılda bu tür siber tehditlerin devletlerin güvenliği için önemli sınamalar yarattığı ifade edilmiştir. Bu kapsamda, yalnızca devletler arasında değil, devletlerle birlikte özel sektör ve sivil toplum kuruluşları arasında da iş birliğinin güçlendirilmesi gerektiği dile getirilmiştir. Milletlerarası bilgi güvenliğinin etkin biçimde sağlanabilmesi için çok taraflı ve kapsamlı iş birliği mekanizmalarının oluşturulmasının zorunluluğu ön plana çıkmıştır. Öte yandan, 1998 yılında RF tarafından BM gündemine taşınan bilgi güvenliği konulu taslak önerilere, başta ABD olmak üzere bazı ülkeler karşıt tutum sergilemiştir. Ancak 2010 yılına gelindiğinde, özellikle Stuxnet saldırısı ve Wikileaks belgeleri gibi siber tehditlerin yarattığı etkiler doğrultusunda ABD'nin bu konudaki politikası değişmiş; ülke, söz konusu taslağa eş-sponsorluk yaparak destek vermeye başlamıştır. Bu gelişmeyle birlikte, ABD, Çin ve Rusya ile ortak çalışmalar yürütmeyi kabul etmiş ve bilgi güvenliği alanında milletlerarası diyaloğu güçlendirme yönünde adımlar atılmıştır. 2013 yılı alınan 68/252 sayılı kararda ise, bilgi güvenliği ihlalleri sonucu ortaya çıkan riskler değerlendirilerek bu risklerin giderilmesine yönelik önlemlerin 2013–2014 dönemine ilişkin BM bütçesi bağlamında planlanması gerektiği belirtilmiştir.[229]

Söz konusu on bir maddeden beşi, bağlayıcı nitelikteki sınırlayıcı normları içermekte; kalan yedisi ise, milletlerarası güvenliğin güçlendirilmesine yönelik iyi uygulamaları ve olumlu sorumlulukları tanımlayan ilkelere işaret etmektedir. BM Genel Kurulu, Aralık 2015 tarihinde HUG tarafından hazırlanan raporu oy birliğiyle kabul etmiş ve bu belgenin, üye devletlerin siber teknolojileri kullanırken yol gösterici bir çerçeve olarak benimsenmesini tavsiye etmiştir.[230]

BM Genel Kurulu'nun 2015 yılı aralık ayında kabul ettiği HUG raporunda, milletlerarası güvenlik çerçevesinde bilgi ve iletişim teknolojilerinin kullanımına ilişkin normların oluşturulduğu gözlemlenmektedir. Raporun III. bölümünde yer alan 13. madde kapsamında, devletlerin uyması beklenen sınırlayıcı kurallar ile teşvik edici ilkeler açıkça ifade edilmiştir. Bu bağlamda, sınırlayıcı normlar arasında; devletlerin kendi topraklarında yer alan siber teknolojilerin milletlerarası hukuka aykırı faaliyetler için

[229] Köksoy, **a.g.e.,** s. 404-405.
[230] Eldem, **a.g.m.,** s. 364.

kullanılmasına izin vermemesi (madde 13/c); kritik altyapıya yönelik kasıtlı zarar verici veya işleyişi engelleyici siber eylemlerde bulunmaktan veya bu tür faaliyetleri desteklemekten kaçınmaları (madde 13/f); tedarik zinciri güvenliğini temin etmeye yönelik gerekli önlemleri almaları, zararlı yazılım ve gizli işlevlerin yayılmasını önlemeye çalışmaları (madde 13/i) bulunmaktadır. Ayrıca devletlerin, diğer devletlerin acil müdahale birimlerinin bilişim sistemlerine zarar verici faaliyetlere katılmaması ya da bu faaliyetleri desteklememesi ve bu birimlerin kötü niyetli eylemlerde araç olarak kullanılmaması (madde 13/k); nihayetinde ise, dijital alanda insan haklarına, özellikle ifade özgürlüğü ve gizlilik haklarına, saygı göstermeleri (madde 13/e) gerekmektedir. Aynı maddenin devamında ise, olumlu görevleri yansıtan ilkeler yer almaktadır. Devletler, zararlı siber faaliyetlerin önlenmesine yönelik iş birliğini güçlendirmeli (madde 13/a); siber olayların kapsamı, bağlamı ve sonuçları dahil tüm yönlerini dikkate alarak değerlendirme yapmalıdır (madde 13/b). Bilgi değişimi, karşılıklı yardımlaşma ve siber suçlara karşı ortak mücadele için mekanizmalar geliştirmeli (madde 13/d); kritik bilgi altyapılarını korumak adına gerekli adımları atmalı (madde 13/g) ve bu yapılara yönelik tehditler karşısında yardım taleplerine uygun yanıtlar vermelidir (madde 13/h). Ayrıca, siber güvenlik açıklarının sorumlu şekilde bildirilmesini teşvik etmeli, bu açıkların bertaraf edilmesine yönelik bilgileri paylaşmalı ve küresel güvenlik kültürünün gelişimine katkı sağlamalıdırlar (madde 13/j). Söz konusu normların geliştirilmesinde Rusya'nın öncülüğünü yaptığı girişim çerçevesinde, HUG ile benzer yetkilere sahip olan ve tüm BM üyesi devletlere açık bir yapı olarak tasarlanan Açık Uçlu Çalışma Grubu (AUÇG) kurulmuştur. Bu grubun farkı, yalnızca hükümetler arası değil, aynı zamanda özel sektör, sivil toplum ve akademi temsilcilerinin de katılımına olanak tanımasıdır. AUÇG'nin çalışma gündeminde, mevcut ve muhtemel tehditlerin değerlendirilmesi; milletlerarası hukuk, kurallar, normlar ve ilkelerin uygulanması; kurumsal diyalogun sürdürülmesi güven artırıcı önlemlerin belirlenmesi ve kapasite geliştirme yer almaktadır. Grup çalışmalarına 3-4 Haziran 2019 tarihlerinde başlamış; Eylül ve Aralık 2019'da farklı oturumlar gerçekleştirmiştir. Nihai toplantılar Şubat ve Temmuz 2020'de yapılmış ve 75. Genel Kurul kapsamında Eylül 2020'de son rapor sunulmuştur. Rapor, devletlerin ve devlet dışı aktörlerin siber ortamı, kritik altyapıya, sivillere, demokratik sistemlere ve ekonomik rekabete yönelik tehdit olarak kullanma eğiliminde olduğunu ortaya koymuştur. Bu doğrultuda, raporda tüm devletlere, siber uzayda sorumlu davranış

sergilenmesi ve kurallara uymayan aktörlerin sorumlu tutulabilmesi için iş birliği yapılması çağrısı yapılmıştır.[231]

BM, küresel ölçekte siber güvenliğin sağlanması ve sürdürülebilirliğini temin etmek amacıyla çeşitli programlar ve paneller düzenlemektedir. Bu kapsamda, BM Üst Düzey Dijital İş Birliği Paneli ilk toplantısını 24-25 Eylül 2018 tarihlerinde gerçekleştirmiştir. Siber güvenlik alanında öne çıkan etkinliklerden biri 2020 yılında gerçekleştirilen Dijital Mavi Kasklar (Digital Blue Helmets) Programı ile BM Üst Düzey Dijital İş Birliği Paneli olmuştur. Dijitalleşme süreci, bireylerin günlük yaşamını kolaylaştıran pek çok yeniliği beraberinde getirmiştir; ancak bu durum aynı zamanda dijital güvenlik açısından yeni riskleri de ortaya çıkarmıştır. Günümüzde internet üzerinden insan ticareti, siber saldırılar, siber casusluk faaliyetleri ve terör örgütlerinin çevrim içi insan kazanımı gibi tehditlerin arttığı gözlemlenmektedir. Bu tehditlerin önüne geçebilmek amacıyla geliştirilen Dijital Mavi Kasklar Programı, BM bünyesinde siber güvenlik uzmanlığını güçlendirmeyi hedeflemektedir. Program, siber tehditlere karşı hızlı bilgi paylaşımını ve etkili müdahaleyi kolaylaştıracak ortak bir dijital platformun oluşturulmasını amaçlamaktadır. Ayrıca, BM'nin yürüttüğü misyonların siber tehditlerden nasıl etkilendiğine ilişkin sürekli analizler yaparak, bu tehditlere yönelik koruyucu ve karşı koyucu tedbirlerin koordinasyonunu sağlamak da programın temel hedefleri arasında yer almaktadır.

Siber güvenliğin etkin bir biçimde sağlanabilmesi, yalnızca teknik önlemlerle değil, aynı zamanda güvenlik açıklarından kaynaklanan tehditleri, saldırıları, riskleri ve sorunları kavrayabilen, eğitimli ve bilinçli bir topluluğun oluşturulmasıyla mümkündür. Bu doğrultuda, Dijital Mavi Kasklar Programı'nın temel hedeflerinden biri, dünyanın farklı bölgelerinden siber güvenlik uzmanlarını bir araya getirerek uluslararası düzeyde siber güvenlik destek ve eğitim merkezleri kurmaktır. Program kapsamında, başta BM'in merkezi olan New York olmak üzere, stratejik öneme sahip çeşitli bölgelerde bu merkezlerin oluşturulması ve küresel siber güvenlik kapasitesinin güçlendirilmesi planlanmaktadır. Dijital Mavi Kasklar girişimi, özellikle gıda zincirleri ve tedarik ağlarına yönelik siber tehditler, insan ticareti, siber zorbalık, çocuk istismarı, kritik altyapılara yönelik saldırılar, kurumsal siber casusluk, sosyal medya üzerinden terörist

[231] Eldem, **a.g.m.,** s. 369-370.

devşirme, kimlik hırsızlığı ve finansal siber suçlar gibi alanlarda risklerin azaltılmasını hedeflemektedir. Bu kapsamda, program aracılığıyla yürütülecek araştırmalarla siber tehditlerin tespiti, önlenmesi ve müdahalesine yönelik küresel düzeyde koordinasyonun sağlanması amaçlanmaktadır.

2024 yılı itibarıyla dünya nüfusunun yüzde 60'ından fazlasının internet erişimine sahip olması, dijital alanın benzeri görülmemiş bir hızla genişlemesine neden olmuştur. Bu yoğun bağlantısallık, küresel ölçekte ekonomik, sosyal ve kültürel fırsatları artırmakla birlikte, teknolojik gelişmelerle paralel olarak çeşitlenen siber tehditlerin de artmasına yol açmaktadır. Günümüzde maliyetinin trilyonlarca dolar düzeyinde olduğu tahmin edilen siber suç faaliyetleri, BM Siber Suç Sözleşmesi gibi uluslararası ölçekte koordinasyon gerektiren girişimlerin aciliyetini ortaya koymaktadır. Yeni kabul edilen bu sözleşme, son yirmi yıl içinde müzakere edilip kabul edilen ilk uluslararası ceza adaleti anlaşması olma özelliğini taşımaktadır. BM Siber Suç Sözleşmesi, 25 Ekim 2025 tarihinde Vietnam'ın başkenti Hanoi'de düzenlenen resmî törenle imzaya açılmıştır. Sözleşmenin yürürlüğe girmesi, 40. ülke tarafından onaylanmasından doksan gün sonra gerçekleşecektir. BM Uyuşturucu ve Suç Ofisi verilerine göre, bugüne kadar siber suçlarla ilgili olarak küresel düzeyde üzerinde mutabık kalınmış ve resmen kabul edilmiş bir sözleşme bulunmamaktaydı. Bu nedenle, söz konusu belge siber suçlara yönelik yanıtların daha hızlı, etkili ve eşgüdümlü biçimde verilmesini sağlayarak, hem dijital hem de fiziksel güvenliği güçlendirecek önemli bir hukuki çerçeve sunmaktadır. Sözleşme, yalnızca siber suçlarla mücadele etmeyi değil, aynı zamanda insan haklarını koruyarak dijital alanların güvenli, kapsayıcı ve esnek bir yapıya kavuşturulmasını da amaçlamaktadır. Bu yönüyle, küresel dijital güvenliğe ilişkin benzersiz bir iş birliği platformu ve normatif yapı oluşturmaktadır. Hukuki boyutunun ötesinde, sözleşme kapsayıcılık ve eşitlik ilkelerini ön plana çıkararak, özellikle sınırlı teknik kapasiteye sahip devletlere kapasite geliştirme desteği sağlamayı hedeflemektedir. BM Siber Suç Sözleşmesi, siber güvenliğin yalnızca teknik bir mesele değil, aynı zamanda temel bir insan hakları sorumluluğu olduğunu kabul etmektedir. Bu yaklaşım, dışlanmış toplulukların dijital tehditlerden korunmasını, çevrim içi ortamda özgürlüklerin güvence altına alınmasını ve dijital çağda adil, güvenli ve sürdürülebilir bir siber ekosistemin inşasını teşvik etmektedir.[232]

[232] United Nations, https://www.un.org/en/peace-and-security/basic-facts-about-global-cybercrime-treaty, (Erişim Tarihi: 01.11.2025).

Siber suçlular; finansal kazanç elde etmek, veri ve diğer değerli bilgileri çalmak amacıyla kötü amaçlı yazılımlar, fidye yazılımları ve bilgisayar korsanlığı tekniklerini kullanarak dijital sistemleri istismar etmektedir. Bunun yanı sıra, uyuşturucu, silah ve insan ticareti, kara para aklama ve dolandırıcılık gibi organize suç faaliyetlerinin yürütülmesinde de bilgi ve iletişim teknolojilerinden faydalanılmaktadır. Bu durum, yalnızca ekonomik istikrarı zayıflatmakla kalmayıp, kritik altyapıların işleyişini tehdit etmekte ve dijital dünyaya duyulan güveni ciddi biçimde sarsmaktadır. Geçmişte siber suçlarla ilgili küresel ölçekte üzerinde uzlaşılan ve kabul edilen bir antlaşma metni bulunmamakla birlikte, yeni kabul edilen BM Siber Suç Sözleşmesi bu boşluğu doldurmaktadır. Bu yeni uluslararası belge, siber suçlara yönelik müdahalelerin daha hızlı, daha iyi koordine edilmiş ve daha etkili bir şekilde yürütülmesini sağlayarak hem dijital hem de fiziksel güvenlik ortamını güçlendirmeyi hedeflemektedir. Sözleşmenin kapsamı incelendiğinde, en dikkat çekici yönlerinden biri, çocukların çevrim içi cinsel istismarına karşı özel koruma sağlayan ilk küresel anlaşma olmasıdır. Ayrıca, dijital ortamlarda çocuklara yönelik cinsel istismar veya sömürü içeriklerine ilişkin suçlara karşı mevcut ulusal ve uluslararası koruma mekanizmalarını da genişletmektedir. Siber suçların sınır tanımayan doğası gereği, dünyanın her yerinde bireyler bu suçların mağduru olabilmektedir. Bu bağlamda, sözleşme mağdurların desteklenmesi ve korunmasına özel bir önem atfetmektedir. Belge, mağdurlara yönelik yardım ve koruma faaliyetlerinin teşvik edilmesini; fiziksel ve psikolojik iyileşmeye erişim, maddi tazminat, yasa dışı içeriklerin kaldırılması ve iade süreçlerinin etkin biçimde yürütülmesini öngörmektedir. Bu kapsamda yardım ve koruma tedbirleri, devletlerin ulusal hukuk sistemlerine uygun biçimde uygulanacaktır. Öte yandan, sözleşme yalnızca olay sonrası müdahaleye odaklanmamaktadır. Siber suçlarla etkili mücadele, ancak önleyici yaklaşımların güçlendirilmesiyle mümkün olabilir. Bu nedenle, sözleşme tarafı devletlerden risk azaltma, tehdit yönetimi ve siber güvenlik farkındalığının artırılmasına yönelik önleme politikaları geliştirmeleri beklenmektedir. Böylece, uzun vadede siber suçların ortaya çıkmasını engelleyen sürdürülebilir bir küresel güvenlik ekosisteminin oluşturulması amaçlanmaktadır.[233]

[233] United Nations, https://www.unodc.org/unodc/frontpage/2024/December/five-reasons-why-the-new-cybercrime-convention-matters.html, (Erişim Tarihi: 01.11.2025).

