

T.C.
MARMARA ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ
KAMU HUKUKU ANABİLİM DALI
KAMU HUKUKU DOKTORA PROGRAMI

**ULUSLARARASI HUKUKTA
DEVLET EGEMENLİĞİNİN BİR KONUSU OLARAK
SİBER UZAY**

Doktora Tezi

ALP EREN TANYERİ

İstanbul, 2024

T.C.
MARMARA ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ
KAMU HUKUKU ANABİLİM DALI
KAMU HUKUKU DOKTORA PROGRAMI

**ULUSLARARASI HUKUKTA
DEVLET EGEMENLİĞİNİN BİR KONUSU OLARAK
SİBER UZAY**

Doktora Tezi

ALP EREN TANYERİ

Tez Savunma Jürisi

1. Tez Danışmanı:	Prof. Dr. Selami KURAN
2. Üye:	Prof. Dr. Akif Emre ÖKTEM
3. Üye:	Doç. Dr. Hakkı Hakan ERKİNER
4. Üye:	Prof. Dr. Abdullah SEZER
5. Üye:	Doç. Dr. Galip Engin ŞİMŞEK

İstanbul, 2024

ÖZET

ULUSLARARASI HUKUKTA

DEVLET EGEMENLİĞİNİN BİR KONUSU OLARAK

SİBER UZAY

Beşerî düzeni idare eden siyasal iktidar yapılarının mahiyeti, asırlar süren çatışma ve tartışmalar sonucunda modern dönemdeki şekliyle belirlenmiş; egemenlik vasfı, devlete atfedilmiştir. Siyasi iradesine, ülkesine ve vatandaşlarına temas eden tüm olgular üzerinde egemen devlet hukuki ilgi sahibidir. Uluslararası hukuk da bu ilginin sınırlarını çizen ve çizilen sınırların müdafaa esaslarını belirleyen ana disiplindir.

Sosyal bilimler literatürüne hızla yerleşen siber uzay, hukuk ve devletle çok çeşitli ilişki biçimleri içindedir. Ancak fiziksel ve mantıksal unsurları bir arada barındıran siber uzayın, mantıksal boyutun insan zihninde oluşturduğu sanal gerçeklik algısı nedeniyle genellikle mekân metaforlarına konu edildiği görülmektedir. Söz konusu ilişki biçimlerinin sıhhatle çözümlenebilmesi için metaforik yaklaşımlar törpülenmesi, amaca uygun bir tanım ve muhteva belirlenmesi gereklidir.

Bu çalışmada öncelikle, devletin siber uzay ile ilişkilendirilmesinde karşılaşılabilecek tutarsızlıkları izale etmek adına siber uzay, fiziksel ve mantıksal boyutlar ile kişi ve veri unsurlarından müteşekkil teorik bir uzay olarak tanımlanmıştır. Devamında, siber uzayın hukuki düzenlenebilirliğine dair tartışmalar ve uluslararası hukuktaki güncel gelişmeler değerlendirilmiştir. Son olarak, devlet egemenliğinin siber uzay üzerindeki görünümü ele alınmıştır. Devletin siber uzayın boyut ve unsurları üzerindeki yetkisi, iç egemenlik bağlamında incelenmiş; dış egemenlik bağlamında ise “siber egemenlik” ve “siber ülke” kavramları ile egemenliği ihlal edecek fiillere ve ihlalin sonuçlarına dair hukuki değerlendirmeler sunulmuştur.

ABSTRACT

CYBERSPACE AS AN ISSUE OF STATE SOVEREIGNTY IN INTERNATIONAL LAW

The nature of the political power structures that govern the human order has been determined in its modern form as a result of centuries-long conflict and debate; the sovereignty has been attributed to the state. The sovereign state has a legal interest in all phenomena that touch its political will, territory and citizens. International law is the main discipline that draws the boundaries of this interest and determines the principles of defence of these drawn boundaries.

Cyberspace, gaining rapid prominence in the social sciences literature, has various forms of relations with law and the state. However, it is seen that cyberspace, which contains physical and logical elements together, is often conceptualised through spatial metaphors due to the virtual reality perception created in the human mind by the logical dimension. In order to analyse these forms of relations properly, it is necessary to refine metaphorical approaches and determine a suitable definition and content for the purpose.

In this study, firstly, cyberspace is defined as a theoretical space consisting of physical and logical dimensions, people and data elements in order to eliminate inconsistencies to be encountered in the association of the state with cyberspace. Subsequently, debates surrounding the legal regulability of cyberspace and current developments in international law are evaluated. Finally, the manifestations of state sovereignty over cyberspace are discussed. The state's jurisdiction over the dimensions and elements of cyberspace is examined in the context of internal sovereignty; and in the context of external sovereignty, the concepts of “cyber sovereignty” and “cyber territory” and legal assessments on acts that would violate sovereignty and the consequences of such violations are presented.

İÇİNDEKİLER

Sayfa No.

İÇİNDEKİLER.....	iii
KISALTMALAR.....	viii
GİRİŞ.....	1

Birinci Bölüm

SİBER UZAY VE EGEMENLİK

I. SİBER UZAY	7
A. Tanım ve Tarihsel Gelişim	7
1. Kubernetes ve Sibernetik	7
2. İnternet ve Web.....	10
3. Tanımların Sınıflandırılması.....	14
a. Ansiklopedik Sözlükler.....	14
b. Devletler.....	15
c. Uluslararası Örgütler ve Sivil Toplum Kuruluşları.....	18
d. Öğreti	20
B. Bir Uzay Olarak Siber Uzay	24
C. Siber Uzayın Boyutları ve Unsurları	28
1. Analiz Yöntemleri	28
2. Egemenlik Amaçlı Siber Uzay Modellemesi	31
a. Fiziksel Boyut	32
b. Mantıksal Boyut.....	34
c. Veri / Bilgi Unsuru.....	35
d. İnsan Unsuru	37
II. EGEMENLİK	38
A. Tarihsel ve Teorik Düzlem	39
1. İktidar.....	39
2. Kabuller ve Meşruiyet	40
3. Avrupa'nın İki Kılıcı	42
4. Egemenliğin doğuşu	44
5. Sözleşmecî Düşünürler ve Modern Devletin Doğuşu	45
6. Modern Egemenliğe Eleştiriler.....	47