Türkiye Cumhuriyeti adına imza törenine katılan Adalet Bakanı Yılmaz Tunç, BM Siber Suçlara Karşı Sözleşmesi'nin, siber suçların önlenmesi ve cezalandırılmasında uluslararası düzeyde kalıcı, etkin ve sürdürülebilir çözümlerin geliştirilmesine önemli katkılar sağlayacağına inandıklarını ifade etmiştir. Bakan Tunç, dijitalleşmenin getirdiği çok yönlü faydaların yanında, siber suçların da küresel güvenlik, istikrar ve refah açısından ciddi bir tehdit unsuru haline geldiğini vurgulamıştır. Bu tehditlerin sınır aşan yapısına dikkat çekerek, etkili bir mücadele için devletlerin ortak ve koordineli bir yanıt üretmesinin zorunluluğuna değinmiştir. Ayrıca siber suçların yalnızca büyük ekonomik kayıplara yol açmakla kalmadığını aynı zamanda demokrasileri, insan haklarını ve toplumsal güvenliği doğrudan tehdit ettiğini, siber saldırılar, veri ihlalleri, terör, insan ticareti, göçmen kaçakçılığı, çocuk istismarı, uyuşturucu ticareti ve kültürel miras kaçakçılığı gibi sınır ötesi suçlarla mücadele, yeni önlemlerin alınmasını ve uluslararası iş birliğinin güçlendirilmesini zorunlu kıldığını belirtmiştir. Bu kapsamda BM'nin söz konusu sözleşmesinin, devletlere siber suçlarla mücadelede gerekli hukuki çerçeveyi ve iş birliği mekanizmalarını sunduğunu; bu yönüyle de alandaki ilk evrensel ve hukuken bağlayıcı belge olma niteliği taşıdığını belirtmiştir. Türkiye'nin siber uzayın belirli aktörlerin tekelinde kalmaması gerektiğini, bu alanın tüm insanlığın ortak değeri olarak korunmasının önem taşıdığını belirtmiştir. Siber güvenlik ve dijital yönetişim konularında milletlerarası iş birliğinin, devletlerin öncülüğünde ve egemen eşitlik ilkesi temelinde yürütülmesi gerektiğinin altını çizmiştir. Türkiye'nin siber suçlarla mücadele kapsamında birçok ulusal girişimde bulunduğunu, teknik destek ve kapasite geliştirme faaliyetlerini sürdürdüğünü ifade etmiş, bu doğrultuda Siber Güvenlik Başkanlığı'nın kurulduğunu ve ilgili yasal düzenlemelerin hayata geçirildiğini hatırlatmıştır. Türkiye'nin bu sözleşmeye taraf olarak "kurallara dayalı, kapsayıcı ve iş birliğine açık bir dijital düzene olan bağlılığını" yeniden teyit ettiğini belirtmiş ve sözleşmenin Türkiye açısından stratejik öneminin olduğuna değinmiştir. Türkiye'nin bu sözleşmeye imza atması, yalnızca siber suçların önlenmesi, delillendirilmesi ve cezalandırılması alanında uluslararası iş birliğini güçlendirmekle kalmayıp, aynı zamanda küresel ölçekte adil, güvenli ve sürdürülebilir bir dijital düzenin tesisine yönelik kararlılığını da bir kez daha ortaya koyduğunu belirtmiştir.[234]

[234] Anadolu Ajansı, https://www.aa.com.tr/tr/gundem/adalet-bakani-tunc-vietnamda-siber-suclara-karsi-bm-sozlesmesi-imza-toreninde-konustu/3726455, (Erişim Tarihi: 01.11.2025).

3.2.1.2. Avrupa Birliği (AB)

Küreselleşmenin hız kazandığı günümüzde, internet ve dijital teknolojiler hem bireysel hem de kurumsal düzeyde, özel ve kamusal alanlarda yoğun biçimde kullanılmaktadır. İnternet, dijital platformlar, sanal uygulamalar ve genel olarak BİT, yalnızca bireyler arası değil, aynı zamanda siyasi, toplumsal ve kurumsal yapılar arasındaki etkileşimi de kolaylaştıran çok yönlü bir iletişim altyapısı sunmaktadır. Bu teknolojiler, devletlerin yanı sıra sivil toplum kuruluşları ile yerel, bölgesel, ulusal ve milletlerarası düzeyde faaliyet gösteren aktörler için vazgeçilmez bir araç hâline gelmiştir. Bilgi ve iletişim teknolojileri, kullanım alanları itibarıyla sadece iletişimle sınırlı kalmayıp, güvenlikten toplumsal düzene, ekonomiden kamu hizmetlerinin etkinliğine kadar pek çok sektörde temel işlevler üstlenmektedir. Her ne kadar bu teknolojiler devlet yönetimi ve ekonomik yapının dijital dönüşümünde önemli avantajlar sunmakta olsa da aynı zamanda yeni güvenlik risklerini ve kırılganlıkları da beraberinde getirmektedir. Bu durum, siber tehditlerin artan boyutu nedeniyle siber güvenlik alanında ulusal ve milletlerarası düzeyde çeşitli stratejik ve hukuki düzenlemelerin geliştirilmesini zorunlu kılmıştır. Birçok ülke, ulusal siber güvenlik stratejileri oluşturarak bu alanda düzenleyici çerçeveler benimsemiş; bu düzenlemelerle bir yandan bireysel hak ve özgürlüklerin korunması, diğer yandan ise, siber uzay, siber saldırı, siber tehdit ve siber güvenlik gibi temel kavramların tanımlanması hedeflenmiştir. AB, siber tehditlerin Birliğin siyasal, ekonomik ve güvenlik çıkarlarına zarar vermesini önlemek amacıyla çeşitli tedbirler almış; buna karşılık, Birlik düzeyinde siber güvenliğe dair yürütülen faaliyetlerin kurumsal olarak dağınık bir yapı arz ettiği dikkati çekmektedir. Bu çerçevede ilgili bölümde, AB'nin siber güvenlik konusundaki hukuki düzenlemeleri ile bu alanda faaliyet gösteren farklı kurumsal yapıların analizi yapılmaktadır.[235]

Strateji belgesinde, siber suç tekniklerindeki hızlı gelişmeler nedeniyle, kanun uygulayıcı kurumların güncel olmayan operasyonel araçlarla etkin mücadele yürütmesinin giderek zorlaştığı ifade edilmektedir. Belgeye göre, günümüzde AB üyesi tüm ülkelerin siber suçlara karşı yeterince etkili müdahale mekanizmalarına sahip olmadığı görülmektedir. Bu bağlamda, strateji, üye devletlerin etkin ulusal siber suç birimlerine duyduğu ihtiyacın önemini özellikle vurgulamaktadır. Ayrıca, belgede alınan

[235] Köksoy, **a.g.e.,** s. 441-442.

önlemlerin yetersizliğine dikkat çekilmesi, konunun güvenlik perspektifiyle ele alındığını ve aciliyet gerektiren bir sorun olduğunu göstermektedir.[236]

Siber suçlarla etkin bir biçimde mücadele edebilmenin temel koşullarından biri, uluslararası düzeyde adli iş birliğinin sağlanmasıdır. Bu gerekliliğin farkında olan devletler, uluslararası kuruluşlar ve sivil toplum örgütleri, siber suçlara karşı uyumlu ve bütüncül bir mücadele mekanizması oluşturmak amacıyla çeşitli girişimlerde bulunmuşlardır. Bu çabaların sonucu olarak ortaya çıkan hukuki araçlar arasında en dikkat çekeni, Avrupa Konseyi tarafından 2001 yılında kabul edilen "Siber Suçlar Sözleşmesi" (Budapeşte Sözleşmesi) olmuştur. Bu sözleşme, siber suçlarla mücadelede uluslararası iş birliğini kurumsallaştıran ilk ve en kapsamlı hukuki düzenleme niteliğini taşımaktadır.[237]

Sözleşmenin ortaya çıkışı, Avrupa Konseyi Suç Sorunlarına İlişkin Avrupa Komitesi'nin 1996 yılında Avrupa Konseyi'ne, siber suçlarla ilgili özel bir uzman komitesi kurulması yönündeki tavsiyesine dayanmaktadır. Bu öneri doğrultusunda, Avrupa Konseyi Bakanlar Komitesi, Şubat 1997'de "Siber Uzay Suçları Uzman Komitesi" adlı çalışma grubunu oluşturmuştur. Komitenin temel görevi, siber suçların tanımlanması, önlenmesi ve cezalandırılmasına ilişkin kapsamlı bir inceleme yürütmek ve bu doğrultuda bağlayıcı nitelikte bir uluslararası hukuk belgesi taslağı hazırlamaktı. Yaklaşık dört yıllık yoğun bir hazırlık sürecinin ardından, Komite tarafından oluşturulan taslak metin Haziran 2001'de Suç Sorunlarına Dair Avrupa Komitesi tarafından onaylanmış, ardından 8 Kasım 2001 tarihinde Avrupa Konseyi Bakanlar Komitesi tarafından resmen kabul edilmiştir. Siber Suçlar Sözleşmesi 23 Kasım 2001 tarihinde Budapeşte'de devletlerin imzasına açılmış ve gerekli onay sürecinin tamamlanmasının ardından 1 Temmuz 2004 tarihinde yürürlüğe girmiştir. Bu sözleşme, siber suçlarla mücadele alanında uluslararası düzeyde hukuken bağlayıcı ilk anlaşma olarak kabul edilmektedir.

Budapeşte Sözleşmesi'nin temel amaçları üç ana başlık altında özetlenebilir. Birincisi, belirli suçların ortak tanımlarının yapılması yoluyla taraf devletlerin ulusal

[236] Eren, **a.g.e.,** s. 90.
[237] Murat Önok, "Avrupa Konseyi Siber Suç Sözleşmesi Işığında Siber Suçlarla Mücadelede Uluslararası İş Birliği", **Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi**, C.19, S.2, 2013, s. 1232.

mevzuatlarını uyumlaştırmak ve siber suçlara ilişkin kavramsal bir birlik sağlamak; ikincisi, siber suçların soruşturulmasında bilişim ortamının özelliklerine uygun ortak usul ve yetki kurallarını tanımlayarak devletler arasındaki adli süreçlerin yeknesaklığını temin etmek; üçüncüsü ise, geleneksel adli yardımlaşma yöntemlerinin ötesine geçerek, yeni uluslararası iş birliği mekanizmalarını belirlemek ve bu hükümlerin taraf devletlerce uygulamaya hızla geçirilmesini sağlamaktır. Bununla birlikte, sözleşmede bazı yenilikçi yetki düzenlemeleri öngörülmüş olsa da ulusal egemenlik ve mülkilik ilkelerine ilişkin hassasiyetler nedeniyle, Avrupa Konseyi üyesi devletler arasında bu yetkilerin kapsamı konusunda tam bir uzlaşma sağlanamamıştır. Bu durum, klasik adli yardımlaşma anlayışının ötesine geçen uygulamalara dair çekincelerin sürmesine yol açmıştır. Sözleşme dört ana bölümden oluşmaktadır: İlk bölümde, sözleşmede yer alan temel kavramlar ve tanımlar açıklanmaktadır. İkinci bölüm, ulusal düzeyde alınacak hukuki ve kurumsal önlemler üzerine odaklanmaktadır. Bu kapsamda, önce maddi ceza hukuku bakımından belirli suç tipleri (örneğin, bilişim sistemlerine izinsiz erişim, veri müdahalesi, cihazların kötüye kullanımı gibi) tanımlanmakta; ardından ceza muhakemesi hukuku açısından uygulanacak usuli yetkiler ve yargı yetkisinin sınırlarına ilişkin genel ilkeler ortaya konulmaktadır. Bu yapısıyla Budapeşte Sözleşmesi, siber suçlarla mücadelede hem ulusal mevzuat uyumunu hem de uluslararası adli iş birliğini kurumsallaştıran çerçeve bir metin niteliği taşımaktadır.

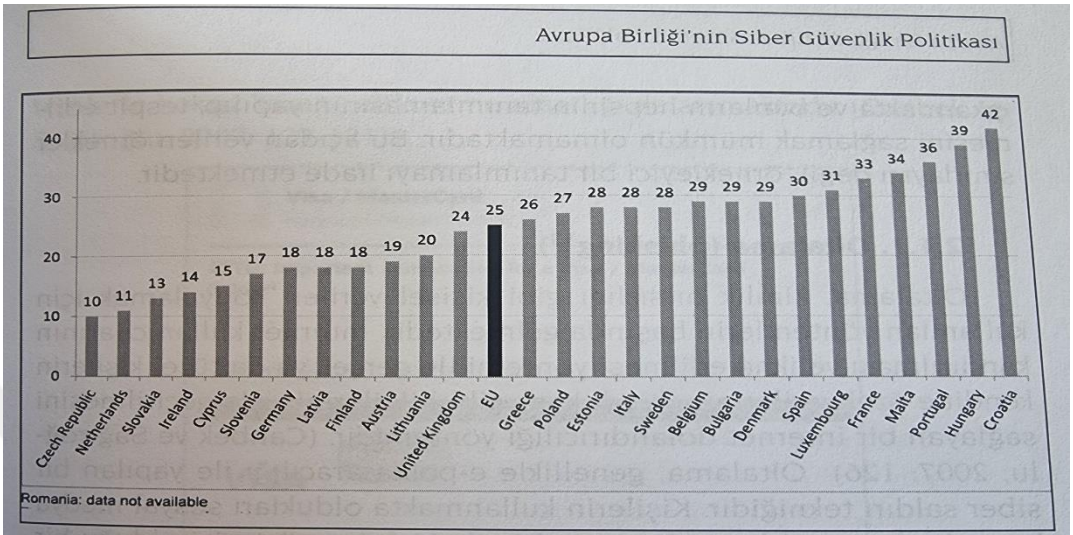
Budapeşte sözleşmesi, internet ve diğer bilgisayar ağları üzerinden işlenen, özellikle de telif hakkı ihlalleri, bilgisayarlarla ilgili dolandırıcılık, çocuk pornografisi ve ağ güvenliği ihlallerinin ele alındığı ilk uluslararası sözleşmedir. Sözleşme aynı zamanda bilgisayar ağlarının araştırılması ve bunlara müdahaleyle ilgili yetki ve usulleri de içermektedir.[238]

Siber suçların yaygınlığı incelendiğinde, birçok AB ülkesinde bu mesele, Ulusal Güvenlik Stratejileri kapsamında organize suç ve dolandırıcılık gibi konularla birlikte en öncelikli üç tehdit arasında yer almaya başlamıştır. Özellikle Fransa, Hollanda ve Birleşik Krallık gibi ülkelerde siber suç, kayıtlar bazında birinci derecede önemli bir tehlike olarak öne çıkmaktadır. Ancak, 2013 yılında Avrupa Parlamentosu için hazırlanan "AB'de Organize Suçların Ekonomik, Finansal ve Sosyal Etkileri" başlıklı raporda, siber suçların

[238] Councıl of Europe, https://www.coe.int/tr/web/impact-convention-human-rights/convention-on-cybercrime#/, (Erişim Tarihi: 01.11.2025).

maliyetine ilişkin yapılan değerlendirmeler tartışmalı bulunmuş ve çeşitli eleştiriler gündeme gelmiştir.[239]

Şekil 2: AB'de Güvenlik Sorunları ile Karşılaşan İnternet Kullanıcısı Yüzdesi (2015)



Şekil 2: AB'de Güvenlik Sorunları ile Karşılaşan İnternet Kullanıcısı Yüzdesi (2015)

Eurostat tarafından AB üyesi ülkelerde gerçekleştirilen bir araştırmaya dayanarak, farklı cinsiyet, yaş ve eğitim düzeylerine sahip internet kullanıcılarının deneyimleri analiz edilmiştir. Elde edilen bulgular, AB genelinde her dört internet kullanıcısından birinin çevrimiçi güvenlikle ilgili sorunlarla karşılaştığını göstermektedir. Şekil 2'de de görülebileceği üzere, en yüksek güvenlik problemleri Hırvatistan (%42), Macaristan (%39) ve Portekiz (%36) gibi ülkelerde yoğunlaşmıştır. Buna karşılık, en az çevrimiçi güvenlik problemi yaşayan ülkeler arasında Çek Cumhuriyeti (%10), Hollanda (%11) ve Slovakya (%13) yer almaktadır. Bu veriler ışığında, AB'nin siber güvenlik alanına verdiği önemin yerinde ve zorunlu olduğu söylenebilir.[240]

AB'nin siber güvenlik politikası ve strateji belgesinin şekillenmesinde, günlük hayatta karşılaşılan örnekler önemli bir rol oynamaktadır. Bu bağlamda, AB'nin strateji belgesi, güvenlikleştirme sürecinin temel yapıtaşlarından biri olarak değerlendirilmelidir. Belgenin hazırlanmasında, AB yetkililerinin açıklamaları, küresel çapta gerçekleşen siber olaylar ve AB'yi doğrudan etkileyen siber saldırılar belirleyici olmuştur. Özellikle Estonya'ya yönelik saldırılar, Alman Parlamentosuna düzenlenen siber saldırılar ve TV5

[239] Köksoy, **a.g.e.,** s. 443.
[240] Eren, **a.g.e.,** s. 35.

Monde olayı, AB için sürekli referans noktaları olarak öne çıkmaktadır. AB vatandaşlarını hedef alan kamuoyuna yönelik açıklamalarda, güvenlikleştirme sürecinde tehdit algısının oluşturulması ve kabul görmesi aşamasında, gündelik yaşamdan örneklerin vurgulandığı görülmektedir.[241]

AB'nin 1990'lı yıllardan itibaren siber güvenlik alanındaki çalışmaları Birlik seviyesine taşıma çabaları gözlemlenmektedir. 1998 yılında, Europol çatısı altında, AB ülkeleri ile üçüncü ülkelerin güvenlik güçleri arasında terörizm ve milletlerarası organize suçlarla mücadele amacıyla iş birliği sağlanmıştır. 2004 yılında AB Siber Güvenlik Ajansı (ENISA) kurulmuş ve ajansın temel hedefi, üye ülkeler arasında siber güvenlik alanında iş birliğini geliştirmek olmuştur. Başlangıçta ENISA, daha çok danışmanlık ve bilgilendirme hizmetleri sunmaya odaklanmıştır. Dijital ekonominin sağlıklı işleyişini temin etmek amacıyla, AB telekomünikasyon altyapısında meydana gelebilecek arızalar ve siber saldırılar karşısında etkin yanıt verebilmek için 2013 yılında AB Siber Güvenlik Stratejisi yayımlanmıştır. 27 Haziran 2019 tarihinde yürürlüğe giren AB Siber Güvenlik Yasası ile birlikte, ENISA'nın yetki ve görev alanları genişletilmiş; aynı zamanda AB genelinde siber güvenlik sertifikasyon sisteminin oluşturulması hedeflenmiştir. Bu kapsamda, Avrupa Belgelendirme Çerçevesi geliştirilerek hem AB vatandaşlarının hem de işletmelerinin güvenilir dijital ürünleri tercih etmesi amaçlanmıştır. Örneğin, "Nesnelerin İnterneti" gibi teknolojilere dayalı ürünlerin siber güvenlik açısından sertifikalandırılması, kullanıcıların günlük hayatta kullandıkları dijital cihazlara olan güvenini artırmıştır.[242]

23 Kasım 1995 tarihinde kabul edilen Verilerin Korunması Direktifi, kişisel verilerin işlenmesi sürecinde bireylerin hak ve özgürlüklerinin korunması ile mahremiyetin sağlanmasını hedeflemiştir. Ayrıca, işlenen kişisel verilerin AB üyesi ülkelerin ulusal sınırları içinde güvenli ve serbestçe dolaşımını mümkün kılacak çerçeve kurallar belirlenmiştir. Direktif, yalnızca gerçek kişilere ilişkin veri işleme uygulamalarını düzenlerken, tüzel kişilere ilişkin hususlar üye devletlerin takdirine bırakılmıştır. Direktifte, kişisel veri, anonim veri, veri işleme ve veri koruma görevlisi gibi temel kavramların tanımlamaları yer almakta; verilerin kalitesi, hukuka uygun

[241] Eren, **a.g.e.,** s. 64-65.
[242] Köksoy, **a.g.e.,** s. 455-456.

işlenmesi ve ilgili kişinin açık rızası ile işlenmesi gibi ilkeler vurgulanmaktadır. Ayrıca, veri işleyenlerin bilgi verme yükümlülüğü, ilgili kişilerin işlenen verileri talep etme hakkı ve haklı sebeplerle veri işlenmesine itiraz etme hakları da düzenlenmiştir. Direktifin 25. ve 26. maddeleri ise, işlenen verilerin AB üyesi olmayan ülkelerle paylaşımı konusunda ayrıntılı düzenlemeler getirmekte; Avrupa Komisyonu, veri transferi yapılacak ülkelerde yeterli veri koruma güvenliğinin sağlandığı kanaatine varmadığı takdirde veri paylaşımına izin vermemektedir. 31 Temmuz 2002 tarihli Elektronik Haberleşme Sektöründe Gizliliğin Korunması Direktifi ise, 1995 tarihli direktifi tamamlayıcı nitelikte olup, bu kez tüzel kişileri de kapsama dahil etmiştir. Bu düzenleme ile elektronik haberleşme alanında temel hak ve özgürlüklere saygı gösterilmesi, özel hayatın gizliliği ve kişisel verilerin korunması amaçlanmıştır. Direktif ayrıca, teknolojik gelişmelerin ortaya çıkardığı yeni koruma gereksinimlerine de yanıt vermiştir. Ticari elektronik iletiler ve istenmeyen e-postalara ilişkin olarak da önceden rıza alınmaksızın gönderilen elektronik mesajların yasaklanması ve doğrudan reklam içeren iletilerde gönderenin kimliğinin gizlenmemesi ile geçerli bir adresin bulunmasının zorunlu kılınması gibi hükümler getirilmiştir. Direktifte, 1995 yılındaki düzenlemede yer alan ancak bu metinde belirtilmeyen konular için önceki düzenlemelerin geçerliliği sürdürülmüştür. 24 Şubat 2005 tarihli AB Konseyi Çerçeve Kararı ise, Birlik genelinde bilgi sistemlerine yönelik siber saldırılarla mücadelede ceza yargılamasının güçlendirilmesi amacını taşımakta, üye devletler arasında iş birliğinin geliştirilmesini hedeflemektedir. Çerçeve kararın 11. maddesi uyarınca, üye devletlerin 7 gün 24 saat hizmet veren operasyonel iletişim noktaları oluşturması zorunlu kılınmıştır. Karar kapsamında, yetkisiz erişim ve sistem engelleme gibi eylemler bilişim suçu olarak tanımlanmış, üye devletler ise, bu tür suçlara karşı caydırıcı, etkili ve orantılı para cezalarını içeren yasal düzenlemeler yapmakla yükümlü kılınmıştır. 15 Mart 2006 tarihli Verilerin Saklanması Direktifi ise, 2002 tarihli düzenlemede değişiklik yaparak, üye devletlerin yasal mevzuatlarında yer alan telefon ve e-posta verilerinin suç soruşturması, tespiti ve kovuşturması amacıyla saklanmasına ilişkin uyumu sağlamayı amaçlamıştır. Söz konusu yasal düzenlemeler, günümüzde güvenlikleştirme sürecinin temel yapı taşları arasında yer almakta ve bu süreçte tehdit algısının tanımlanması ile kamuoyuna kabul ettirilmesi aşamalarında önemli rol

oynamaktadır. Çıkartılan mevzuatlar, tehdidin resmî olarak tanımlanıp kabul edilmesini sağlayarak, önleyici tedbirlerin meşruiyet kazanmasına katkıda bulunmuştur.[243]

AB Siber Güvenlik Stratejisi, 2013 yılında kabul edilmiş olup, dijital ekonominin sürdürülebilir ve güvenli bir şekilde gelişimini desteklemek amacıyla dünyanın en güvenli internet ekosisteminin oluşturulmasını hedeflemektedir. Bu strateji, Birliğin telekomünikasyon altyapılarında meydana gelebilecek arızalar ve siber saldırılar karşısında önleyici tedbirlerin alınması ve etkili müdahale mekanizmalarının geliştirilmesi için hazırlanmıştır. 2013 yılının başında yayımlanan bu strateji iki temel bölümden oluşmaktadır. Birinci bölüm, Avrupa Komisyonu ile AB Dışişleri ve Güvenlik Politikası Yüksek Temsilcisi tarafından ortaklaşa yayımlanan İletişim Belgesini içermekte; ikinci bölüm ise Avrupa Komisyonu'nun Ağ ve Bilgi Güvenliği Direktifi taslağına dayanmaktadır. Bu direktif, Avrupa'nın dijital geleceği açısından en stratejik düzenleyici metinlerden biri olarak kabul edilmektedir. Söz konusu stratejinin temel amacı, AB üyesi devletlerin ve özel sektör kuruluşlarının siber tehditlerle başa çıkma kapasitelerini güçlendirmek ve bu doğrultuda bütün paydaşlar arasında koordineli bir iş birliği kültürü oluşturmak olmuştur. Ayrıca, strateji kapsamında kamu ve özel sektörün siber güvenlik yatırımlarını artırması, bilgi paylaşımı mekanizmalarının güçlendirilmesi ve uluslararası düzeyde siber güvenlik alanındaki iş birliklerinin yoğunlaştırılması teşvik edilmiştir. Bu yaklaşım, AB'nin siber güvenliği yalnızca teknik bir mesele değil, aynı zamanda ekonomik istikrar, toplumsal güven ve siyasi dayanıklılıkla doğrudan ilişkili bir stratejik öncelik olarak gördüğünü açıkça ortaya koymaktadır.

AB, artan dijitalleşme süreciyle birlikte siber güvenlik tehditlerinin Birliğin bütünlüğü ve istikrarı açısından stratejik bir risk unsuru haline geldiğini vurgulamaktadır. Bu çerçevede, 2016 tarihli AB Küresel Stratejisi doğrultusunda yürütülen kamuoyu araştırmalarına göre, AB vatandaşlarının yaklaşık %87'si siber suçları ciddi bir toplumsal sorun olarak değerlendirmektedir. 2016 Küresel Stratejisi, AB'nin siber güvenlik alanında "siber diplomasi" kapasitesini geliştirerek, uluslararası ortaklarının bu alandaki yetkinliklerini güçlendirecek öncü ve vizyoner bir aktör konumuna gelmesini hedeflemektedir. Bu vizyon doğrultusunda, siber savunmaya ilişkin politikalar, aynı yıl kabul edilen AB Savunma Eylem Planı'na dâhil edilmiş ve 2018 yılında Avrupa Savunma

[243] Eren, **a.g.e.,** s. 75-77.

Ajansı'nın öncelikli çalışma alanlarından biri olarak belirlenmiştir. Ayrıca, AB'nin NATO ile yürüttüğü ortak güvenlik girişimleri kapsamında da siber savunma önemli bir iş birliği ekseni haline gelmiştir. Birlik, siber güvenlik konusundaki stratejik kapasitesini yalnızca kendi içinde değil, aynı zamanda BM, Avrupa Güvenlik ve İş Birliği Teşkilatı, OECD gibi çok taraflı kuruluşlarla; ayrıca ABD, Kanada ve Japonya gibi ortak ülkelerle yürüttüğü diplomatik temaslar aracılığıyla da güçlendirmektedir. Bu doğrultuda, 27 Haziran 2019 tarihinde yürürlüğe giren AB Siber Güvenlik Yasası, Birliğin dijital güvenlik mimarisinde dönüm noktası niteliğinde bir düzenleme olmuştur. Söz konusu yasa ile ENISA yeni görev ve yetkiler tanımlanmış; dijital ürünler, hizmetler ve süreçler için AB genelinde geçerli olacak Avrupa siber güvenlik sertifikasyon çerçevesi oluşturulmuştur. Bu düzenleme, siber güvenlik alanında standartlaşmayı, güvenilirliği ve tüketici güvenini artırmayı amaçlayan bütüncül bir Avrupa yaklaşımının kurumsal temelini oluşturmuştur.

3.2.1.3. Kuzey Atlantik Anlaşması Teşkilatı (NATO)

Brüksel'de 2021 yılında gerçekleştirilen NATO Zirvesi'nde müttefikler, NATO'nun üç temel misyonunu ve genel caydırma ile savunma stratejisini destekleyen Kapsamlı Siber Savunma Politikası'nı kabul etmişlerdir. Müttefikler, NATO'nun savunma yetkisinin geçerliliğini tekrar teyit ederek, toplu savunma kapsamında siber tehditlerin tüm spektrumunu aktif şekilde caydırmak, bunlara karşı savunma geliştirmek ve etkili karşılık vermek amacıyla mevcut tüm yeteneklerin kullanılmasına kararlılık göstermişlerdir. Verilecek yanıtların sürekliliği önem taşımakta olup, politik, diplomatik ve askeri araçlar dahil olmak üzere NATO'nun tüm imkanlarının entegre biçimde kullanılması gerekmektedir. Ayrıca, müttefikler, belirli koşullar altında ciddi ve kasıtlı siber faaliyetlerin, Kuzey Atlantik Konseyi'nin NATO Antlaşması'nın 5. maddesi uyarınca vakıa bazlı olarak kolektif savunmayı tetikleyebilecek bir silahlı saldırı olarak değerlendirilebileceğini kabul etmişlerdir. Siber alanın karmaşık yapısı, politik, askeri ve teknik boyutlarda eşgüdümlü çabaları zorunlu kılan bütüncül bir yaklaşımı gerektirmektedir. 2021 yılında kabul edilen politika ve eşlik eden eylem planı, bu üç alandaki faaliyetlerin koordinasyonunu sağlamaya yöneliktir. [244]

[244] NATO, https://www.nato.int/cps/en/natohq/topics_78170.htm, (Erişim Tarihi: 28.06.2025).

Estonya'ya yönelik gerçekleştirilen siber saldırıların milletlerarası ilişkiler alanında önemli etkileri olduğu değerlendirilmektedir:

1. Bu saldırı, siber güvenlik, siber güç, siber uzay ve siber saldırı gibi kavramların milletlerarası ilişkiler analizlerinde derinlemesine incelenmesi için dönüm noktası niteliği

2. RF, 2000'li yılların başından itibaren geliştirdiği siber güvenlik ve savunma stratejileri doğrultusunda, Estonya saldırısıyla birlikte milletlerarası sistemde etkili bir siber güç olarak konumunu güçlendirmiştir. Bu bağlamda, RF'nin siber kapasitesinde Rus İstihbarat Servisleri ile bağlantılı siber kapasiteye sahip suç örgütlerinin önemli rol oynadığı tespit edilmiştir.

3. RF, sahip olduğu bu siber kapasiteyi, özellikle bölgesel dış politika sorunlarında zor kullanma ve baskı aracı olarak kullanmaktan çekinmeyeceğini açıkça göstermiştir.

4. Estonya saldırısı, başta ABD olmak üzere NATO üyeleri tarafından siber alanın sunduğu yeni tehdit algısının şekillenmesine neden olmuş ve bu doğrultuda ABD öncülüğünde NATO'nun ortak bir siber güvenlik stratejisi geliştirmesine yönelik ciddi adımlar atılmaya başlanmıştır. Ayrıca, her NATO üyesi ülke kendi ulusal siber güvenlik stratejilerini oluşturmak için girişimlerde bulunmuştur.[245]

NATO'nun web sunucuları, Eski Yugoslavya Cumhuriyeti askeri personeline bağlı oldukları şüphesiyle NATO kaynaklarınca belirlenen saldırgan gruplar tarafından sürekli olarak hedef alınmıştır. Yaklaşık 100 sunucudan oluşan ve NATO'nun milletlerarası web sitesi ile e-posta trafiğini yöneten altyapı, DoS saldırılarına maruz kalmış ve binlerce zararlı yazılım içeren e-posta ile yoğun şekilde bombardımana tutulmuştur. Bu saldırılar sonucunda bazı NATO sunucuları günlerce faaliyet dışı kalmıştır. Ayrıca, aynı dönemde Eski Yugoslavya Cumhuriyeti hükümet yanlısı Sırp, Rus ve Çin kökenli aktörler, Amerikan askeri, kamu ve ticari internet sitelerine yönelik çok sayıda siber saldırı gerçekleştirmiştir. NATO'nun iletişim altyapısına yönelik bu

[245] Darıcılı, **a.g.e.,** s. 209.

saldırılar hem iç hem de dış iletişimde önemli kesintilere ve hizmet aksaklıklarına yol açmıştır.[246]

2023 yılında Vilnius'ta gerçekleştirilen NATO Zirvesi'nde, müttefikler siber savunmanın ittifakın genel caydırıcılık ve savunma stratejisine katkısını güçlendirmeyi amaçlayan yeni bir konsepti onaylamıştır. Bu yeni yaklaşım, NATO'nun siber savunma faaliyetlerini politika, askeri ve teknik olmak üzere üç düzeyde daha entegre hale getirerek, barış, kriz ve çatışma dönemlerinde sürekli sivil-askeri iş birliği ve gerektiğinde özel sektörle koordinasyon sağlamayı hedeflemektedir. Böylece, ittifakın paylaşılan durumsal farkındalığı artırılarak siber dayanıklılığın güçlendirilmesi, ittifakın genel güvenliğinin artırılması ve siber tehditlerin yol açabileceği zararların etkili biçimde azaltılması amaçlanmaktadır. Vilnius Zirvesi'nde ayrıca müttefikler, NATO'nun Siber Savunma Taahhüdünü yeniden teyit etmiş ve kritik altyapılar da dahil olmak üzere öncelikli alanlarda ulusal siber savunmaları güçlendirmek için yeni ve iddialı hedefler benimsemiştir. Önemli kötü niyetli siber faaliyetlere karşı ulusal düzeyde yapılan azaltma çabalarını desteklemek amacıyla NATO'nun Sanal Siber Olay Destek Yeteneği başlatılmıştır. Müttefikler ayrıca, diğer ülkeler, milletlerarası kuruluşlar, endüstri ve akademi gibi paydaşlarla karşılıklı fayda ve etkinlik temelinde iş birliği geliştirmeyi ve NATO'nun siber uzaydaki milletlerarası istikrar çabalarını ilerletmeyi kabul etmiştir. 2024 yılında Washington'da düzenlenen NATO Zirvesi'nde ise, devlet ve hükümet başkanları, SHAPE bünyesinde kurulan yeni NATO Entegre Siber Savunma Merkezi aracılığıyla ağ koruması, durumsal farkındalık ve siber uzayın barış, kriz ve çatışma dönemlerinde operasyonel bir alan olarak etkin kullanımı yönündeki taahhütlerini dile getirmişlerdir. Ayrıca, NATO ağlarının güvenliğini artırmaya yönelik kapsamlı bir politika geliştirme sözü verilmiştir.[247]

2024 yılında Washington'da gerçekleştirilen NATO Zirvesi'nde, müttefikler, ağ güvenliğini artırmak, durumsal farkındalığı güçlendirmek ve siber alanın operasyonel bir ortam olarak etkin kullanımını sağlamak amacıyla NICC kurulması hususunda mutabakata varmıştır. Ayrıca NATO, siber savunma alanında AB, BM ve Avrupa

[246] Yılmaz ve Salcan, **a.g.e.,** s. 46.
[247] NATO, https://www.nato.int/cps/en/natohq/topics_78170.htm, (Erişim Tarihi: 28.06.2025).