B.	Uluslararası Hukuk ve Egemenlik.....	51
1.	Uluslararası Hukukun Doğuşu.....	51
2.	Vestfalya Barışı ve Modern Uluslararası Hukuk İlişkisi.....	53
3.	Uluslararası Hukukta Egemenliğe Pozitivist Bakış.....	56
4.	Birleşmiş Milletler Düzeni ve Self Determinasyon Hakkı.....	57
C.	Modern Uluslararası Hukukta Devlet Egemenliğine Hâkim İlkeler.....	60
1.	Egemenlik ve Bağımsızlık İlişkisi.....	60
2.	İç Egemenlik – Dış Egemenlik Ayrımı.....	61
3.	Devletlerin Egemen Eşitliği İlkesi.....	62
4.	Müdahale Etmeme ve Karışmama İlkesi.....	65
5.	Doğal Kaynaklar Üzerinde Sürekli Egemenlik İlkesi.....	71
D.	Devlet Egemenliğinin Unsurları ve Konuları.....	72
1.	Devletin Hak ve Vazifeleri Teorisi.....	72
2.	Egemenlik ve Yetki İlişkisi.....	74
3.	Yetkiye İlişkin Ayrımlar.....	75
a.	Düzenleme Yetkisi, İcra Yetkisi ve Yargı Yetkisi.....	76
b.	Hukuki Yetki ve Cezai Yetki.....	77
c.	Ülkesel Yetki ve Kişisel Yetki.....	78
d.	Ortak ve Mütedahil Yetkiler.....	81
4.	Devletin Yetkisinin İstisnaları ve Egemenliğe Tabi Olmayan Alanlar.....	81
a.	Egemenlik Alanında İrade Beyanına Dayalı veya İlkesel Kısıtlamalar.....	81
b.	Terra Nullius, Res Communis ve İnsanlığın Ortak Mirası.....	82
c.	Vatansızlık.....	85

İkinci Bölüm

SİBER UZAY GENEL HUKUKU

I.	SİBER UZAYIN HUKUK İLE İLİŞKİLENDİRİLMESİ.....	87
A.	Erken Dönem.....	89
B.	Klasik Dönem.....	92
1.	İlk Analoji Tartışmaları.....	92
2.	İlkesel Tartışmalar.....	94
3.	“At Hukuku”.....	97
4.	Siber Uzayın Özerklik Talebi Olarak “Siber Hukuk”.....	100
5.	Lex Mercatoria ve Siber Uzay.....	104
C.	Modern Dönem.....	105
1.	Kodun Gücü.....	105

2. Mekânsallığın Dönüşümü	110
3. Devletin Fiziksel Cebri	115
D. Genel Değerlendirmeler	117

II. ULUSLARARASI TOPLULUK NEZDİNDE SİBER UZAYIN

DÜZENLENMESİ VE YÖNETİMİ 120

A. İnternetin Küresel Yönetişi ve Çok Paydaşlılık	120
B. Birleşmiş Milletler Nezdinde Yürütülen Başlıca Süreçler	124
1. Birleşmiş Milletler Yolunda İlk Adımlar	124
2. Hükümet Uzmanları Çalışma Grubu	126
3. Açık Uçlu Çalışma Grupları	127
C. Başlıca Devlet Pozisyonları.....	131
1. Amerika Birleşik Devletleri.....	132
2. Çin Halk Cumhuriyeti.....	136
3. Rusya Federasyonu	141
4. Türkiye Cumhuriyeti	147
D. Uluslararası Örgütler ve Sivil Toplum Kuruluşları.....	148
1. Uluslararası Telekomünikasyon Birliği.....	149
2. İnternet Tahsisli Sayılar ve İsimler Kurumu	152
3. Sivil Teknik Topluluklar.....	155
E. Uluslararası Hukuk Düzenlemeleri	159
1. Genel Kapsamlı Uluslararası Düzenlemelerdeki Hükümler.....	160
2. Bölgesel Uluslararası Örgütler Nezdindeki Antlaşmalar	161
a. Avrupa Konseyi Sanal Ortamda İşlenen Suçlar Sözleşmesi.....	162
b. Şangay İşbirliği Örgütü Uluslararası Bilgi Güvenliğinin Sağlanmasında İş Birliği Anlaşması	165
c. Bağımsız Devletler Topluluğu Bilgi Teknolojileri Alanındaki Suçlarla Mücadelede İş Birliği Anlaşması	166
d. Arap Devletleri Ligi Bilgi Teknolojisi Suçlarıyla Mücadele Sözleşmesi.....	167
e. Afrika Birliği Siber Güvenlik ve Kişisel Verilerin Korunması Sözleşmesi ...	167
3. Avrupa Birliği Düzenlemeleri	168
4. Tallin El Kitabı	172
F. Uluslararası Hukukta Siber Uzaya Hâkim İlkeler	174

Üçüncü Bölüm
SİBER UZAY ÜZERİNDE DEVLET EGEMENLİĞİNİN
GÖRÜNÜMLERİ VE SORUNLARI

I. SİBER UZAYIN BOYUT VE UNSURLARI ÜZERİNDE DEVLETİN

YETKİSİ.....	181
A. Siber Uzayın Fiziksel Boyutu Üzerinde Devletin Yetkisi.....	183
1. Ülkesel Yetkiye Tabi Fiziksel Unsurlar	183
2. Ülke Dışı Fiziksel Unsurlar	184
a. Açık Deniz Sualtı Kabloları	184
b. Siber Kapasiteli Uydular ve Uzay Araçları.....	186
B. Siber Uzayın Kişi Unsuru Üzerinde Devletin Yetkisi.....	187
1. Yükleyen ve İndiren Teorisi	188
2. İnternet Søjelerinin Modern Tasnifi	192
a. Erişim Sağlayıcı	194
b. Yer Sağlayıcı.....	197
c. Web Sitesi İşletmecisi	198
d. İçerik Sağlayıcı	203
e. Kullanıcı.....	206
3. Ülke Dışındaki Yabancı Søjeler Üzerinde Yetki Tespiti ve İcrasına İlişkin Teorik Zemin	208
a. Pasif Vatandaşlık İlkesi	208
b. Objektif Ülkesellik İlkesi ve Etki Doktrinleri.....	209
c. Seçici Uyum Doktrini ve Mevcut Sisteme Yönelik Eleştiriler	213
4. Otonom Araçların Eylemlerinde ve Yapay Zekâ Sistemleri Tarafından Üretilen İçeriklerde İsnat Sorunu	217
C. Siber Uzayın Mantıksal Boyutu ve Veri Unsuru Üzerinde Devletin Yetkisi.....	220
1. Fikri Mülkiyet.....	222
2. İnternet Üzerinde Yetki İcrası	226
a. Gözetim ve Denetim	227
b. İçerik Kaldırma	233
c. Filtreleme ve Erişim Engeli	236
3. Büyük Veri, Bulut Bilişim ve Holizm Bağlamında Veri ve Kişisel Veriler	239
4. Finansal Teknolojiler	245

II. SİBER UZAYDA SINIR ÇİZGİLERİ VE EGEMENLİK

MÜCADELESİ....	250
A. Siber Uzayda Devlet Egemenliğinin Genel Teorisi	250

1. Siber Vestfalyacılık	250
2. Siber Egemenlik.....	252
3. Siber Uzayda Ülkesel Egemenlik ve Kritik Altyapı.....	255
4. Siber Uzayda Egemenliğe Karşı “Ortak Mal” Yaklaşımı	260
5. Genel Değerlendirmeler.....	263
B. Siber Uzayda Egemenliğin İhlali.....	269
1. İlke Olarak Egemenlik ve Kural Olarak Egemenlik.....	269
2. Genel Esaslar	273
a. Metoda Dair	273
b. Fail ve Siber İsnat	273
c. Teşebbüs, Kast ve Rıza	275
3. Devletin Fiziksel Ülkesinde Gerçekleşen Yabancı Siber Faaliyet Kaynaklı Egemenlik İhlali	276
4. Devletin Fiziksel Ülkesi Dışında Gerçekleşen Siber Faaliyet Kaynaklı Egemenlik İhlali	277
a. Uzaktan Siber Faaliyet ile Ülkesel Bütünlüğe Müdahale Edilmesi	278
b. Uzaktan Siber Faaliyet ile Siyasi Bağımsızlığa Müdahale Edilmesi	282
SONUÇ	287
KAYNAKÇA	297