Güvenlik ve İş birliği Teşkilatı gibi milletlerarası kuruluşlarla iş birliğini sürdürmektedir.[248]

NATO müttefikleri, 10 Temmuz 2024 tarihinde, artan karmaşıklığa sahip siber tehditlere karşı daha etkin bir koruma sağlamak amacıyla yeni bir merkezin kurulması üzerinde mutabakata varmıştır. NATO Entegre Siber Savunma Merkezi (NICC), NATO ve müttefiklerin ağlarını koruma kapasitesini güçlendirecek ve siber uzayın operasyonel bir alan olarak kullanımını destekleyecektir. Bu merkez, NATO askeri komutanlarına, askeri operasyonları desteklemek için kritik öneme sahip özel sektöre ait sivil altyapılar da dahil olmak üzere, siber uzaydaki potansiyel tehditler ve güvenlik açıkları hakkında bilgi sağlayacaktır. NICC, NATO girişimi, müttefik ülkeler ve endüstri alanından uzmanlardan oluşan sivil ve askeri personeli bir araya getirerek, gelişmiş teknolojiler aracılığıyla siber uzaydaki durumsal farkındalığı artırmayı ve kolektif dayanıklılık ile savunma kapasitesini geliştirmeyi amaçlamaktadır. Merkez, müttefiklerin ortak değerleri ve milletlerarası yükümlülükleri doğrultusunda, siber uzaya yönelik norm temelli, öngörülebilir ve güvenli bir yaklaşımı teşvik edecektir. Kuruluş, Belçika'daki SHAPE bünyesinde bulunan NATO'nun stratejik askeri karargahında faaliyet gösterecek olup, merkezin yapısına ve işlevlerine ilişkin detaylar önümüzdeki dönemlerde şekillendirilecektir.

Vilnius Zirvesi Bildirisi, 11 Temmuz 2023 tarihinde Vilnius'ta düzenlenen Kuzey Atlantik Konseyi toplantısına katılan NATO Devlet ve Hükümet Başkanları tarafından yayınlanmıştır.

Vilnius Zirvesi Bildirisi madde 66

"Siber uzay, tehdit aktörlerinin giderek artan bir şekilde kötü niyetli siber faaliyetler ve kampanyalar kullanarak İttifakı istikrarsızlaştırmaya çalışmasıyla her zaman tartışmalıdır. Rusya'nın Ukrayna'ya karşı saldırganlık savaşı, siberin modern çatışmanın bir özelliği olduğu ölçüyü vurguladı. Demokratik sistemlerimiz ve kritik altyapımız da dahil olmak üzere önemli, sürekli ve artan siber tehditlere karşı koyuyoruz ve bunların karma kampanyaların parçası olduğu yerlerde de mücadele ediyoruz. Toplu yanıtları da göz önünde bulundurarak siber

[248] NATO, https://www.nato.int/cps/en/natohq/topics_78170.htm, (Erişim Tarihi: 28.06.2025).

tehditlerin tüm yelpazesini caydırmak, savunmak ve bunlara karşı koymak için tüm yetenekleri kullanmaya kararlıyız. Tek bir veya kümülatif kötü niyetli siber faaliyetler kümesi silahlı saldırı seviyesine ulaşabilir ve Kuzey Atlantik Konseyi'nin vaka bazında Washington Antlaşması'nın 5. maddesini uygulamaya koymasına yol açabilir. BM Şartı, uluslararası insancıl hukuk ve uluslararası insan hakları hukuku da dahil olmak üzere uluslararası hukuka uygun hareket etmeye kararlıyız. Özgür, açık, barışçıl ve güvenli bir siber alanı teşvik etmeye devam ediyoruz ve uluslararası hukukun saygı görmesini sağlayarak ve siber alanda sorumlu devlet davranışının gönüllü normlarını destekleyerek istikrarı artırma ve çatışma riskini azaltma çabalarını daha da ileri götürüyoruz. Bugün, siber savunmanın genel caydırıcılığımıza ve savunma duruşumuza katkısını artırmak için yeni bir konsepti onaylıyoruz. Bu, NATO'nun üç siber savunma düzeyini- politik, askeri ve teknik - daha da entegre ederek barış zamanı, kriz ve çatışma sırasında her zaman sivil-askeri iş birliğini ve ayrıca uygun olduğunda özel sektörle etkileşimi sağlayacaktır. Bunu yapmak, ortak durumsal farkındalığımızı artıracaktır. Siber dayanıklılığımızı güçlendirmek, İttifakımızı daha güvenli hale getirmek ve siber tehditlerden kaynaklanan önemli zarar potansiyelini daha iyi azaltma yeteneğine sahip olmak için çok önemlidir. Bugün Siber Savunma Sözümüzü yeniden belirtiyor ve güçlendiriyoruz ve kritik altyapılar da dahil olmak üzere öncelikli olarak ulusal siber savunmalarımızı daha da güçlendirmek için iddialı yeni ulusal hedeflere kendimizi adadık. Önemli kötü niyetli siber faaliyetlere yanıt olarak ulusal azaltma çabalarını desteklemek için NATO'nun yeni Sanal Siber Olay Destek Yeteneği'ni başlattık. Bu, Müttefiklere ek bir yardım aracı sağlar. Ortak ülkeler, uluslararası örgütler, endüstri ve akademi dahil olmak üzere uygun şekilde karşılıklı olarak faydalı ve etkili ortaklıklar geliştirmeye devam ederek siber uzayda uluslararası istikrarı artırma çabalarımızı ilerleteceğiz. Mevcut değişimlerimizi tamamlayarak, bu Kasım ayında Berlin'de ilk kapsamlı NATO Siber Savunma Konferansını düzenleyerek siyasi, askeri ve teknik düzeylerdeki karar vericileri bir araya getireceğiz". [249]

NATO İttifakı'nın güvenliğini tehdit eden siber saldırılar, giderek daha karmaşık, yıkıcı ve yoğun hale gelmektedir. Siber uzay, sürekli olarak değişken ve tartışmalı bir alan olup, basitten teknoloji açısından gelişmiş karmaşık saldırılara kadar her gün çeşitli kötü niyetli siber olaylara sahne olmaktadır. NATO ve müttefikleri, ittifakın kötü niyetli siber faaliyetleri tespit etme, önleme ve etkili şekilde yanıt verme kapasitesini güçlendirmek suretiyle bu tehditlere karşı aktif bir tutum sergilemektedir. İttifak,

[249] Vilnius Zirvesi Bildirisi, https://www.nato.int/cps/en/natohq/official_texts_217320.htm, (Erişim Tarihi: 28.06.2025).

caydırıcılık ve savunma, kriz önleme ve yönetimi ile iş birliğine dayalı güvenlik olmak üzere üç temel görevini yerine getirebilmek için sağlam ve dayanıklı siber savunma sistemlerine dayanmaktadır. Artan karmaşıklığa sahip siber tehditlere karşı ağların ve operasyonların korunması için hazırlıklı olunması zorunludur. Özellikle şu hususlar önem taşımaktadır:

- Siber savunma, NATO'nun caydırıcılık ve savunma görevlerinin ayrılmaz bir parçasıdır.
- NATO'nun siber savunmadaki önceliği; kendi ağlarının korunması, siber alanda operasyon yürütülmesi, müttefiklerin ulusal dayanıklılıklarını artırmalarına destek verilmesi ve siyasi istişare ile kolektif eyleme yönelik platform sağlanmasıdır.
- Temmuz 2016'da müttefikler, NATO'nun savunma yetkisini teyit ederek siber uzayı resmi bir operasyon alanı olarak kabul etmişlerdir.
- NATO, müttefiklerin kötü niyetli siber faaliyetlere ilişkin kaygılarını paylaşmaları, ulusal stratejileri ve müdahale yaklaşımlarını karşılıklı değerlendirmeleri için bir istişare platformu işlevi görmektedir. Müttefikler, siber saldırıların önlenmesi, etkilerinin azaltılması, iyileşme süreçleri ve yanıt mekanizmalarında bilgi alışverişi ve karşılıklı desteği artırmayı kararlılıkla sürdürmektedir.
- Müttefikler, özgür, açık, barışçıl ve güvenli bir siber ortamı teşvik etmekte, milletlerarası hukuk ve gönüllü normlarla uyumlu sorumlu devlet davranışlarını destekleyerek küresel istikrarı sağlamaya ve çatışma risklerini azaltmaya çalışmaktadır.
- 2016'da başlatılan Siber Savunma Taahhüdü, 2023'te kritik altyapılar da dahil olmak üzere ulusal siber savunmaların güçlendirilmesine yönelik daha iddialı hedeflerle yeniden teyit edilmiştir.
- NATO, siber yeteneklerin geliştirilmesi amacıyla eğitim, öğretim ve tatbikat faaliyetlerini kapsamlı şekilde artırmaktadır.

- 2021 yılında kabul edilen Kapsamlı Siber Savunma Politikası, İttifakın dayanıklılığını artırarak temel görevlerine ve genel caydırıcılık ile savunma duruşuna katkı sağlamaktadır.

- 2023 Vilnius Zirvesi'nde müttefikler, siber savunmanın NATO'nun caydırıcılık ve savunma duruşundaki rolünü güçlendiren yeni bir konsepti onaylamış ve kritik kötü niyetli siber faaliyetlere karşı ulusal azaltma çabalarını desteklemek amacıyla NATO'nun Sanal Siber Olay Destek Yeteneği'ni hayata geçirmişlerdir.

Bu gelişmeler, NATO'nun siber alandaki kapasitesini ve iş birliği mekanizmalarını güçlendirerek, İttifakın karşı karşıya olduğu siber tehditlere karşı etkin ve bütüncül bir savunma stratejisi oluşturma yönündeki kararlılığını ortaya koymaktadır.

Soğuk Savaş'ın sona ermesinin ardından NATO, yeni misyonlar belirleme arayışına girerken, BM'de Yugoslavya'daki iç savaşın sonlandırılması amacıyla askerî güce sahip bir müttefik aramıştır. NATO'nun bu görevi üstlenmesi ve devamında Orta ve Doğu Avrupa ülkelerinin ittifaka katılması, NATO'nun varlığını sürdürme yönündeki kararlılığını ortaya koymuş ve bu durum, Varşova Paktı'nın dağılacağını öngören Rusya açısından büyük bir sürpriz teşkil etmiştir. Bu dönüşüm sürecinin resmî başlangıcı, 24 Nisan 1990 tarihinde Washington Zirvesi'nde kabul edilen ilk Stratejik Konsept belgesi olmuştur. NATO'nun en güncel stratejik konsepti ise, 19 Kasım 2010'da Lizbon Zirvesi'nde onaylanmıştır. Lizbon Zirvesi'nde kabul edilen bu belge, önceki 1999 tarihli stratejik konseptten farklı olarak, NATO'nun küresel sorumluluklarını ön plana çıkarmasıyla dikkat çekmektedir; böylece NATO, yalnızca Avrupa-Atlantik bölgesinin güvenliğine odaklanmaktan çıkarak küresel bir aktör konumuna yükselmiştir. Ayrıca, 2010'daki stratejik konseptte, 1999 belgesinde yer almayan siber saldırı tehdidi yeni ve önemli bir güvenlik sorunu olarak vurgulanmıştır.[250]

Türkiye devletinin de NATO ittifakına üye bir ülke olması nedeniyle, NATO tarafın düzenlenen tatbikatlara katılarak iş birliği yapmaktadır. Buna örnek olarak 2025 mayıs ayında siber alanda gerçekleştirilen ve Milli Savunma bakanlığı tarafından açıklanan tatbikattır.

[250] Köksoy, **a.g.e.,** s. 424.

Kilitli Kalkan 2025 Tatbikatı, NATO Siber Savunma Mükemmeliyet Merkezi'nin koordinasyonunda 5-9 Mayıs 2025 tarihleri arasında gerçekleştirilmiştir. Türkiye, uzun yıllardır katıldığı bu tatbikata bu yıl Macaristan Cumhuriyeti ile ortak kurulan Türkiye-Macaristan mavi takımı ile iştirak etmiştir. Sanal bir ağ ortamında düzenlenen ve 40 ülkenin 17 mavi takımıyla katıldığı etkinlikte, Türkiye Mavi Takımı, Genelkurmay Başkanlığı ve Türk Silahlı Kuvvetleri Siber Savunma Komutanlığı önderliğinde görev almıştır. Tatbikat kapsamında, siber varlıklar ve kritik altyapılara yönelik çeşitli siber saldırı senaryoları test edilmiş; Türk Silahlı Kuvvetleri, kamu kurumları ve siber güvenlik sektöründeki firmalarımızın siber yetkinlikleri başarıyla sınanmıştır. Ayrıca, her yıl olduğu gibi bu sene de tatbikatın temel amacı, Siber Vatan'ın korunmasında kritik öneme sahip kurumlar arası bilgi paylaşımı ve koordinasyonun en üst düzeye çıkarılması olmuştur.[251]

NATO'nun etkili bir siber güvenlik politikası uygulamasında karşılaştığı önemli zorluklardan biri, böyle büyük ve kurumsal bir yapının, siyasi liderlerin katılımıyla gerçekleşen zirvelerde alınan kararları pratikte hayata geçirmesinin güçlüğüdür. Ayrıca, milletlerarası örgütler ile üye devletler arasındaki ilişkilerin doğasında bulunan, merkez ile üyelerin eş zamanlı ve uyumlu hareket edememesi nedeniyle NATO ve müttefiklerinin değişim hızları da birbirinden farklılık göstermektedir. Bunun yanı sıra, NATO'ya özgü olmamakla birlikte, siber güvenlik politikasının etkin biçimde işletilememesi, siber saldırıların asimetrik, görünmez ve sürekli evrilen doğasından kaynaklanmaktadır. Bu özellikler, siber tehdidin sürekli izlenmesini zorunlu kılarak yüksek maliyetlere neden olmaktadır. Bilişim teknolojilerindeki gelişmeler, savunma sistemlerinin evrimini tetikleyerek milletlerarası hukukta kuvvet kullanımı ve meşru müdafaa kavramlarıyla ilgili yeni tartışmaları gündeme getirmiştir. Siber saldırı terimi, ne askeri literatürde ne de devletlerin ulusal hukukunda ya da milletlerarası hukuk kaynaklarında kesin ve üzerinde uzlaşılan bir tanıma sahip değildir. Genel kabul, bilişim teknolojileri aracılığıyla yürütülen siber saldırıların asimetrik savaş biçimi olarak değerlendirilmesidir. NATO Antlaşması'nın 5. maddesi, üye devletlerden birine yapılan saldırının tüm üyelere yapılmış sayılacağını belirtmektedir. Bu bağlamda, müttefiklerden birine yönelen silahlı

[251] Kilitli Kalkan-2025 Tatbikatı Basın Duyurusu, https://www.msb.gov.tr/Basin-ve-Yayin/Aciklamalar/2baf4d7de031407e801609e83c11a606, (Erişim Tarihi: 28.06.2025).

saldırı, diğer üyelerin BM Antlaşması'nın 51. maddesine dayanarak bireysel veya kolektif yardımda bulunma yükümlülüğünü doğurmaktadır.[252]

Günümüzde siber saldırıların ortaya koyduğu en önemli gerçek, yalnızca güçlü bir ordunun ulusal gücü temsil etmek için yeterli olmadığıdır. Bilgi ve iletişim teknolojileri, ulusal güç unsuru olarak zorunlu hale gelmiştir. Bu durum, milletlerarası örgütler için de geçerliliğini korumaktadır. NATO'nun Siber Güvenlik Politikası bağlamında değerlendirildiğinde, milletlerarası sistemdeki hızlı dönüşüm ve değişen güvenlik ortamı dikkate alındığında, 2010 yılında kabul edilen stratejik konseptin üzerinden kısa bir süre geçmiş olmasına rağmen tehditler farklılaşmakta ve yeni biçimler almaktadır. Teknolojik gelişmelerin hızı, siber tehditlerin NATO açısından giderek daha ciddi bir sorun haline gelmesini sağlamıştır. Bu bağlamda, NATO sürekli reform ve dönüşüm süreçlerine adapte olmak zorundadır. 1990'larda Avrupa-Atlantik dışını operasyonel alan dışında gören NATO, 70. yıldönümünde siber uzayı artık operasyon sahalarından biri olarak kabul etmektedir. Ancak NATO'nun siber güvenlik politikaları ve hukuk alanındaki ilerlemesi, özellikle ABD'nin gerisinde kalırsa, ne üye müttefikler ne de üye olmayan devletler için yapıcı bir iş birliği platformu oluşturma kapasitesine ulaşabilecektir. Küresel siber güvenlik alanında NATO'nun daha etkin ve öncü bir rol üstlenebilmesi, ancak müttefiklerin bu misyona tam destek vermesiyle mümkün olacaktır. NATO'nun çözüm bulması gereken temel meselelerden biri, siber saldırı, siber terörizm ve siber savaş başlatma eylemlerinin bir devlete hangi koşullar altında atfedilebileceğinin açık ve net sınırlarla belirlenmesidir. Mevcut milletlerarası hukuk normları, BM Antlaşması maddeleri, NATO uygulamaları bu konuda temel bir zemin sağlasa da, bunlar halen yeterli görülmemektedir. Ayrıca, siber uzayla ilgili milletlerarası hukuk ilkeleri oluşturulurken temel insan hakları, özgürlükler ve ölçülülük prensiplerine özellikle önem verilmesi gerekmektedir. Sonuç olarak, NATO'nun etkili bir siber güvenlik stratejisi geliştirmesi için öncelikle siber savunmayı ana savunma alanlarından biri olarak konumlandırması gerekmektedir. Ayrıca, müttefikler arasında sürekli bilgi paylaşımını teşvik ederek iyi uygulama örneklerinin yaygınlaşmasına olanak sağlamalı; böylece üye ülkelerin siber savunma kapasitelerinin güçlendirilmesi ve siber güvenlik normlarının belirlenmesine katkıda bulunulmalıdır. Bunun yanı sıra, NATO'nun diğer milletlerarası örgütlerle iş birliği yaparak, gelişmiş siber saldırı yeteneklerini yüksek maliyetlere

[252] Köksoy, **a.g.e.,** s. 434.

katlanmadan kazanması mümkündür. NATO'nun Europol gibi kurumlarla yürüttüğü iş birliği ve AB ile tamamlayıcı yapıda sürdürdüğü ortaklık, siber uzay alanındaki etkinliğinin devamı açısından kritik öneme sahiptir.[253]

3.2.2.Türkiye'de Siber Egemenliğe İlişkin Hukuki Düzenlemeler

Türkiye'de internet kullanımı, 1980'lerin ortalarından itibaren gündeme gelmiş ve bu dönemde ilk bilgisayar ağları öncelikle üniversiteler tarafından kurulmuştur. Başlangıçta sadece üniversiteler ile araştırma kurumlarının erişimine açık olan bu ağ, zamanla artan ihtiyaçlar doğrultusunda akademik kurumlar tarafından çok sayıda yeni bağlantının oluşturulmasına olanak sağlamıştır. Günümüzde ise, hem akademik ve araştırma kurumları hem de ticari kuruluşlar ve bireyler için internete erişim sağlayan çeşitli bağlantı merkezleri faaliyet göstermektedir.[254]

2000 yılının ocak ayında kurulan Telekomünikasyon Kurumu, 2008 yılı Kasım ayında Bilgi Teknolojileri ve İletişim Kurumu (BTK) olarak yeniden yapılandırılmıştır. BTK, telekomünikasyon sektörünün düzenleyici kuruluşu olarak faaliyet göstermekte olup, yetkilendirme, denetim, ihtilafların çözümü, tüketici haklarının korunması, sektör rekabetinin düzenlenmesi, teknik standartların belirlenmesi ile frekans spektrumunun yönetimi ve izlenmesinden sorumludur. Ayrıca kurum, bilgi teknolojileri alanındaki otorite görevini Telekomünikasyon İletişim Başkanlığı (TİB) aracılığıyla yerine getirmektedir. 2005 yılında kurulan TİB, doğrudan BTK Başkanına bağlı olup, personel yapısında Milli İstihbarat Teşkilatı Müsteşarlığı, Emniyet Genel Müdürlüğü ve Jandarma Genel Komutanlığı gibi güvenlik birimlerinden temsilciler de bulunmaktadır.[255]

Türkiye'nin siber uzay ve bilgi güvenliği alanındaki teknolojik başarısının temel taşlarından biri, Türkiye Bilimsel ve Teknik Araştırma Kurumu (TÜBİTAK) çatısı altında kurulan Gebze'deki Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü (UEKAE) olarak gösterilebilir. Günümüzde ulaşılan teknolojik seviyenin önemli bir kısmı, bu enstitüde gerçekleştirilen çalışmaların bir sonucudur. UEKAE'nin kurulmasından önce, Türkiye siber uzay ve bilgi güvenliği alanındaki ihtiyaçlarını dış kaynaklardan karşılamak zorunda kalmaktaydı ki bu durum, ulusal kaynaklar tarafından

[253] Köksoy, **a.g.e.,** s. 436-437.
[254] Şeker, **a.g.e.,** s. 68-69.
[255] Ekonomi ve Dış Politikalar Araştırma Merkezi, **a.g.e.,** s. 33.

sağlanmayan güvenliğin yeterince etkin olamayacağı ilkesine aykırıdır. Bu anlayış doğrultusunda, Türk Silahlı Kuvvetleri güvenliğin yerli kaynaklardan temin edilmesi kararını almış ve 1975 yılında TÜBİTAK Başkanlığı ile yakın iş birliği içinde çalışmalar başlatılmıştır. Bu girişimler sonucunda, ulusal bir altyapının oluşturulması ve milli cihaz ile teçhizatların geliştirilmesi amacıyla Türkiye'de ilk kez kriptografik test ve tasarım merkezinin kurulması kararlaştırılmıştır. Türkiye'nin siber uzay ve bilgi güvenliği alanında dünya çapında belirli bir konuma yükselmesinde, bu test ve tasarım merkezinin hayata geçirilmesi önemli bir dönüm noktası olmuştur. Bugün gelinen noktada, Türk Silahlı Kuvvetleri bünyesinde bu hedef doğrultusunda adım atanların cesareti, azmi ve sabrı ile UEKAE'de görev alan personelin bilgi birikimi, araştırma gayretleri ve bitmeyen enerjisi kritik rol oynamıştır.[256]

Türkiye, bilgisayar korsanları, saldırganlar ve hackerlar, ulusal güvenliği tehdit etmeye başlamadan önce siber savunma alanında belirgin bir politika geliştirmemiştir. 1991 yılında ulusal mevzuatta siber suçlara ilişkin düzenlemeler yer almasına rağmen, siber güvenlik konusuna yönelik kapsamlı bir politika benimsenmemiştir. Siber tehditlerin önemine yönelik farkındalığın sınırlı kalması nedeniyle, 2000'li yılların ortalarına kadar bu alanda kayda değer bir gelişme yaşanmamıştır. Ayrıca, internet erişiminin ülke genelinde yaygınlaşmaması da bu gecikmenin temel sebeplerinden biri olarak değerlendirilebilir. Türkiye'nin ulusal hukukunda siber güvenlikle ilgili ilk yasal düzenleme olan 3756 sayılı Kanun, 1991'de kabul edilmiş olsa da, Türkiye Büyük Millet Meclisi bu dönemde siber tehditlere karşı bütüncül bir mücadele stratejisi oluşturmakta tereddüt göstermiştir. Ancak 2000'li yılların ortalarından itibaren Türkiye, siber tehditlere karşı resmi politikalar geliştirmeye başlamıştır. Bu bağlamda, Devlet Planlama Teşkilatı tarafından 2006-2010 dönemini kapsayan Bilgi Toplumu Stratejisi ve Eylem Planı hazırlanmıştır. Planın 87 numaralı eyleminde "ülke güvenliğini ilgilendiren bilgilerin elektronik ortamda korunması ve devletin bilgi güvenliği sistemlerinin geliştirilmesi amacıyla gerekli yasal altyapının oluşturulacağı ve uygulanacağı" ifade edilmiştir. Ayrıca, Kişisel Verilerin Korunması Kanunu'nun yasalaştırılması hedeflenmiştir. Bu Eylem Planı ile birlikte Türk yetkililer, kritik bilgilerin mevzuat yoluyla korunmasına yönelik önemli adımlar atmıştır.[257]

[256] Yılmaz ve Salcan, **a.g.e.,** s. 135-336.
[257] Köksoy**, a.g.e.,** s. 303.

Ayrıca, belgenin 88 numaralı eylem planı da şu hususları içermektedir:

"Siber âlemdeki güvenlik tehditlerini sürekli olarak takip edecek, uyarılar yayınlayacak, bu risklere karşı ne şekilde tedbir alınabileceğine dair bilgilendirme yapacak, risklerin ortaya çıkması durumunda karşı tedbirleri koordine edebilecek bir "bilgisayar olaylarına acil müdahale merkezi" kurulacaktır. Kamu kurumları için gerekli minimum güvenlik seviyeleri kurum ve yapılan işlem bazında tanımlanacak, kurumlar tarafından kullanılan sistem, yazılım ve ağların güvenlik seviyeleri tespit edilecek ve eksikliklerin giderilmesi yönünde alacaktır."[258]

Türkiye'ye yönelik siber saldırıların artış göstermesi üzerine, Bakanlar Kurulu Haziran 2012 tarihinde ulusal siber güvenlik faaliyetlerinin yürütülmesi, yönetilmesi ve koordinasyonu ile ilgili kararı kabul etmiştir. Bu karar doğrultusunda, Ulaştırma, Denizcilik ve Haberleşme Bakanlığı liderliğinde bir Siber Güvenlik Kurulu kurulmuştur. Kurulun temel sorumluluğu, ülkenin siber güvenliğini temin etmek amacıyla politika, strateji ve eylem planları geliştirmektir. Ayrıca, BTK tarafından 22 Mayıs 2013 tarihinde Ulusal Siber Olaylara Müdahale Merkezi'nin (USOM) kuruluşu ve yetkilendirilme usul ve esasları onaylanmıştır. USOM'un başlıca görevi, siber olayların etkilerini azaltmak ve ortaya çıkan tehditlerle mücadele etmek amacıyla yeni stratejiler ile önlemler geliştirmektir. Bu bağlamda, tespit edilen siber tehditlere ilişkin ülke genelinde veya ilgili taraflara alarm, uyarı ve duyurular yaparak, muhtemel olayların etkilerinin azaltılması ya da ortadan kaldırılmasına yönelik tedbirlerin alınmasını sağlar. USOM ayrıca, siber güvenlik olaylarına maruz kalan bilişim sistemlerinin korunmasına yönelik önleyici faaliyetlerde bulunur. Söz konusu çalışmalar sırasında suç teşkil eden bulgularla karşılaşıldığında ise, adli makamlar ve kolluk kuvvetleri ile koordineli hareket eder.[259] Bu karar ile birlikte, siber güvenlik kurulu, ulaştırma, denizcilik ve haberleşme bakanlığı başkanlığında oluşturulmuştur. Kurulun temel görevi, ülkeyi siber güvenlik sağlamak için politikalar, stratejiler ve eylem planları hazırlamaktır. Türkiye bilgi ve iletişim

[258] Bilgi Toplumu Stratejisi ve Eylem Planı (2006-2010), https://ms.hmb.gov.tr/uploads/2019/01/Bilgi-Toplumu-Stratejisi-Eylem-Plani-2006-2010.pdf, (Erişim Tarihi: 30.06.2025).
[259] Ulusal Siber Güvenlik Çalışmalarının Yürütülmesi, Yönetilmesi ve Koordinasyonuna İlişkin Karar, https://hgm.uab.gov.tr/uploads/pages/siber-guvenlik/some-bkk.pdf, (Erişim Tarihi: 30.06.2025).

teknolojileri kurumu, 22 Mayıs 2013 tarihinde Ulusal siber olaylara müdahale merkezinin kuruluş ve yetkilendirme usul ve esaslarını onaylamıştır. USOM'un temel görevi siber olayların etkisini azaltmak ve siber tehditlerle mücadele etmek için yeni stratejiler ve önlemler geliştirmektir. Bu kapsamda yapılan çalışmalarda tespit edilen siber tehditlerle ilgili olarak ilgili taraflara ya da ülke çapında alarm, uyarı ve duyurular yaparak yaşanabilecek olayların etkilerini azaltmaya veya ortadan kaldırmaya yönelik önlemlerin geliştirilmesini sağlar. Siber güvenlik olaylarına maruz kalan bilişim sistemlerine yönelik koruyucu tedbirlerin alınması konusunda faaliyetlerde bulunur. Ayrıca yapılan siber güvenlik çalışmaları esnasında konusu suç teşkil eden bulgular ile karşılaşılması halinde adli makamlar ve kolluk kuvvetleri ile koordinasyon içerisinde hareket eder.[260]

"Siber suç" kavramı, Türkiye'de ilk olarak 3756 sayılı Kanun ile TCK'nın 756 sayılı maddesine dahil edilmiştir.[261] Ancak, siber suçlara ilişkin en kapsamlı düzenleme 2004 yılında yürürlüğe giren 5237 sayılı TCK ile gerçekleştirilmiş ve bu suçlar "Bilişim Alanında Suçlar" başlığı altında toplanmıştır. [262] Bu kapsamda, 243. maddede bilişim sistemine izinsiz girme suçu, 244. maddede sistemin işleyişini engelleme, bozma, veri silme veya değiştirme fiilleri, 245. maddede banka ve kredi kartlarının kötüye kullanımı ile yasaklı cihazlar ve kişiler hakkında güvenlik tedbirlerinin uygulanması düzenlenmiştir. 2016 yılında ise, bu kapsama programlar da eklenmiştir. Ayrıca, 246. madde ile tüzel kişiler hakkında güvenlik tedbirleri getirilmiştir. Bunun yanı sıra, bilişim ve iletişim teknolojileri aracılığıyla işlenen suçlar da çeşitli maddelerde düzenlenmiştir. Örneğin, 5237 sayılı Kanun'un 124. maddesi haberleşmenin engellenmesini, 125. maddesi hakareti, 132. maddesi haberleşmenin gizliliğinin ihlalini, 133. maddesi kişiler arasındaki iletişimin dinlenmesi ve kayda alınmasını, 135. maddesi kişisel verilerin kaydedilmesini, 136. maddesi verilerin hukuka aykırı olarak ifşa edilmesini veya ele geçirilmesini, 138. maddesi verilerin yok edilmesini, 142. maddenin ikinci fıkrası nitelikli hırsızlığın bilişim sistemleri kullanılarak işlenmesini, 158. madde ise, nitelikli dolandırıcılığın bilişim sistemleri ve banka ya da kredi kurumları aracılığıyla yapılmasını

[260] Ulusal Siber Olaylara Müdahale Merkezi, https://www.usom.gov.tr/hakkimizda, (Erişim Tarihi: 30.06.2025).
[261] 3756 Sayılı Kanun, https://www5.tbmm.gov.tr/tutanaklar/KANUNLAR_KARARLAR/kanuntbmmc074/kanuntbmmc074/kanuntbmmc07403756.pdf, (Erişim Tarihi: 30.06.2025).
[262] 5237 Sayılı Tük Ceza Kanunu, https://www.mevzuat.gov.tr/mevzuat?MevzuatNo=5237&MevzuatTur=1&MevzuatTertip=5, (Erişim Tarihi: 30.06.2025).

düzenlemiştir. Ayrıca, 226. madde müstehcenlik suçunu, 228. madde ise, bilişim sistemleri aracılığıyla kumar oynanması için yer ve imkân sağlanmasını kapsamaktadır.