KISALTMALAR

<i>AB</i>	Avrupa Birliđi
<i>ABAD</i>	Avrupa Birliđi Adalet Divanı
<i>ABD</i>	Amerika Birleşik Devletleri
<i>AfB</i>	Afrika Birliđi
<i>AIA</i>	Artificial Intelligence Act
<i>AİHM</i>	Avrupa İnsan Hakları Mahkemesi
<i>BDT</i>	Bağımsız Devletler Topluluđu
<i>BİT</i>	Bilgi ve iletişim teknolojileri
<i>Bkz.</i>	Bakınız
<i>BM</i>	Birleşmiş Milletler
<i>BMDHS</i>	Birleşmiş Milletler Deniz Hukuku Sözleşmesi
<i>CERN</i>	Conseil Européen pour la Recherche Nucléaire
<i>CRA</i>	Cyber Resilience Act
<i>Çev.</i>	Çeviren
<i>DIKW</i>	Data – Information – Knowledge – Wisdom
<i>DLT</i>	Distributed ledger technology
<i>DMCA</i>	Digital Millennium Copyright Act
<i>DNS</i>	Domain Name System
<i>DSA</i>	Digital Services Act
<i>DTÖ</i>	Dünya Ticaret Örgütü
<i>Ed.</i>	Editör
<i>EFF</i>	Electronic Frontier Foundation
<i>ENISA</i>	European Union Agency for Cybersecurity (European Union Network and Information Security Agency)
<i>FISA</i>	Foreign Intelligence Surveillance Act
<i>FSEK</i>	Fikir ve Sanat Eserleri Kanunu
<i>FSF</i>	Free Software Foundation
<i>FTP</i>	File Transfer Protocol
<i>GDPR</i>	General Data Protection Regulation
<i>Hızl.</i>	Hazırlayan

<i>Ibid.</i>	İbidem (Aynı yer)
<i>ICANN</i>	Internet Corporation for Assigned Names and Numbers
<i>IEC</i>	International Electrotechnical Commission
<i>IGF</i>	Internet Governance Forum
<i>ISAD'96</i>	Information Society and Development Conference
<i>ISO</i>	International Organization for Standardization
<i>Iss.</i>	Issue
<i>IT</i>	Information technology
<i>ITU</i>	International Telecommunication Union
<i>İSS</i>	İnternet servis sağlayıcı
<i>KVKK</i>	Kişisel Verilerin Korunması Kanunu
<i>m.</i>	Madde
<i>NTIA</i>	National Telecommunications and Information Administration
<i>P2P</i>	Peer to peer
<i>Para.</i>	Paragraf
<i>PoC</i>	Points of Contact
<i>PDE</i>	Products with digital element
<i>R. G.</i>	Resmî Gazete
<i>RUDRP</i>	Rules for Uniform Domain Name Dispute Resolution Policy
<i>s.</i>	Sayfa
<i>ss.</i>	Sayfa aralığı
<i>ŞİÖ</i>	Şangay İşbirliği Örgütü
<i>T.C.</i>	Türkiye Cumhuriyeti
<i>TCP/IP</i>	Transmission Control Protocol / Internet Protocol
<i>TOR</i>	The Onion Router
<i>TLD</i>	Top level domain
<i>UAD</i>	Uluslararası Adalet Divanı
<i>UNCHR</i>	United Nations High Commissioner for Refugees
<i>UNECA</i>	Afrika Ekonomik Kurulu
<i>UNESCO</i>	United Nations Educational, Scientific and Cultural Organization
<i>UNGGE</i>	United Nations Group of Governmental Experts
<i>UNOEWG</i>	United Nations Open-Ended Working Group

<i>UNTS</i>	United Nations Treaty Series
<i>vb.</i>	Ve benzeri
<i>vd.</i>	Ve devamı
<i>VoIP</i>	Voice over Internet Protocol
<i>Vol.</i>	Volume
<i>VPN</i>	Virtual private network
<i>yy</i>	Yüzyıl
<i>WIPO</i>	World Intellectual Property Organization
<i>WWW</i>	World Wide Web



GİRİŞ

Tel örgüler, duvarlar, gümrük kapıları, mayın tarlaları, haritalar; bayraklar, anıtlar, tanklar, kimlikler, pasaportlar, kâğıt ve madeni paralar... Etten ve çelikten yorgun devlerin¹ hayat emarelerinin, mekân ve mesafe unsurlarını bulanıklaştıran gelişmeler karşısında bir an için anlamını yitirdiği düşünülmüştü. Oysa dev(let)ler için elektriğe, sinyallere, dalgalara, birlere ve sıfırlara hükmetmek, 90'lı yıllara göre bugün daha zor fakat daha mümkün görünmektedir.

Fertlerin iradelerini ulusa, ulusun iradesini devlete teslim eden tarihsel süreç, ilahi vasıflarla donattığı modern devleti doğurduğunda henüz telgraf dahi icat edilmemişti. Çizilen sınırlar, kişilerin ve eşyaların bir taraftan diğerine geçişine yeni bir nizam getirirken; bilginin iletimi, bundan bağımsız kalamazdı. O kerte de posta, telgraf ve telefon teşkilatları hem ulusal hem uluslararası bağlamda ortaya çıkıp, nizamın iletişim sahasına hâkimiyetinin öncülüğünü yaptılar. Radyo ve televizyonun meydan okuması, devlet için resimli bir tost makinesininkinden² daha zorlu değildi. Soğuk Savaş döneminde yörüngelere oturmaya başlayan uydular dahi devletler ve uluslararası hukuk bakımından gerçek bir güçlük teşkil etmemiştir.

Bilgisayar ve devamında işlemeye başlayan internet ise sadece iletişimi değil; ticareti, finansı, kamu hizmetlerini, kitle hareketlerini ve hatta savaşları etkileyerek insan algısında yeni bir boyuta taşıdı. Elektriğin veriye dönüşmesi ve her geçen gün artan işlem kabiliyeti, salt insanlar arası iletişim bağlamında kalmayıp, insan ve cansız varlık (makine) ilişkisinde “siber” evresine geçişin de yolunu açtı. 1990'ların heyecanı, özünde bir bilimkurgu fenomeni olan siber uzay, akademik literatürün ve bilhassa hukukun ciddi konularından biri haline getirdi. Zira siber uzayın devlete ve uluslararası sisteme meydan okuması, öncekilerden çok daha farklıydı.

Hukuk akademisi, 30 yılı aşkın süredir siber uzay üzerine tartışmaktadır. İlk zamanlar, menşesine sadık kalınmak suretiyle, alternatif bir hayatın sürdüğü sanal bir evren olarak kabul edilen siber uzay, günümüzde çok daha kapsamlı ve gerçekçi bir

¹ John Perry Barlow, “A Declaration of the Independence of Cyberspace”, Electronic Frontier Foundation, <https://www.eff.org/tr/cyberspace-independence> (31.12.2024).