Türkiye, diğer terörizm türlerine karşı tedbirli yaklaşmakla birlikte, siber terörizmi bu kapsamın dışında tutmaktadır. Ülkenin siber güvenlik politikasında karşılaşılan önemli sorunlardan biri, siber güvenliğin geliştirilme sorumluluğunun Ulaştırma, Denizcilik ve Haberleşme Bakanlığına verilmiş olmasıdır. Oysaki ülke güvenliğinin sağlanması, bu bakanlığın uzmanlık alanının çok ötesinde bir konudur ve siber güvenlik, diğer alanlardan daha fazla odaklanma ve kaynak gerektiren karmaşık bir alandır. Bahsi geçen sorumluluğun, dönemin yapısal özellikleri göz önüne alındığında, Başbakanlık gibi daha merkezi ve koordinasyon gücü yüksek bir makama verilmesi etkinlik düzeyini artırabilirdi. Günümüzde ise, bu tür politikaların hazırlanması ve koordinasyonunun Cumhurbaşkanlığı çatısı altında gerçekleştirilmesinin önemi giderek artmaktadır.[263]

5651 sayılı Kanun, internet ortamında gerçekleştirilen yayınların düzenlenmesi ile bu yayınlar vasıtasıyla işlenen suçlarla mücadeleyi amaçlayan hukuki bir düzenlemedir. Yaygın olarak "loglama kanunu" olarak da adlandırılan bu mevzuat, internet servis sağlayıcılarının en az iki yıl süreyle veri kayıtlarını tutmalarını zorunlu kılmaktadır. Kanun kapsamında, log kayıtlarının muhafaza süresi altı aydan başlayarak iki yıla kadar değişebilmektedir. Bilişim suçları veya bilgisayar suçları terimi, bilgisayar sistemleri ya da bilgi işlem ağları kullanılarak işlenen her türlü hukuka aykırı fiili tanımlamak amacıyla ortaya çıkmıştır. Örneğin, "ortadaki adam" (man-in-the-middle) saldırısı gibi bilişim suçlarının ceza yaptırımları genellikle en az bir yıl hapis cezası ile başlamaktadır. TCK'nın 243, 244 ve 245. maddeleri, bilişim suçlarına ilişkin hükümleri içermekte ve bu suçlara yönelik cezai yaptırımları düzenlemektedir. Madde 243, izinsiz ve hukuka aykırı şekilde bir bilişim sistemine girme ve sistemde kalmaya devam etme fiillerini suç olarak tanımlar. Bu kapsamda, sisteme zarar verme kastı olmasa dahi, sistemde bulunan güvenlik açıklarının sistem yöneticisine bildirilmesi veya sadece yardım amacıyla sisteme giriş yapılması bile suç teşkil etmektedir. Sistemde yer alan verilerin silinmesi halinde cezanın artması söz konusudur. Madde 244 ise, bilişim sistemlerinin işleyişini engellemek veya bozmak amacıyla işlenen suçları kapsamaktadır. Bu madde kapsamında

[263] Köksoy, **a.g.e.,** s. 322-323.

verilen cezalar daha ağırdır ve kamu kurumları ile kuruluşlarının bilişim sistemlerine yönelik saldırılarda ceza yarı oranında artırılır. Örneğin, banka sistemlerine yönelik gerçekleştirilen DDoS saldırıları bu maddede yer almakta, saldırganlar ceza miktarının artırılmasıyla karşılaşmaktadır. Ayrıca, saldırgan bu eylemden haksız kazanç elde etmişse, beş bin güne kadar adli para cezası da uygulanabilmektedir. Madde 245 ise, banka ve kredi kartlarının usulsüz kullanımına yöneliktir. Başkasına ait banka veya kredi kartlarının izinsiz kullanımı kesinlikle yasaktır ve bu suçu işleyenler hapis ve para cezası ile cezalandırılmaktadır. Ayrıca, yasaklanmış cihaz ve programların kullanımı ile bunların satışını gerçekleştiren kişiler de bu madde kapsamında cezai yaptırımlara tabidir.[264]

Türkiye'ye yönelik yapılan siber saldırı örneklerine bakıldığında, Türkiye genelinde geniş çaplı elektrik kesintileri yaşanmış olup, en az kırk ilde etkili olan bu kesintilerin ardından bazı bölgelerde elektrik arzı kademeli olarak yeniden sağlanmaya başlanmıştır. Başbakan Ahmet Davutoğlu, kesintilerin nedenlerine ilişkin olarak, "Terör dahil tüm olasılıkların titizlikle araştırıldığını" belirtmiştir. Enerji Bakanlığı bünyesinde kriz yönetimi için özel bir çalışma grubu oluşturulmuştur. Enerji ve Tabii Kaynaklar Bakanı Taner Yıldız ise, yaptığı açıklamada, Türkiye genelinde elektrik arzının büyük oranda sağlandığını; özellikle İstanbul'da ise, elektrik enerjisinin yaklaşık yüzde seksen seviyesinde verildiğini ifade etmiş ve kısa sürede kesintilerin tamamen giderileceğini öngördüklerini dile getirmiştir. Bakan Yıldız ayrıca, İzmir bölgesinde özel sektöre ait bir enerji santralinin geçici olarak devre dışı kaldığını ve bu durumun zincirleme etkiler oluşturmuş olabileceğini belirtmiş; ancak söz konusu bilgilerin doğrulanması gerektiğini vurgulamıştır. Yıldız, sistemin temel olarak izole çalıştığını da ifade etmiştir.[265]

31 Mart 2015 tarihinde Türkiye genelinde yaşanan ve 81 ilin 44'ünü etkileyen elektrik kesintileri önemli bir olay olarak kayda geçmiştir. Bu kesintilerin siber saldırı sonucu meydana gelmiş olabileceği yönündeki değerlendirmeler, dönemin Başbakanı Ahmet Davutoğlu tarafından da dile getirilmiştir. Bazı medya organlarında ise, saldırının arkasında İran'ın olabileceğine dair iddialar ortaya atılmıştır. Kesintiler gün boyu devam etmiş ve Türkiye'deki 298 organize sanayi bölgesinde üretimin durmasına neden

[264] Ertuğrul, **a.g.e.,** s. 288-289.
[265] Sputnik Türkiye, https://anlatilaninotesi.com.tr/20150331/1014730458.html, (Erişim Tarihi: 02.07.2025).

olmuştur. Bu durumun ekonomik kaybının yaklaşık 700 milyon dolar civarında olduğu tahmin edilmekle birlikte, bazı uzmanlar zarar miktarının 1 milyar dolara kadar çıkabileceği yönünde daha karamsar değerlendirmelerde bulunmuştur. İlginç bir şekilde, elektriğini doğrudan İran'dan temin eden Van ilinin bu kesintilerden etkilenmemesi dikkat çekicidir. Ancak, kamuya açık kaynaklar üzerinden yapılan değerlendirmelerde, saldırının failinin kesin olarak İran olduğuna dair net ve doğrulanmış bilgilere ulaşılamamıştır.

Bu olay dışında, 2008 yılında Bakü-Tiflis-Ceyhan petrol boru hattına gerçekleştirilen saldırı, Türk politika yapıcıları için önemli çıkarımlar sunmaktadır. İlk olarak, bu olay siber saldırıların kinetik sonuçlarını ortaya koyması bakımından büyük bir öneme sahiptir. İkinci olarak, saldırı; bölgesel güvenlik dinamikleri, enerji jeopolitiği ve askeri-siyasi rekabet arasındaki etkileşimi açıkça göstermiştir. Son olarak, söz konusu siber taarruz kritik ulusal altyapıların taşıdığı kırılganlıkları ve modern savaşların beşinci boyutu olarak kabul edilen siber tehditlerin ciddiyetini vurgulamıştır.[266]

Siber uzay güvenliğine önem veren ülkeler, kriptografik donanım ve yazılımların üretimi, kullanımı ile ithalat ve ihracatına ilişkin yasal düzenlemeler geliştirmiştir. Elektronik ortamda bilginin kolayca ülke dışına çıkabilmesi ve bunun ulusal güvenlik açısından kritik bir boyut oluşturması nedeniyle, siber uzay güvenliğinin sağlanması zorunluluk arz etmektedir. Türkiye'de de benzer denetim ve kısıtlamaları yasal zemine oturtacak düzenlemelerin acilen hayata geçirilmesi gerekmektedir. Bu düzenlemeler, kısa vadede ulusal güvenliğe yönelik tehdit oluşturabilecek unsurların, özellikle internet aracılığıyla güçlü kriptografik algoritmaları yasadışı iletişimlerinde serbestçe kullanmalarını engelleyecektir. Ancak, ulusal güvenliği ilgilendiren bilgilerin tanımı, gizlilik derecelendirmeleri ile bu bilgilerin nasıl üretileceği, korunacağı, aktarılacağı, kullanılacağı ve imha edileceği hususunda Türkiye Cumhuriyeti'nin henüz kapsamlı bir yasal altyapısı bulunmamaktadır. Bu tür düzenlemeler, geçici ve dağınık platformlarla aşılabilecek basit mevzuat yapılarından ziyade, birbirleriyle uyumlu karmaşık bir yasal düzenlemeler bütünü gerektirmektedir. Ayrıca, teknolojik gelişmeler ışığında bu yasal çerçevelerin sürekli güncellenmesi ve teknolojiye uygun hale getirilmesi zorunludur. Türkiye'de ulusal bilgi güvenliği politikasının bulunmayışı, ülkenin genel ulusal güvenlik

[266] Ekonomi ve Dış Politikalar Araştırma Merkezi, **a.g.e.,** s. 19.

hassasiyetini artırmaktadır. Kamu ve özel sektör kuruluşları arasında ulusal güvenlik ihtiyaçlarına yönelik bilgi güvenliğini koordine edecek, yönlendirecek ve ulusal bilgi güvenlik sistemini etkin şekilde işletilecek kurumsal bir yapı mevcut değildir. Bunun yanı sıra, ulusal bilgi güvenliği gibi karmaşık bir alanda ortak anlayışı geliştirecek ve üzerinde mutabık kalınmış tanımlar henüz oluşturulamamıştır.[267]

Siber harp, modern savaşın yeni bir boyutunu temsil etmekte olup, askeri teknolojideki gelişmelerin somut bir yansıması olarak ortaya çıkmaktadır. Bu bağlamda, Askeri Meselelerde Devrim teorisinin öngördüğü şekilde, adaptasyon kapasitesi yalnızca savunma mekanizması olarak değil, aynı zamanda hem devletler hem de devlet dışı aktörler için saldırgan üstünlük sağlama amacıyla da kritik bir öneme sahiptir. Türkiye, 21. yüzyılın karmaşık siber tehdit ortamında istisna teşkil etmemektedir. Ülke ekonomisinin büyümesi, enerji altyapısı, elektrik üretimi ve hidro-stratejik öneme sahip barajlara sıkı bir biçimde bağlıdır. Ayrıca Türkiye, enerji geçiş noktası olma hedefi ile İstanbul'u önemli bir havayolu ulaşım merkezi haline getirme stratejisini sürdürmektedir. Devlet ve özel sektör kurumlarına ait veri tabanlarının büyük bir kısmı, finans ve bankacılık sektöründeki önemli faaliyetler ve bilgi akışı dijital platformlarda yoğunlaşmıştır. Bu durum, siber güvenliği Türk ulusal güvenlik perspektifinde merkezi bir unsur haline getirmektedir.[268]

Güvenlik alanında ortaya çıkan yeni tehditler ışığında, Türkiye'nin kritik ulusal altyapıya yönelik stratejik planlarını yeniden değerlendirmesi önem arz etmektedir. Bu değerlendirme sürecinde siber casusluk, ağ merkezli savaş, psikolojik savaş, bilgi savaşı, elektronik harp ve sinyal istihbaratı gibi alanların da göz önünde bulundurulması gerekmektedir. Siber harp kapsamındaki hem kinetik hem de kinetik olmayan etkiler bağlamında gerçekleştirilecek böyle bir dönüşüm için, farklı disiplinlerden uzmanların katılımıyla oluşturulacak bir komisyonun faydalı olacağı düşünülmektedir. Söz konusu komisyon, Millî Güvenlik Kurulu Genel Sekreterliği çatısı altında teşkil edilerek, siber güvenlik konusundaki tartışmaları devletin en üst seviyelerine taşıma işlevini görebilir. Ayrıca, MGK'nın anayasal olarak iki ayda bir toplanması, bu alandaki fikri takip ve politika gelişimi açısından süreklilik sağlayacaktır.[269]

[267] Yılmaz ve Salcan, **a.g.e.,** s. 121.
[268] Ekonomi ve Dış Politikalar Araştırma Merkezi, **a.g.e.,** s. 21.
[269] Ekonomi ve Dış Politikalar Araştırma Merkezi, **a.g.e.,** s. 22.

7545 Sayılı Siber Güvenlik Kanunu ayrıntılı biçimde incelendiğinde, kanunun gerekçesinin ve ortaya çıkış sürecinin, küresel ölçekteki dijital dönüşümün hızlanmasıyla doğrudan ilişkili olduğu görülmektedir. Hem dünyada hem de Türkiye'de bilişim teknolojilerinin kullanımının olağanüstü bir hızla artması, ülkenin dijitalleşme alanında attığı stratejik adımların da etkisiyle üretilen veri miktarının katlanarak büyümesine yol açmıştır. Bu gelişmeler, Türkiye'nin dijital altyapısının ve bilgi sistemlerinin korunmasını ulusal güvenlik meselesi haline getirmiştir. Günümüzde, klasik savaş anlayışının yerini giderek hibrit savaş stratejilerine bıraktığı; devlet destekli aktörler veya terör örgütleri tarafından yürütülen siber saldırıların yeni bir tehdit boyutu kazandığı gözlemlenmektedir. Dolayısıyla 7545 Sayılı Kanun, yalnızca dijital alanın düzenlenmesini değil, aynı zamanda ulusal güvenliğin dijital boyutunun güçlendirilmesini amaçlayan kapsamlı bir yasal çerçeve olarak değerlendirilmelidir. Bu bağlamda kanun, Türkiye'nin siber tehditlere karşı dayanıklılığını artırmak, bilgi güvenliğini kurumsallaştırmak ve ulusal düzeyde siber savunma kapasitesini güçlendirmek üzere tasarlanmıştır.[270]

7545 Sayılı Siber Güvenlik Kanunun temel hedefinin Türkiye'nin siber uzaydaki ulusal güvenliğini güçlendirmek ve bu alanda yürütme ile denetim fonksiyonlarını yerine getirecek kurumsal bir yapı oluşturmak olduğu görülmektedir. Bu doğrultuda, kanun ile Siber Güvenlik Kurulu adı altında merkezi bir koordinasyon ve karar organı tesis edilmiştir. Kanunun kapsamı, "siber uzayda faaliyet gösteren, hizmet sunan ya da varlık bulunduran kamu kurum ve kuruluşları, kamu kurumu niteliğindeki meslek örgütleri, gerçek ve tüzel kişiler ile tüzel kişiliği bulunmayan diğer yapılar"[271] şeklinde geniş bir çerçevede tanımlanmıştır. Ancak, bu geniş kapsamın yanı sıra, belirli faaliyet alanları ve kurumlar kanun kapsamı dışında bırakılmıştır. Bu yönüyle 7545 sayılı Kanun, hem kamu hem de özel sektör düzeyinde siber güvenliğin kurumsal temellerini güçlendirmeyi amaçlamakta; Türkiye'nin dijital egemenliği ve bilgi güvenliği politikalarının yasal altyapısını oluşturan stratejik bir düzenleme niteliği taşımaktadır.

[270] Emir Yücel, "Türkiye'nin Siber Güvenlik Yaklaşımı ve 7545 Sayılı Siber Güvenlik Kanunu Üzerine Bir Değerlendirme", **Selçuk Üniversitesi Hukuk Fakültesi Dergisi**, C.33, S.3, s. 1861

[271] 7545 Sayılı Kanun, https://www.resmigazete.gov.tr/eskiler/2025/03/20250319-1.htm, (Erişim Tarihi: 01.11.2025).