² Cass R. Sunstein, “The First Amendment in Cyberspace”, *The Yale Law Journal*, Vol.104, No.7, (1995), s.1760.

yaklaşım ile ele alınmaktadır. Devletler, bu olguyu bir süre doğal gidişatına bırakırken, sonradan yoğun şekilde hukuki düzenlemelere konu etmeye başlamıştır. Uluslararası hukuk da başta Birleşmiş Milletler ve bölgesel nitelikteki uluslararası örgütler bünyesindeki girişimlerle şekillenmeye devam etmektedir. Geline nokta, siber uzayı düzenleyen kapsamlı ve küresel bir uluslararası antlaşma henüz ortaya konamamış; ancak siber suçlar ve siber güvenlik alanlarında bölgesel nitelikteki uluslararası antlaşmalar akdedilebilmiştir. Gelişim aşamasında olan uluslararası örf ve âdet hukuku kurallarının tespiti yönündeki akademik faaliyetler de sürmektedir.

Siber uzaya dair akademik literatür, ekseriyetle siber operasyonlar ve bilişim suçları üzerinde yoğunlaşmıştır. Siber uzayın doğrudan, hukuk, uluslararası hukuk ya da devlet egemenliği ile ilişkisi bağlamında (Türkçe literatürdeki az sayıda örnek de dahil olmak üzere) üretilen eserlerden, eldeki çalışmanın hazırlanma sürecinde tespit edilebildiği kadarına, çalışma içerisindeki muhtelif noktalarda atıfta bulunulmuştur.

Bu tez çalışmasının başlığı olarak seçilen “Uluslararası Hukukta Devlet Egemenliğinin Bir Konusu Olarak Siber Uzay” ibaresi, ilk olarak siber uzay olgusunun egemenlikle ilişkisine dair tercih edilen bir konumlanmayı yansıtmaktadır. Ayrıca, egemenliğin modern dönemde devlete nispet edilen bir nitelik olduğu ve egemen devletlerin varlığından bahsedilecekse, meselenin modern uluslararası hukuk bağlamında değerlendirilmesi gerektiği hakikatine işaret edilmektedir. Devletin bir olguyla ilişkisini, kendi ulusal sınırları içerisinde incelemek de pek tabii mümkündür. Fakat olgu tüm devletlerin aynı anda temasına açık nitelikteyse, bir sepet dolusu yumurtayı kırmadan taşımanın çabası olan uluslararası hukuk kaçınılmaz olarak incelemenin merkezine oturacaktır.

“Siber uzayda devlet egemenliği” düşüncesine muhalif sesler artık nadiren duyulmaktadır. Ancak devletin siber uzaydaki egemenliğinin nasıl yorumlanacağı, kapsamı, icra şekli gibi birçok husus hakkında belirsizlikler sürmektedir. Aslında sadece siber uzayda değil, yaşamın binlerce yıldır devam ettiği fiziksel uzayda da egemenlik olgusunun çok sayıda gri bölgesinin varlığından bahsedilebilmektedir. Karayı, denizi ve havayı ülkeye dönüştüren devletin buralarda neler yapabileceği, denizin ve havanın ne kadarına hâkim olduğu, uzayda hangi haklara sahip olduğu gibi meseleler uluslararası

hukukta hâlen canlılığını korumaktadır. Diğer yandan, egemen eşit devletlerin aralarındaki alıngan ve kırılğan ilişkiler, birbirlerinin siyasi bağımsızlığına müdahale etmeme yükümlülüğünün kapsamını karmaşık bir hale sokmuştur. Yerleşik uluslararası hukuk, bütün bu sorunlarıyla günümüze tevarüs ederken; siber uzay gibi sınır aşan bir olgunun doğuşu, cevap bekleyen yeni soruları da beraberinde getirip, ilgili sorunların derinleşmesine sebep olmuştur. Eldeki çalışma pek tabii siber uzayın uluslararası hukukta doğurduğu tüm sorulara cevap bulmayı amaçlamamaktadır. Lakin uluslararası hukukta devlet egemenliği bağlamında, literatür tartışmalarına konu olan aşağıdaki temel sorulara cevap aranması zaruri görülmüştür:

Siber uzay nedir; soyut ve sanal olarak deneyimlenebilir ayrı bir mekân mıdır yoksa fiziksel unsurların da dahil olduğu çok boyutlu bir yapı mıdır?

Devletlerin “egemen” yapılar olması ne anlama gelir; egemen devleti doğuran koşullara nispetle günümüz egemenlik anlayışının kapsamı ve unsurları dikkate alındığında, bir olgunun egemenliğe konu olabilmesi hangi şartlara tabidir?

Siber uzay, egemen devletin kollarının erişemeyeceği bir kurtarılmış bölge midir; yoksa ulusal ve uluslararası hukuk düzenlemelerine konu olması mümkün veya gerekli midir?

Devlet, siber uzayda hangi yetkilere sahiptir; yetki icrasında karşılaşılan sorunlar nelerdir ve bunların nasıl üstesinden gelinebilir?

Egemen devlet için bir “siber ülke” var mıdır; varsa mahiyeti ve sınırları nasıl tespit edilebilir?

Hangi devlet fiilleri, diğer bir devletin siber uzaydaki egemenliğini ihlal eder?

Çalışmada, tartışmalı hususlara yönelik literatürün ve vakaların yorumlanması sonucunda, tercih edilen yaklaşımın gerekçesiyle birlikte izah edilmesi usulü izlenmiştir. Siber uzay hakkındaki meselelere dair çözümlemeler, konunun devingen yapısı gereği sıklıkla güncellenmektedir. Bu sebeple, mümkün olduğunca, yerleşik ilke ve esaslar üzerinden hareket edilmiş; siber uzay ile ilişkili sayısız vaka arasından, konunun amacına uygun ve güncel olanlara yer verilmesi için gayret gösterilmiş; süregelen tartışmalar,

yazar görüşlerinin ve devlet pozisyonlarının zaman içinde gösterdiği değişim gözetilerek ele alınmıştır.

Konunun bilgi ve iletişim teknolojileri ile doğrudan ilişkili olması, neredeyse tamamen İngilizce kökenli olan bir terminolojik zeminde çalışılmasını gerektirmiştir. Modern uluslararası hukuk terminolojisi zaviyesinden de benzer durumun söz konusu olduğu malumdur. Çalışmada terimlerin Türkçe karşılıklarının tercih edilmesine özen gösterilmiştir. Kullanılan terimlerde sarahatin sağlanması açısından, kaynak dildeki ifadeler de parantez içlerinde belirtilmiştir.

Siber uzay, teknolojinin insan algısına etkisinin sonucu olarak, sanallığı ve gerçekliği bir arada barındırmaktadır. Ayrıca hukuk düzenlemelerine konu olan olguların en genç olanlarından. Bu sebeple siber uzay ve hukuk ilişkisine dair literatür, metafor ve analogilerle doludur. Mevcut şartlarda, bu yollara başvurulması kısmen kaçınılmazdır. Diğer taraftan hukuk açıklık, belirlilik ve kesinlik gerektirmektedir. Dolayısıyla eldeki çalışmada da yer yer metafor ve analogilere başvurulmuş olsa dahi nihayetinde siber uzayın incelenmesinde realist bir yaklaşım izlenmeye çalışılmıştır. Bu alandaki çalışmalarda isabetli sonuçlara ulaşabilmek adına realizmin dozunun doğru ayarlanması ise kritik önem taşımaktadır.

Güvenlik ve özgürlük, düzenleme ve serbestlik, devletler ve şirketler, küreselleşme ve egemenlik gibi ikiliklerden müteşekkil fay hatlarının en aktif olduğu alanlardan biri siber uzaydır. Eldeki çalışmanın amacı, söz konusu kutuplardan birinin tarafgirliğini ve savunmasını yapmak değildir. Öncelikle var olan hukuku tespit etmek; gerekli görülen yerlerde de başta hakkaniyet ve diğer hukuk ilkelerine dayanarak, olması gereken hukuka yönelik mülahazalarda bulunmak amaçlanmıştır.

Bu tez çalışması, üç ana bölümden oluşmaktadır. Her bir bölüm de kendi içinde iki ana başlığa ayrılmıştır. Birinci bölümün ilk başlığında siber uzayın; ikinci başlığında egemenlik kavramının mahiyeti ele alınmıştır. Aslında ne olduğuna yönelik dahi bir mutabakatın bulunmadığı siber uzay için önemli bir tanım problemi söz konusudur. Zira tanımlardaki ihtilaf, yalnız teferruata değil; bizzat kavramın özüne de taalluk etmektedir. Bu çalışmada ise *“uluslararası hukukçular için kelimeler, uluslararası hukukçular ne*

anlama geldiğine karar verirlerse o anlama gelir”³ düsturunca, çalışmanın amaç ve kapsamına uygun bir tanım ve modelleme öngörülmüştür. Böylece siber uzay, özgün bir yaklaşım aranarak, “boyutları” ve “unsurları” ile modellenmiştir. Ayrıca hem siber uzay hem egemenlik mefhumlarının izahında “hiçbir tesis hakkında, mazisi bilinmedikçe malumatımız tamam olamaz”⁴ düsturunca, mefhumları ortaya çıkaran tarihsel sürecin ana hatları ve kırılma noktaları üzerinden hareket edilmiştir. Çalışma boyunca rehberlik etmesi bakımından, uluslararası hukukta devlet egemenliğine hâkim ilkelere ve kurallara da birinci bölümde yer verilmiştir.

Bir olgunun egemenliğe konu olması, en başta hukuk düzenlemelerine konu olması anlamına gelmektedir. İkinci bölümün ilk başlığında, siber uzayın bu vafına yönelik tartışmalar ele alınmıştır. Nitekim siber uzayın egemenlikten azade olması ile egemenliğe konu olması arasındaki esas fark bu tartışmaların kodlarında saklıdır. Günümüzde her ne kadar tartışmanın kazananı belli gibi görünse de uygulamadaki zorluklar ve teorideki gri bölgeler, hâlen katedilmesi gereken mesafelerin varlığına delalet etmektedir. Hukuk düzenlemelerine konu olma meselesinin egemen devletler arasındaki görünümü ise uluslararası hukuk disiplininde tezahür edecektir. Buna binaen ikinci başlıkta, uluslararası hukuk bağlamında siber uzayın düzenlenmesine yönelik girişimlere ve sonuçlarına yer verilmiştir. Birleşmiş Milletler bünyesinde özel hukuk süjelerinin de katılımıyla devam eden süreçler ve bazı bölgesel uluslararası örgütlerin yürürlüğe koymayı başardığı antlaşmalar, bu başlığın ana unsurlarıdır.

Üçüncü bölümde, siber uzay üzerinde devlet egemenliğinin görünimleri ve sorunları, literatürde zaman zaman kullanılan iç egemenlik – dış egemenlik ayrımının izdüşümünü yansıtacak şekilde iki başlıkta ele alınmıştır. Birinci bölümde modellenmiş olan siber uzayın boyutları ve unsurları üzerinde devletin sahip olduğu yetkiler; uluslararası hukukta devletin yetkisine dair esaslar çerçevesinde, üçüncü bölümün ilk başlığında tahlil edilmiştir. Düzenleme, icra ve yargı yetkilerine dair sorunlara ve birtakım önerilere burada yer verilmiştir. İkinci başlıkta ise “siber egemenlik” teorisi bağlamında; “siber ülke” ifadesiyle karşılık bulan, siber uzayda fiziksel uzaydaki gibi

³ Steven Wheatley, “Foreign Interference in Elections under the Non-intervention Principle: We Need to Talk about ‘Coercion’”, *Duke Journal of Comparative & International Law*, Vol.31, No.1, (2020), s.195.

⁴ Cemil Bilsel, *Devletler Hukuku: Giriş*, İkinci Bası, İstanbul: İstanbul Üniversitesi Yayınları, 1940, s.80.

sınırlar çizme fikrinin imkânı sorgulanmıştır. Devamında da devletlerin siber uzaydaki egemenliklerinin hangi durumlarda ihlal edilmiş olacağına dair *lex lata* tespitlerde ve *de lege ferenda* değerlendirmelerde bulunulmuştur.



Birinci Bölüm

SİBER UZAY VE EGEMENLİK

I. SİBER UZAY

Tanım yapmak, birçok disiplin dâhilinde en zor ve hassas akademik faaliyetler arasındadır. Hukuk disiplini ise tanım, doğuracağı sonuçlar bakımından ayrıca önem arz etmektedir. Yapılan tanımın geleneksel olarak ifade edildiği üzere “efrâdını câmi, ağyârını mâni” olması, hukuk normlarının bir kavram üzerine inşa edilip uygulanması sürecinde özen gerektiren bir husustur.

İnsanlığın hukuk ile olan ilişkisinin geçmişine kıyasla siber uzay (*cyberspace*) kavramının henüz emekleme aşamasında olduğunu ifade etmek mümkündür. Çeşitli alanlardan önde gelen yazarlar bu kavrama yönelik farklı tanımlamaları tercih ederken; yerli literatürde tanımın yanı sıra tercüme açısından da farklılıklar görülmektedir. İdeali bulma iddiası için henüz erken bir dönemde olunmasına rağmen, eldeki çalışmanın sağlam temellere oturması adına en doğru kavramsal zeminin hususen tespit edilmesi gerekmektedir. Zira uluslararası hukuk ve devlet egemenliği gibi halihazırda derinlikli ve tartışmalı alanlarla ilişkilendirilecek olan siber uzay kavramının, hukuk mühendisliği açısından üzerinde çalışılacak bir malzeme olarak görülüp iyi tanınması elzemdir. Bu bakımdan siber uzayı ayrıntılı şekilde analiz etmeden önce “siber uzay” kavramının tanımı üzerinde durulacak, ardından da “uzay” tercümesinin tercih gerekçesinden bahsedilecektir.