Türkiye'nin siber güvenlik politikalarının gelişim süreci, dijital dönüşümün beraberinde getirdiği yeni risk ve tehditlere verilen kurumsal ve hukuki yanıtların evrimi olarak değerlendirilebilir. 1990'lı yılların başında internetin toplumsal yaşama girmesiyle birlikte, bilişim suçlarına yönelik sınırlı hukuki düzenlemelerle şekillenen yaklaşım, zaman içinde daha kapsamlı, stratejik ve kurumsal bir siber güvenlik mimarisine dönüşmüştür. Bu dönüşümün en önemli dönüm noktalarından biri, 2025 yılında yürürlüğe giren 7545 Sayılı Siber Güvenlik Kanunu olmuştur. Söz konusu düzenleme, daha önce yönetmelik ve sektörel strateji belgeleri ile sınırlı, dağınık bir yapıya sahip olan Türkiye'nin siber güvenlik politikasını bütüncül ve ulusal düzeyde koordineli bir sisteme taşımıştır. Bu bağlamda, Siber Güvenlik Kurulu, Ulusal Siber Olaylara Müdahale Merkezi, Siber Olaylara Müdahale Ekipleri ve nihayetinde Siber Güvenlik Başkanlığı, siber güvenlik alanında koordinasyon, denetim ve stratejik yönlendirme görevlerini üstlenen temel kurumsal unsurlar haline gelmiştir. Türkiye, bu yapılanma aracılığıyla AB'nin siber güvenlik ekosistemiyle işlevsel düzeyde paralellik gösteren bir yapıya ulaşmıştır. 7545 sayılı Kanun'un getirdiği yeni kurumsal düzen, Siber Güvenlik Başkanlığı'nı merkezi otorite konumuna yerleştirerek Türkiye'de siber güvenliğin kurumsallaşmasını sağlamıştır. Bu yapı, işlev ve görev tanımları bakımından ENISA ile önemli benzerlikler taşımaktadır. Bununla birlikte, Türkiye'de siber güvenlik alanındaki mevcut uygulamaların düzenleyici netlik, denetim mekanizmalarının bağımsızlığı ve kurumsal hesap verebilirlik bakımından daha da geliştirilmesi gerekmektedir. Türkiye'nin siber güvenlik politikaları, teknolojik tehditlere uyum sağlama kabiliyeti bakımından olgunlaşmış; ancak kurumsal şeffaflık, etkin denetim ve uluslararası standartlarla uyum alanlarında ilerlemeye açık bir evrede bulunmaktadır.[272]

Siber Güvenlik Kanunu, kapsamı itibarıyla hem makro düzeyde politika belirlemeye hem de uygulamaya yönelik icrai işlevler içeren çok boyutlu bir düzenleme niteliğindedir. Kanunun hedefleri, Türkiye'nin dijital güvenlik kapasitesini güçlendirmek ve siber tehditlere karşı ulusal ölçekte bütüncül bir koruma sistemi kurmak yönündedir. Kanunun temel amaçları şu şekilde özetlenebilir: 1- Türkiye Cumhuriyeti'nin siber uzaydaki ulusal gücünü oluşturan tüm bileşenlere yönelik iç ve dış tehditleri tanımlamak, değerlendirmek ve etkisiz hale getirmek, 2- Siber olayların olası etkilerini azaltmaya yönelik temel ilkeleri ve müdahale esaslarını belirlemek, 3- Kamu kurumları, kamu

[272] Yücel, **a.g.m.,** s. 1871-1872.

kurumu niteliğindeki meslek kuruluşları, özel sektör ve tüzel kişiliği olmayan oluşumların siber saldırılara karşı korunmasına ilişkin yasal ve teknik çerçeveyi oluşturmak, 4- Ülke genelinde siber güvenliği güçlendirmeye yönelik strateji ve politikaları tanımlamak, 5- Siber Güvenlik Kurulu'nun kuruluşuna, görev ve yetkilerine ilişkin düzenlemeleri belirlemek. Bu bağlamda, söz konusu kanun Türkiye'nin dijital egemenlik alanında gerçekleştirdiği en kapsamlı yasal adımlardan biri olarak değerlendirilmektedir. Kanunun temel yaklaşımı, siber güvenliği ulusal güvenliğin ayrılmaz bir bileşeni olarak konumlandırmaktadır. Bu doğrultuda ilk ve öncelikli hedef, siber tehditlerin tespiti, önlenmesi ve etkisiz hale getirilmesi olarak belirlenmiştir. Bu anlayış, metinde açık biçimde yer alan "siber güvenlik, millî güvenliğin ayrılmaz bir parçasıdır" ilkesiyle somutlaştırılmış ve Türkiye'nin siber savunma politikalarının normatif temelini oluşturmuştur.[273]

[273] Mehmet Bedii Kaya, **Siber Güvenlik Hukuku**, mbkaya.com/hukuk/siber-guvenlik-hukuku.pdf, İstanbul: Dijital Baskı, 2025, s. 163.

SONUÇ

İnternet, başlangıçta bilgisayar sistemlerini birbirine bağlamak amacıyla geliştirilen bir ağ yapısıyken, günümüzde toplumsal, ekonomik ve siyasal yaşamın ayrılmaz bir parçası hâline gelmiştir. Yalnızca bireysel iletişim ya da bilgiye erişim amacı taşımamakta; aynı zamanda devletler arası etkileşimleri, güvenlik stratejilerini ve güç dengelerini yeniden şekillendirmektedir. Bilhassa 1990'lı yıllardan itibaren internetin ticarileşmesi ve yaygınlaşması, siber uzayın doğuşunu hızlandırmış ve bu alanın küresel ölçekte stratejik bir öneme kavuşmasına neden olmuştur.

İnternet ve ağ teknolojilerindeki gelişmeler, devletlerin güvenlik politikalarını dijital ortamda yeniden yapılandırmasını zorunlu kılmıştır. Özellikle siber saldırıların devlet destekli gruplarca yürütülmeye başlanması, milletlerarası güvenlik algılarını da derinden etkilemiştir. Hacking faaliyetleri başlangıçta bireysel çıkar odaklıyken, zamanla ulus-devletlerin çıkarları doğrultusunda yürütülen siber operasyonlara dönüşmüştür. Bu durum, siber uzayı sadece bir iletişim mecrası değil; aynı zamanda saldırı ve savunma stratejilerinin merkezinde yer alan çok boyutlu bir çatışma alanı hâline getirmiştir.

Siber tehditlerin artması, bilgi ve iletişim teknolojilerinin devletler nezdinde birer stratejik unsur olarak görülmesine neden olmuştur. ABD ve Rusya gibi küresel aktörler, askeri kapasitelerini siber alanda da güçlendirme yönünde ciddi adımlar atarken, Estonya ve İsrail gibi ülkeler dijital altyapılarını siber güvenlik ekseninde şekillendirmeye başlamıştır. Türkiye ise, bölgesel tehdit ortamını göz önünde bulundurarak, siber güvenlik politikalarını ulusal çıkarlarına uygun biçimde geliştirmektedir.

Siber güvenlik kavramı, klasik güvenlik anlayışının ötesinde bir çerçeve sunmakta ve yalnızca teknik önlemleri değil; hukuki, kurumsal ve toplumsal düzenlemeleri de kapsayan çok katmanlı bir yapı ortaya koymaktadır. Bu bağlamda, bireyler güvenliğin en zayıf halkası olarak görülse de aynı zamanda en kritik aktörlerdendir. Zira pek çok siber saldırı, kullanıcı hataları veya zayıf güvenlik önlemleri nedeniyle mümkün olmaktadır. Bu nedenle, bireylerin siber güvenlik konusunda bilinçlendirilmesi, ulusal güvenliğin dijital boyutta sürdürülebilirliği açısından büyük önem taşımaktadır.

Siber güvenliğin devlet politikalarında merkezi bir konuma yükselmesi, egemenlik kavramının da dijital çağda yeniden tanımlanmasını gerekli kılmıştır.

Geleneksel olarak kara, deniz ve hava sahalarında tesis edilen egemenlik, siber uzayda fiziki sınırların olmaması nedeniyle belirsizlik taşımaktadır. Siber saldırıların kaynağının tespit edilmesindeki zorluk, devletlerin meşru müdafaa hakkının sınırlarını da muğlaklaştırmaktadır. Bu durum, milletlerarası hukukun siber alana dair normatif boşluklarını daha görünür kılmaktadır.

BM, NATO ve AB gibi milletlerarası kuruluşlar, siber güvenlik konusunda düzenlemeler geliştirmeye çalışmakta; ancak karar alma süreçlerinin siyasi mutabakata bağlı olması, etkinliklerini sınırlamaktadır. Bu noktada, milletlerarası hukukta siber egemenlik kavramının açık şekilde tanınması ve bağlayıcı antlaşmalarla desteklenmesi büyük önem arz etmektedir. Aksi halde, devletlerin siber alandaki müdahaleleri keyfi uygulamalara dönüşebilir ve bireysel hak ve özgürlükler tehdit altına girebilir.

Siber tehditlerin milletlerarası barış ve istikrar üzerindeki etkisi, bu alanda küresel iş birliğini zaruri kılmaktadır. İstihbarat paylaşımı, ortak savunma mekanizmaları ve teknik yardımlaşma gibi araçların güçlendirilmesi; küresel ölçekte etkin bir siber güvenlik mimarisinin inşası açısından elzemdir. Bu bağlamda ulusal stratejilerin yalnızca devlet kurumlarını değil, özel sektör ve sivil toplumu da kapsayacak şekilde katılımcı ve şeffaf biçimde oluşturulması gerekmektedir. Bilgi ve iletişim teknolojilerinin baş döndürücü şekilde ilerlemesi, egemenliğin klasik yorumlarının yetersiz kaldığı yeni bir gerçeklik ortaya koymuştur. Devletlerin bu yeni alanda egemenlik iddiasında bulunması, yalnızca ulusal güvenliği değil aynı zamanda milletlerarası hukuk sisteminin yeniden tanımlanmasını da gerekli kılmaktadır.

21. yüzyılda siber uzaydaki gelişmeler ve yenilikler, farklı düzeydeki aktörlere önemli iletişim imkânları sağlarken, aynı zamanda bu paydaşları çeşitli risk ve tehditlerle de karşı karşıya bırakmaktadır. Siber uzay, sunduğu avantajlarla kullanıcılarını bu ortama bağımlı hale getirirken, kötü niyetli aktörlerin de aynı olanaklardan faydalanmasına olanak tanımaktadır. Çünkü bu ortamda, saldırı gerçekleştirmek isteyen bireylerin ihtiyaç duyduğu teknolojik araçlar hem kolay erişilebilir hem de ekonomik açıdan ulaşılabilirdir. Siber güvenlik kavramı ise, siyasi ve sosyal bağlamlarda sınırlarının net olarak belirlenememesi sebebiyle oldukça karmaşık ve dinamik bir yapıya sahiptir. Geleneksel güvenlik anlayışının bu alandaki eksiklikleri de bu karmaşıklığı teyit etmektedir. Başlangıçta kişisel cihazlardaki bilgi güvenliği ile özdeşleşen siber güvenlik, günümüzde

bireysel düzeyden küresel ölçeğe kadar genişleyen çok boyutlu bir kavram halini almıştır. Bilginin kritik bir güç unsuru haline geldiği günümüzde, bilginin güvenliğinin sağlanması önemli bir gereklilik olarak öne çıkmaktadır. Ancak, siber uzayın karmaşık yapısı, yüksek hızı, aktörlerin belirsizliği, saldırıların anonimliği, merkeziyetsiz yapısı ve etkili bir hukuki düzenlemenin eksikliği gibi faktörler, siber güvenliğin sağlanmasını zorlaştırmaktadır.

Milletlerarası hukuk, esasen antlaşmalar ve milletlerarası teamül gibi temel kaynaklara dayanan, ancak klasik hukuk geleneklerine sıkı sıkıya bağlı kalmak zorunda olan görece genç bir hukuk dalıdır. Bu durum, milletlerarası hukukta meydana gelen değişim ve dönüşümlerin ağır ve uzun soluklu bir süreçte gerçekleşmesine neden olurken, teknolojik gelişmelerin hızla ilerlemesi karşısında esnekliğini sınırlamaktadır. Özellikle 21. yüzyılın ilk çeyreğinde teknolojinin hızlı gelişimi ve küresel ölçekte yaygın kullanımı, milletlerarası hukuk sisteminin siber güvenlik alanında etkin çözümler üretmesini zorlaştırmıştır. Teknolojideki hızlı değişimlere karşın, milletlerarası hukuktaki dönüşümler görece yavaş ilerlemektedir. Bu bağlamda, milletlerarası hukukun teknolojik yeniliklere uyum sağlama yolları, günümüzde bu alanda çalışan akademisyenler tarafından üzerinde durulan önemli araştırma konularından biri olmuştur. Siber güvenlik, hem ulusal hem de milletlerarası düzeyde, yeni kamu düzeninin şekillendirilmesinde kritik bir kavram olarak ön plana çıkmaktadır.

Bu bağlamda yapmış olduğumuz çalışmada ulaşılan temel sonuçları şöyle sıralayabiliriz. Siber alan; fiziki sınırların olmadığı, zaman, mekân kısıtlarının geçerliliğini yitirdiği bir mecradır. Bu nedenle devletlerin klasik anlamda egemenlik anlayışı siber alanda karşılığını bulmakta zorlanmaktadır. Milletlerarası hukuk, kara, deniz ve hava sahaları gibi fiziki egemenlik alanlarını net şekilde tanımlamışken; siber uzay için bu tür düzenlemeler henüz yeterli düzeye ulaşmamıştır. Devletler, siber saldırılara karşı kendi güvenliklerini sağlama yükümlülüğüne sahiptir. Ancak bu savunma hakkının sınırları, saldırının kaynağının belirlenmesindeki güçlük nedeniyle gri alanlar içermektedir. Milletlerarası örgütlerin (BM, AB, NATO) siber güvenlik konusunda rolü artmakta, ancak bu örgütlerin karar alma süreçleri hala siyasi konsensüse bağlı olduğu için etkinlik düzeyleri sınırlı kalmaktadır. Siber egemenlik kavramının milletlerarası hukukta tanınması, devletlerin dijital alanda kendi politikalarını belirleme özgürlüğünü

teminat altına alabilir; ancak bu, bireysel hak ve özgürlüklerle çelişmediği sürece mümkün olmalıdır.

Çalışmamızın sonucunda verebileceğimiz öneriler şöyledir. Milletlerarası hukukta, bu alanla ilgili hukuki düzenlemeler hızlı bir şekilde yapılmalı ve boşluklar giderilmeli, siber uzayda egemenlik ve müdahale sınırlarını açıkça belirleyen bağlayıcı antlaşmalar yapılmalı ve bu çalışmalar geliştirilmelidir. Devletler arasında iş birliği mekanizmaları güçlendirilmeli, özellikle istihbarat paylaşımı ve teknik yardımlaşma alanında küresel platformlar teşvik edilmelidir. Ulusal düzeyde siber güvenlik stratejileri, temel hak ve özgürlüklerle uyumlu şekilde hazırlanmalı, özel sektör ve sivil toplumun katılımıyla şeffaf mekanizmalar oluşturulmalıdır. Küresel bir siber hukuk mahkemesi ya da düzenleyici otorite kurulması yönünde ön adımlar atılmalı; bu yapı bireysel hakları ve devletin meşru güvenlik kaygılarını dengeleyecek bir normatif zemin sağlamalıdır. Avrupa İnsan Hakları Mahkemesi küresel düzeyde bir yapısı olmaması ve bu konularda çağa ayak uyduramaması nedeniyle yetersiz bir mekanizma olarak kalmıştır. Dünyada sekiz milyarı aşkın insanın olduğu ve bu insanların çoğunluğunun internet ve telefon gibi her türlü saldırıya açık bir yapıyı kullandığı düşünüldüğünde konunun ne derecede önem arz ettiği ortaya çıkmaktadır. Siber saldırılara karşı insan haklarını koruyacak küresel düzeyde ve tüm insanlığı kapsayacak daha güçlü, çağın gereklerine ve ihtiyaçlarına cevap verecek bir kurum ve sistem oluşturulmalıdır. Çünkü hak ihlalinde bulunan saldırganların bile tespitinin zor olduğu bir ortamda devletlerin ve tüm insanlığın haklarının korunması devletlerin tek başına baş edebileceği ve caydırıcı olabileceği bir alan değildir. Türkiye özelinde baktığımızda; son zamanlarda oluşturulan ulusal siber güvenlik stratejisinin kapsamı daha da genişletilmeli, milletlerarası iş birliklerine daha fazla ağırlık verilerek güncel teknolojik gelişmeler yakalanmaya ve uygulanmaya çalışılmalıdır.

Siber güvenlik artık sadece teknolojik bir mesele değil; siyasal egemenlik, insan hakları, milletlerarası hukuk ve diplomatik ilişkiler açısından çok boyutlu bir stratejik önceliktir. Devletlerin dijital çağda egemenliklerini koruyabilmeleri, yalnızca siber tehditlere karşı alınacak teknik önlemlere değil; aynı zamanda milletlerarası hukukla uyumlu, insan haklarına duyarlı ve küresel iş birliğini esas alan bir anlayışa bağlıdır. Siber egemenliğin milletlerarası hukuki düzlemde tanımlanması, bu yeni güvenlik paradigmalarıyla baş edebilmek için atılması gereken en önemli adımlardan biridir. Devletlerin siber egemenliği milletlerarası hukukun yeni sınav alanlarından biridir. Bu

alanda atılacak adımlar, sadece ulusal güvenliği değil; küresel barışı, insan haklarını ve dijital çağın hukuk normlarını şekillendirme potansiyeline sahiptir. Bu nedenle konu hem akademik hem de siyasi düzeyde stratejik önem arz etmektedir.

KAYNAKÇA

AKDENİZ, Yaman. **Beyaz Kitap**. 1. b. İstanbul: Papatya Yayıncılık. 2003.

AKIL, Abdülkadir. **Küreselleşen Hukuk ve Ulusal Egemenliğe Etkisi**. 1. b. İstanbul: Kitap Yayınevi. 2023.

ALTINKAYNAK, Mustafa. **Uygulamalı Siber Güvenlik ve Hacking**. 3. b. İstanbul: Ezgi Matbaacılık. 2017.

Anadolu Ajansı. https://www.aa.com.tr/tr/gundem/adalet-bakani-tunc-vietnamda-siber-suclara-karsi-bm-sozlesmesi-imza-toreninde-konustu/3726455. (Erişim Tarihi: 01.11.2025).

ARSLANEL, M. Nazan ve Ertuğrul ERYÜCEL. "Küreselleşme Sürecinde Egemenlik Kavramının Dönüşümü". **Atatürk Üniversitesi Sosyal Bilimler Enstitüsü Dergisi**. C.17. S.1. 2013. ss. 23–36.

BAGHERİ, Saeed. "Uluslararası Hukukta Suçluların İadesi ve Suçluları Kovuşturma Yükümlülüğü". **Ankara Üniversitesi Hukuk Fakültesi Dergisi**. S.1. 2013. ss. 1-40.

BARTLETT, Jamie. (Çev. Yasin Konyalı). **Dark Net İnternetin Yeraltı Dünyası**. 1. b. İstanbul: Timaş Yayınları. 2016.

BERİŞ, Hamit Emrah. **Egemenlik & Bir Kavramın Geçmişi, Bugünü ve Geleceği**. 1. b. İstanbul: Tezkire Yayıncılık. 2014.

BİLGİLİ, Fatih ve Ertan DEMİRKAPI. **Hukukun Temel Kavramları**. 9. b. Bursa: Dora. 2013.

Bilgi Toplumu Stratejisi ve Eylem Planı (2006-2010). https://ms.hmb.gov.tr/uploads/2019/01/Bilgi-Toplumu-Stratejisi-Eylem-Plani-2006-2010.pdf. (Erişim Tarihi: 30.06.2025).

Birleşmiş Milletler Antlaşması. https://inhak.adalet.gov.tr/Resimler/SayfaDokuman/2212020141836bm_01.pdf. (Erişim Tarihi: 29.06.2025).

BM Genel Kurulu'nun 14 Aralık 1974 tarih ve A/3314 sayılı "Saldırının Tanımı" kararı. http://www.un-documents.net/a29r3314.htm. (Erişim Tarihi: 01.11.2025).

BOZKURT, Enver. Yasin POYRAZ ve Selcen ERDAL. **Devletler Hukuku**. 11. b. Ankara: Yetkin Yayınları. 2021.

CANSEL, Erol. Çağla ÖZEL, Mehmet YÜKSEL ve Burcu Özcan BÜYÜKTANIR. **Hukuka Giriş**. 1. b. Ankara: Seçkin Yayıncılık. 2012.

ÇELEBİ, Edip F. **Milletlerarası Hukuk**. 4. b. İstanbul: Fakülteler Matbaası. 1980.

CİN, Mustafa. "Suçluların geri verilmesi ve Türk Hukuk". (İstanbul Üniversitesi SBE Yayımlanmamış Yüksek Lisans tezi). İstanbul. 1996.

Councıl of Europe, https://www.coe.int/tr/web/impact-convention-human-rights/convention-on-cybercrime#/, (Erişim Tarihi: 01.11.2025).

DARICILI, Ali Burak. **Siber Uzay ve Siber Güvenlik ABD ve Rusya Federasyonu'nun Siber Güvenlik Stratejilerinin Karşılaştırmalı Analizi**. 1. b. Bursa: Dora Basım-Yayın. 2017.

DEĞDAŞ, Ulaş Can. "Uluslararası Hukukta Önleyici Meşru Müdafaa Hakkı", **Anadolu Üniversitesi Hukuk Fakültesi Dergisi**. C.1. S.6. 2018. ss. 21–40.

DOĞAN, Nejat. Cenap ÇAKMAK ve Halil Kürşad ASLAN (der). **Birleşmiş Milletler: BM Sistemi ve Reformu**. Ankara: Siyasal Kitabevi. 2014.

DERYAL, Yahya. **Temel Hukuk Bilgisi**. 1. b. Trabzon: Derya Kitabevi. 2007.

DİRİCAN, Can Okan. **Teori ve Uygulamalar ile TCP/IP ve Ağ Güvenliği**. 2. b. İstanbul: Açık Akademi Yayınları. 2007.

DONAY, Süheyl. "Suçluların İadesinde Yeni Gelişmeler". **İstanbul Hukuk Fakültesi Dergisi**, C.50. S.1-4. 1984. ss. 239-274.

DUMAN, Berat. "Türk Hukukunda Geri Verme Kurumu ve Usulü". **Türkiye Adalet Akademisi Dergisi**. S.24. 2016.

Ekonomi ve Dış Politikalar Araştırma Merkezi, **Türkiye'de Siber Güvenlik ve Nükleer Enerji**. 1. b. İstanbul: Edam. 2016.

ELDEM, Tuba. "Uluslararası Siber Güvenlik Normları ve Sorumlu Siber Egemenlik". **İstanbul Hukuk Mecmuası**. S.79. 2021. ss. 345-376.

EREN, Mehmet. **Avrupa Birliği'nin Siber Güvenlik Politikası**. 1. b. İstanbul: Beta Basım. 2017.

ERTUĞRUL, İlker. **Network, Linux, Kriptoloji, Deep Web, Sızma Testleri, Ofansif ve Defansif Siber Güvenlik**. 1. b. İstanbul: Dikeyeksen. 2020.

GÜNGÖR, Gülin. "Suçluların İadesine Dair Avrupa Sözleşmesi (SİDAS)"**. Milletlerarası Hukuk ve Milletlerarası Özel Hukuk Bülteni**, C.19. S.1-2. 1999. ss. 359-382.

GÜRİZ, Adnan. **Hukuk Başlangıcı**. 12. b. Ankara: Siyasal Kitabevi. 2009.

GÖZLER, Kemal. **Devletin Genel Teorisi**. 4. b. Bursa: Ekin Yayınevi. 2012.

HERZOG, Stephen. "Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses". **Journal of Strategic Security**. C.4. S.2. 2011. ss. 49-60.

İÇEL, Kayıhan. Suçluların Geri Verilmesi Üzerine Bir İnceleme. **İstanbul Hukuk Fakültesi Dergisi**. C.30. S.3-4. 2011. ss. 692-721.

İÇEL, Kayıhan. **Türk Ceza Hukuku Genel Hükümler**. 6. b. İstanbul: Beta Yayınları. 2021.

İnsan Hakları Evrensel Beyannamesi. https://www.un.org/en/about-us/universal-declaration-of-human-rights. (Erişim Tarihi: 28.06.2025).

KAYA, Mehmet Bedii. **Siber Güvenlik Hukuku**. mbkaya.com/hukuk/siber-guvenlik-hukuku.pdf. İstanbul: Dijital Baskı. 2025.

KAYAR, İsmail ve İlhan ÜZÜLMEZ. **Hukukun Temel Kavramları**. 7. b. Ankara: Detay Yayıncılık. 2011.

KILLIOĞLU, Mehmet Erkan. "Siber Egemenlik Konusu". **Mehmet Akif Ersoy Üniversitesi Sosyal Bilimler Enstitüsü Dergisi**. S.40. 2024. ss. 132-149.

Kilitli Kalkan-2025 Tatbikatı Basın Duyurusu. https://www.msb.gov.tr/Basin-ve-Yayin/Aciklamalar/2baf4d7de031407e801609e83c11a606. (Erişim Tarihi: 28.06.2025).

KOCA, Mahmut ve İlhan ÜZÜLMEZ. **Türk Ceza Hukuku Genel Hükümler**. 14. b. Ankara: Seçkin Yayınevi. 2021.

KÖKSOY, Fulya. **Yeni Küresel Tehdit Siber Saldırılar, Siber Güvenlik ve Politika Uygulamaları**. 1. b. Nobel Akademik Yayıncılık. 2020.

KÖPRÜLÜ, Timuçin. "Türkiye–Çin Halk Cumhuriyeti Suçluların İadesi Andlaşmasına Dair Hukuki Bir Değerlendirme". **Ceza Hukuk ve Kriminoloji Dergisi**. C.9. S.1. 2021. ss. 85-133.

Kuzey Atlantik Antlaşması. https://www.nato.int/cps/en/natohq/official_texts_17120.htm. (Erişim Tarihi: 28.06.2025).

Milletler Cemiyeti Misakı. https://hukukbook.com/milletler-cemiyeti-antlasmasi/. (Erişim Tarihi: 29.06.2025).

NATO. https://www.nato.int/cps/en/natohq/topics_78170.htm. (Erişim Tarihi: 28.06.2025).

NYE, Joseph S. "The Regime Complex for Managing Global Cyber Activities". **Global Commission on Internet Governance Paper Series**. 2014, ss. 1-20.

OORSCHOT, Paul c. Van. (Çev. Kemal Bıçakçı). **Siber Güvenliğe Giriş Bilgisayar Güvenliği ve İnternet Araçlar ve Mücevherler**. Ankara: Palme Yayınevi. 2002.

ÖNOK, Murat. "Avrupa Konseyi Siber Suç Sözleşmesi Işığında Siber Suçlarla Mücadelede Uluslararası İş Birliği". **Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Derneği**. C.19. S.2. 2013. ss. 1229-1270

ÖZBEK, Veli, Koray DOĞAN, Pınar BACAKSIZ ve İlker TEPE. **Türk Ceza Hukuku**. 8. b. Ankara: Seçkin Yayıncılık. 2017.

ÖZGENÇ, İzzet. **Türk Ceza Hukuku Genel Hükümler**. 17. b. Ankara: Seçkin Yayıncılık. 2021.

ÖZKARCI, İsmail. Ulusal ve Uluslararası Hukukta Terör Suçlularının İadesi**.** (Ankara Yıldırım Beyazıt Üniversitesi SBE Yayımlanmamış Doktora tezi). Ankara. 2019.

PAZARCI, Hüseyin. **Uluslararası Hukuk**. 20. b. Ankara: Turhan Kitabevi. 2021.

PAZARCI, Hüseyin. **Uluslararası Hukuk Dersleri II. Kitap**. Ankara: Ankara Üniversitesi Siyasal Bilgiler Fakültesi ve Basın-Yayın Yüksekokulu Basımevi. 1989.

PEHLİVAN, Hasan Basri. **Türk Anayasalarında Egemenlik Kavramı**.1. b. İstanbul: Doğu Kütüphanesi. 2020.

RUHİ, Ahmet Cemal. "Türk Hukukunda Suçluların İadesi". **Erzincan Binali Yıldırım Üniversitesi Hukuk Fakültesi Dergisi**. C.7. S.1-2. 2003. ss. 497-521.

SCHMİTT, Michael N. (ed.). **Tallinn Manual on the International Law Applicable to Cyber Warfare**. Cambridge: Cambridge University Press. 2013.

SELÇUK, Sami. **Zorba Devletten Hukukun Üstünlüğüne**. 3. b. Ankara: Yeni Türkiye Yayınları. 1999.

Sputnik Türkiye. https://anlatilaninotesi.com.tr/20150331/1014730458.html. (Erişim Tarihi: 02.07.2025).

ŞEKER, Tülay Bektaş. **İnternet ve Bilgi Açığı**. Konya: Çizgi Kitabevi. 2025.

TOLUNER, Sevin. **Milletlerarası Hukuk Dersleri & Devletin Yetkisi (Yer ve Kişiler Bakımından Çevresi ve Niteliği)**. 2. b. İstanbul: Fakülteler Matbaası. 1979.

United Nations. https://www.un.org/en/about-us/un-charter. (Erişim Tarihi: 28.06.2025).

United Nations, Hükümet Uzmanları Grubu. https://disarmament.unoda.org/group-of-governmental-experts/. (Erişim Tarihi: 28.06.2025).

United Nations. https://www.un.org/en/peace-and-security/basic-facts-about-global-cybercrime-treaty. (Erişim Tarihi: 01.11.2025).

United Nations. https://www.unodc.org/unodc/frontpage/2024/December/five-reasons-why-the-new-cybercrime-convention-matters.html. (Erişim Tarihi: 01.11.2025).

Ulusal Siber Güvenlik Çalışmalarının Yürütülmesi, Yönetilmesi ve Koordinasyonuna İlişkin Karar. https://hgm.uab.gov.tr/uploads/pages/siber-guvenlik/some-bkk.pdf. (Erişim Tarihi: 30.06.2025).

Ulusal Siber Olaylara Müdahale Merkezi. https://www.usom.gov.tr/hakkimizda. (Erişim Tarihi: 30.06.2025).

Uluslararası Telekomünikasyon Birliği. https://ourworldindata.org/grapher/share-of-individuals-using-the-internet?tab=chart. (Erişim Tarihi: 01.07.2025).

ULUTAŞ, Ahmet. **Avrupa İnsan Hakları Sözleşmesi Işığında Suçluların Geri Verilmesi**. Ankara: Türkiye Barolar Birliği Yayınları. 2012.

ULUTAŞ, Ahmet. “Suçluların İadesine Dair Avrupa Sözleşmesi ve Türkiye”. (Gazi Üniversitesi SBE Yayımlanmamış Doktora Tezi). Ankara. 2010.

ULUTAŞ, Ahmet. “Türk Geri Verme Hukukunda Terminoloji Birliği İhtiyacı ve Bu Açıdan Türkiye-Tunus Sözleşmesi’nin Değerlendirilmesi”. **Ankara Hacı Bayram Veli Üniversitesi Hukuk Fakültesi Dergisi**. C.16. S.3. 2012.

UYGUN, Oktay. **Devlet Teorisi**. 8. b. İstanbul: On iki Levha Yayıncılık. 2021.

YAŞAR, Yusuf ve Zafer İÇER. “Tutuklu ve Hükümlülerin Takası ve İadesi”. **Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi**. C.25. S.2. 2019. ss. 1486-1519.

YAZGI, Ahmet Can. “6706 Sayılı Cezai Konularda Uluslararası Adli İş Birliği Kanunu Çerçevesinde İadenin Kabul Edilemeyeceği Haller”. (İstanbul Üniversitesi SBE Yayımlanmamış Yüksek Lisans Tezi). İstanbul. 2019.

YERLİKAYA, Mehmed. “Türk Ceza Hukuku'nda Geri Verme Kurumu ve Avrupa Tutuklama-Yakalama Müzekkeresi”. (İstanbul Üniversitesi SBE Yayımlanmamış Yüksek Lisans Tezi). İstanbul. 2010.

YILDIRIM, Murat. **Her Yönüyle İnternetin Altyapısı TCP/IP Hızla Genişleyen ve Taşınmaya Hazırlanan IP Ağları İçin Tek Kapsamlı Kaynak**. 10. b. İstanbul: Pusula Yayıncılık. 2009.

YILMAZ, Sait ve Olcay SALCAN. **Siber Uzay’da Güvenlik ve Türkiye**. 1. b. İstanbul: Milenyum Yayınları. 2008.

YILMAZ, Sercan ve Murat AKÇAKAYA. “Türklerde Egemenlik ve Devlet Kanunu”. **Çankırı Karatekin Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi**. S.2. C.13. 2023.

YÜCEL, Emir. “Türkiye’nin Siber Güvenlik Yaklaşımı ve 7545 Sayılı Siber Güvenlik Kanunu Üzerine Bir Değerlendirme”. **Selçuk Üniversitesi Hukuk Fakültesi Dergisi**. C.33. S.3. 2025. ss. 1849–1879.

Vilnius Zirvesi Bildirisi. https://www.nato.int/cps/en/natohq/official_texts_217320.htm. (Erişim Tarihi: 28.06.2025).