A. Tanım ve Tarihsel Gelişim

1. Kubernetes ve Sibernetik

Esasen tek başına anlam taşımayan ve günümüzde siber saldırı, siber uzay, siber savaş, siber suçlar vb. çok sayıda farklı ifadeyi oluşturmakta ön ek görevi bulunan “siber” kelimesi, etimolojik açıdan oldukça ilgi çekici bir serüvene sahiptir. Siberin ön ek teşkil ettiği kelimelerden biri olan ve eldeki çalışmaya esas olan siber uzay kavramı,

günümüzdekine yakın anlamıyla ilk olarak *William Gibson* tarafından kullanılmıştır.⁵ *Gibson*, 1984'te yayımlanan "Neuromancer" isimli eserinde siber uzayı "her ulustan milyarlarca ehil kullanıcının, matematiksel kavramlar öğretilen çocuklara benzer şekilde her gün deneyimlediği, mutabakata dayalı bir halüsinasyon. İnsan sistemindeki bütün bilgisayarların hafızalarından soyutlaştırılmış verilerin görsel temsili. Akıl almaz gerçeklik" şeklinde tanımlamıştır.⁶ Aynı yazarın 1982 yılındaki "Burning Chrome" eserinde de bu kavrama yer vermiş olduğu görülse dahi kavramın esas popülerliğini *Neuromancer*'ın edebiyat dünyasındaki başarısıyla kazandığı görülmektedir.⁷

Gibson'ın siber uzayı türetmesindeki ilham kaynağının, "sibernetik (*cybernetics*)" kavramını bugünkü anlamında kullanan ilk kişi olarak bilinen *Norbert Wiener* olduğu söylenebilir. 2. Dünya Savaşı sürecinde, farklı alanlarda uzmanlık sahibi çok sayıda bilim insanı sistem teorisi, kontrol ve iletişim üzerine çalışmalar yapmıştır. Ortak yapılan çalışmalarda, uzmanlar arasında büyük bir iletişim problemi yaşandığı ve ortak bir kavramsal zeminde buluşmakta zorlanıldığı aktarılmaktadır.⁸ Nihayet *Wiener*'in ifadesiyle, ister canlı dokularda ister makinelerde olsun; iletişim, kontrol ve istatistiksel mekanik merkezinde beliren problemler dizisinin esaslı bütünlüğünün farkına varılmıştır.⁹ *Wiener*, çalıştıkları multidisipliner alanı ortak bir başlık altına alıp dil ve terminoloji birliği sağlama ihtiyacına binaen, bilim dünyasında sıkça rastlandığı üzere Neo-Yunanca bir kavram bulmak maksadıyla arayışını Antik Yunan'a çevirmiş ve "dümenci" anlamındaki *κυβερνητικης* kelimesinin latinize hali olan "sibernetik (*cybernetics*)" kavramını tercih etmiştir.¹⁰ Kavramın, *Platon*'un "1. Alkibiades" eserinde, kaptanların alanlarında uzmanlaşarak sahip oldukları "kaptanlık aklı" yahut "seyir bilgi ve becerisi" anlamında kullanımına rastlanmaktadır.¹¹ "Kubernetes" olarak ifade edilen

⁵ *Gibson*'dan önce 1968-1970 yıllarında Danimarkalı sanatçılar *Susanne Ussing* ve *Carsten Hoff*, "Atelier Cyberspace" imzalı eserler ortaya koymuştur. Fakat bilgisayarların henüz yaygınlaşmadığı dönemde buldukları bu isim, siber uzayın günümüzdeki anlamından ziyade doğrudan sibernetik esaslı bir türetmedir; Jacob Lillemose ve Mathias Kryger, "The (Re)invention of Cyberspace", *Kunstkrityk*, 24.08.2015, <https://kunstkrityk.com/the-reinvention-of-cyberspace/> (31.12.2024).

⁶ William Gibson, *Neuromancer*, SF Masterworks, London: Orion Publishing, 2022, s.59.

⁷ Tore Rye Andersen, "Cyberspace Revisited: A Radial Reading of William Gibson's "Burning Chrome"", *The Journal of American Culture*, Vol.42, No.2, (2019), s.121.

⁸ Stafford Beer, "What is cybernetics?", *Kybernetes*, Vol.3, Iss.3/4, (2004), s.856.

⁹ Norbert Wiener, *Cybernetics or Control and Communication in the Animal and the Machine*, Second Edition, Fourth Printing, USA: MIT Press, 1985, s.11.

¹⁰ *Ibid.*

¹¹ Trevor J. Saunders, *Notes on the Laws of Plato*, Bulletin Supplement, University of London. Institute of Classical Studies, No.28, 1972, s.127.

bu kavram, zaman içerisinde Roma’da latinize edilerek “*gubernator*” şeklinde kullanılmış ve İngilizce’de “*governor*” olarak yer bulmuştur.¹² Antik Yunan’da zorlu hava ve deniz koşullarında gemiyi deniz fenerine doğru yönlendirmek adına dümende durmaksızın çaba sarf eden ve değişken şartlar karşısında eşzamanlı tepkiler vermeyi gerektiren bir yönetim görevi üstlenen “dümenci” ile bugün hükümet anlamına gelen “*government*” ve vali anlamındaki “*governor*” kelimelerinin aynı kökten gelmesi hem ilgi çekici hem de sibernetiğin doğasını anlamak adına açıklayıcıdır. Dümencinin, yönlendirdiği gemiyle olan ilişkisinin karşılıklılık arz etmesinin de üzerinde ayrıca durulmalıdır. Dümenci gemiyi yönetmeye çalışırken gemiyle birlikte hareket etmektedir. Geminin seyrüseferi ve dümencinin fiilleri, ortak bağlamda eşzamanlı bir geribildirim mekanizması doğurmaktadır. Bu durum, yönetilenden bağımsız ve tepeden bir yönetim ilişkisinin aksi yönündedir ve ilerleyen bölümlerde ele alınacak olan siber uzayın yapısına kısmen hâkim “yönetişim” kavramını da çağrıştırmaktadır. Ayrıca insan – makine etkileşiminde yeni bir merhaleye geçişi vurgulaması bakımından, modern siber kavramına zemin oluşturmaktadır.

Wiener her ne kadar önceki eserinde, amaçlarına yönelik ilk dikkat çekici eserin, *Clerk Maxwell*’in tahrik gücündeki ve dirençteki değişimlere rağmen makinenin hızını sabit tutmaya yarayan parça için “*governor*”¹³ kelimesini kullandığı 1868 yılındaki “*On Governors*”¹⁴ makalesi olduğunu belirtse de,¹⁵ bu kavramın daha önceki bir tarihte *André Marie Ampère* tarafından siyaset bilimi ile ilişkili olarak kullanıldığını sonradan öğrendiğini ileri tarihli bir eserinde ifade etmiştir.¹⁶ Gerçekten de *Ampère*, Fransız Ulusal Bilimsel Araştırma Merkezi (*Centre National de la Recherche Scientifique* (CNRS)) arşivlerinde bulunan el yazmalarında¹⁷ ve 1843 yılındaki “*Essai sur la Philosophie des Sciences*” eserinin 2. Cilt ekinde görüldüğü üzere “*cybernétique*” kavramını, doğru

¹² Beer, s.857.

¹³ Türkçe’de de benzer parçalar governör ya da governor olarak adlandırılmaktadır; Şaban Böyük, “Bulanık Mantık Yöntemi ile Jeneratörlerde Devir Kontrolü ve Yük Paylaşımı için Elektronik Governör Tasarımı ve Uygulaması”, (Yüksek Lisans Tezi, Marmara Üniversitesi Fen Bilimleri Enstitüsü Mekatronik Anabilim Dalı, 2011); Adem Dalcı, Emre Çelik ve Serdal Arslan, “Mikro ve Mini Hidroelektrik Santralleri için Mikrodenetleyici Tabanlı bir Elektronik Governor Sisteminin Tasarımı”, *Erciyes Üniversitesi Fen Bilimleri Enstitüsü Dergisi*, Cilt.28, Sayı.2, (2012), s.130.

¹⁴ J. Clerk Maxwell, “On Governors”, *Proceedings of the Royal Society of London*, Vol.16, (1868), s.270.

¹⁵ Wiener, s.11.

¹⁶ Norbert Wiener, *The Human Use of Human Beings: Cybernetics and Society*, London: Free Association Books, 1989, s.15.

¹⁷ Centre National de la Recherche Scientifique, Chemise 483, Carton 36, http://www.ampere.cnrs.fr/ice/ice_book_detail.php?lang=fr&type=img&bdd=koyre_ampere&table=ampere_mats&bookId=483&typeofbookId=1&num=0&&num=204 (31.12.2024).

siyaset (*politique proprement dite*) başlığı altında, güç teorisi (*théorie du pouvoir*) kavramının yanında kullanmıştır.¹⁸

Yerli literatürdeki bazı metinlerde, birbirine benzer ifadeler kullanılmak suretiyle, siber kelimesinin ilk kez 1958 yılında *Louis Couffignal* tarafından kullanıldığı yönünde bilgi verilmektedir.¹⁹ *Couffignal*'e “sibernetiğin babası” unvanı da atfeden bu bilgi kalıbı için yapılan atıflar incelendiğinde güncel kök kaynağın “Sesli Sözlük” internet sitesi olduğu görülmektedir.²⁰ Bu yönde tespit edebildiğim en eski atfın ise “Vikipedi” internet sitesine olduğundan²¹ hareketle, ilgili sitedeki maddede yapılan düzenleme kayıtlarına göre 2006 yılından 2021 yılına kadar bilginin söz konusu haliyle bulunduğu, 2021 yılında yapılan düzenleme sonrasında bu ifadenin kaldırıldığı dikkate alındığında,²² literatürdeki sorunun, Vikipedi internet sitesinde yer alan eski ve hatalı bilginin gerek internet ortamındaki diğer sitelerde gerekse akademik çalışmalarda yayılması sonucunda ortaya çıktığı kanaatindeyim. *Louis Pierre Couffignal* her ne kadar sibernetik alanında önemli çalışmalar yapmış olsa da kavramın ortaya çıkış sürecinin yukarıda anlatıldığı şekilde olduğu görülmektedir.

2. İnternet ve Web

İnsanın tabiatı anlama ve yaşamı buna göre tasarlayıp yönetme çabasının bir uzantısı olan sistem teorisi ve sibernetik akımı, modern dönemde öne çıkmıştır. İnternet de söz konusu çabanın günümüzdeki en etkin ve yaygın ürünü olarak değerlendirilebilir. Teknoloji ne kadar ilerlese de iletişim, haberleşme ve yönetim amaçlarına hizmet eden bütün teknikler aslında aynı konseptin zamanla gelişmiş yansımalarıdır. Bizans'ın 9. yy'da Müslüman akınlara karşı Hasan Dağı'ndan İstanbul'a kadar belirli aralıklarla ateşli sinyal kuleleri inşa ederek, haberlerin 720 km gibi bir mesafeyi bir saat içinde kat etmesini

¹⁸ André Marie Ampère, *Essai sur la Philosophie des Sciences ou Exposition Analytique d'une Classification Naturelle de Toutes les Connaissances Humaines: Seconde Partie*, Paris: Bachelier, Libraire-Éditeur, Quai Des Augustins, 55, 1843, s.181.

¹⁹ Bazı örnek eserler için bkz. Sevdâ Korhan, “Siber Uzayda Uluslararası İlişkilerin Değişen Parametreleri”, (**Yüksek Lisans Tezi**, Selçuk Üniversitesi Sosyal Bilimler Enstitüsü, 2018), s.4; Onur Yılmaz, “Küreselleşme Sürecinde Dönüşen Güvenlik Algısı ve Siber Güvenlik”, *Cyberpolitik Journal*, Cilt.2, Sayı.4, (2018), s.28; Müberra Altuner ve Fatma Çakır, “Siber Uzay ve Uluslararası İlişkiler/ Teorisi”, *Cyberpolitik Journal*, Cilt.2, Sayı.4, (2018), s.183.

²⁰ Cyber..., Sesli Sözlük, <https://www.seslisozluk.net/cyber...-nedir-ne-demek>, (31.12.2024).

²¹ Ender Şahinaslan, Önder Şahinaslan ve Selçuk Selimli, “Siber Saldırıların Kritik Altyapılar Üzerindeki Etkileri”, Mustafa Akgül ve Diğerleri (Ed.), *XV. Akademik Bilişim Konferansı Bildirileri* içinde (128-131), Antalya: İnternet Teknolojileri Derneği, 2013, s.129.

²² <https://tr.wikipedia.org/w/index.php?title=Siber&action=history>, (31.12.2024).

sağlayan sistem kurması²³ da bu konseptte dahil bir örnektir. Öyle ki; 19. yy'ın hemen başında, İngiltere'nin Devon Kontluğu'nda, aynı sitemle şehri bir ağ gibi sararak günümüz ağ haritalarına benzeyen bir işleyiş meydana getirildiği de görülmektedir.²⁴ Atlı habercilerden posta teşkilatlarına ve telgraftan uydu sistemlerine kadar iletişimin uzun tarihi, konuyla yakinen ilişkili olsa da eldeki çalışmanın amaç ve kapsamını aşmadan internetin özünü ifade etmek için bu düşünceleri aktarmak kâfi olacaktır.

Soğuk Savaş atmosferindeki 1958 yılında Amerika Birleşik Devletleri (ABD) Savunma Bakanlığı tarafından “İleri Araştırma Projeleri Ajansı (*Advanced Research Projects Agency* (ARPA))”²⁵ kurulmuştur. 2. Dünya Savaşı'nda atom bombasının kullanılması trajik bir “teknolojik sürpriz” örneği idi. ARPA'nın temel fonksiyonunun “ABD aleyhine teknolojik sürpriz yaşanmasını engellemek” olduğu, bunun da ancak “sürprizleri yapan taraf” olmakla mümkün olduğu değerlendirilmiştir.²⁶ Nükleer savaş tehdidinin yükseldiği dönemlerde, olası nükleer saldırı durumunda emir komuta sisteminin işlevini devam ettirebilmesini sağlayacak bir iletişim sistemi ihtiyacı doğmuştur.²⁷ Bu amaçla önerildiği üzere dağıtık ağların (*distributed network*) paket anahtarlama (*packet switching*) yöntemiyle çalışması prensibi²⁸ uygulanan ve ARPA araştırmacılarının bilgisayarlar vasıtasıyla iletişim kurmalarını sağlamak maksadıyla 1969'da faaliyete geçen ARPANET (*Advanced Research Projects Agency Network*) , günümüzde internet olarak adlandırılan yapının temelini oluşturmuştur. 1983'te, ARPANET'in araştırma amaçlı kullanılan ağı aynı isimle devam ederken; askeri amaçlı ağ, MILNET (*Military Network*) adıyla ayrılmıştır. Ağda kullanılan Ağ Kontrol Protokolü'nden (*Network Control Protocol* (NCP)) İletim Kontrol Protokolü / Internet Protokolü'ne (*Transmission Control Protocol / Internet Protocol* (TCP/IP)) geçiş de bu

²³ Philip Pattenden, “The Byzantine Early Warning System”, *Byzantion*, Vol.53, No.1, (1983), ss.258-299.

²⁴ Devon City Council, “Fire Beacons; Warning Signals Across the Countryside”, s.7, <https://devoncc.sharepoint.com/sites/PublicDocs/Environment/Historic/Forms/AllItems.aspx?id=%2Fsites%2FPublicDocs%2FEnvironment%2FHistoric%2FSchools%2FFire%20Beacons%2Epdf&parent=%2Fsites%2FPublicDocs%2FEnvironment%2FHistoric%2FSchools&p=true&ga=1> (31.12.2024).

²⁵ US Department of Defence, Department of Defence Advanced Research Projects Agency, **Directive 5105.15**, 07.02.1958.

²⁶ Stephen J. Lukasik, “Why the Arpanet Was Built”, *IEEE Annals of the History of Computing*, Vol.33, Iss.3, (2011), s.6.

²⁷ Ibid., s.9.

²⁸ Saldırı senaryolarına göre sistem alternatiflerinin verimliliğine yönelik analizler ve söz konusu prensip hakkında ayrıntılı bilgi için bkz. Paul Baran, **On Distributed Communications Networks**, The RAND Corporation, R-2626, Santa Monica, 1962.

yılda gerçekleşmiştir.²⁹ 1989’da da amacını başarıyla gerçekleştirmiş olan ARPANET kapanmıştır.³⁰ Bu süreç, ABD Ulusal Bilim Vakfı’nın (*National Science Foundation* (NSF)) ülke çapındaki birçok üniversiteyi birbirine bağlama çalışmalarının sonucu olarak 1986’da NSFNET’i (*National Science Foundation Network*) faaliyete geçirmesiyle paralellik taşımaktadır.³¹ NSFNET ile internetin omurgası oluşmuş; koordinasyonu ise İnternet Tahsisli Sayılar ve İsimler Kurumu’nun (*Internet Corporation for Assigned Names and Numbers* (ICANN)) 1998’de yetkilendirilerek özelleştirilmesine kadar devlet marifetiyle sürdürülmüştür.³²

Yukarıda arz edilenlerden anlaşılacağı üzere “internet”; esas itibarıyla iletişim ve veri paylaşımı amaçlı, belirli teknik standart ve kurallara göre kurulup işletilen bir dağıtık bağlantı sistemidir. Uygun cihazları, uygun fiziksel altyapıya bağlamak suretiyle internetin bir parçası olunmaktadır. Telefon ya da telgraf ağları da kendi standart ve kuralları dâhilinde farklı bağlantı sistemi örnekleri olarak gösterilebilir. İnterneti başka sistemlere göre çok ileri noktaya taşıyan ilk unsur şüphesiz ki bilgisayar ve ağ bağlantı teknolojilerinin gelişimidir. Bu ileri seviye teknolojik altyapı da Web fikrine yaşam alanı sağlayarak “sanal alem” ifadesiyle karşılık bulan ortamı günümüze kadar taşımıştır.

Cenevre’de faaliyetlerini sürdüren Avrupa Nükleer Araştırma Merkezi (*Conseil Européen pour la Recherche Nucléaire* (CERN)), belirli periyotlarla bünyesinde çalışıp ayrılan araştırmacıların ürettiği verilerin, toplanıp koordine edilerek, yeni araştırmacıların da faydalanabileceği şekilde birikimli hale getirilmesi amacıyla bir formül arayışına girmişti. ARPANET ve NSFNET dönemlerine tekabül eden bu süreçte internet belki ortaya çıkış amacını karşılamıştı ama kullanımı uzmanlık istiyordu, altyapısı çok pahalı ve karmaşıktı ayrıca sınırlı amaçlar dışında verimli kullanımı mümkün değildi.³³ CERN’de görevli olan *Tim Berners-Lee* 1989’da sunduğu “Bilgi Yönetimi: Bir Öneri”

²⁹ Ronda Hauben, “From the ARPANET to the Internet”, 23.06.1998, http://www.columbia.edu/~rh120/other/tcpdigest_paper.txt (31.12.2024).

³⁰ Lukasik, s.17.

³¹ NSF, “A Brief History of NSF and the Internet”, https://www.nsf.gov/news/news_summ.jsp?cntn_id=103050 (31.12.2024).

³² Susan Schiavetta ve Konstantinos Komaitis, “ICANN’s Role in Controlling Information on the Internet”, *International Review of Law, Computers & Technology*, Vol.17, No.3, (2003), s.268 vd.

³³ Tim Berners-Lee, *Weaving the Web: The Original Design and Ultimate Destiny of the World Wide Web by It’s Inventor*, New York: Harper Collins Publishers, 2000, s.18.

başlıklı çalışmasında, dağıtık “hiper metin (*hypertext*)”³⁴ sistemini temel alan bir çözüm öngörmüştü.³⁵ Bu sistem için de tabii ki en uygun altyapı internetti. Bu sayede dünyanın çeşitli yerlerinde bulunan kullanıcıların internet üzerinden aynı bilgilere farklı bilgisayar sistemleriyle ulaşmaları ve bilgilerin bulunduğu hiper metinlere kendi özel bağlantılarını (*link*) eklemeleri sağlanmış; ayrıca daimî değişkenlik arz eden bilgilere eş zamanlı erişmeyi sağlayan “canlı” bağlantıların kurulması mümkün hale gelmiştir.³⁶ Önerinin 1990’da kabulünü izleyen süreçte işlemeye başlayan sisteme ise “Dünya Çapında Ağ (*World Wide Web (WWW)*)” adı verilmiştir.³⁷

Paket anahtarlama mantığı gereği, ileti transferinde paketin bir cihazdan başkasına ulaşabilmesi için internete bağlı her cihazın bir IP adresine sahip olması gereklidir. Dolayısıyla bir Web sitesine erişmek istendiğinde, siteyi barındıran cihazın - sunucunun (*server*)- adresine ihtiyaç duyulmaktadır. Bu adreslerin de bilinirliğinin sağlanması ve kullanıcı dostu olması amacıyla çok sayıda rakamdan³⁸ oluşmuş karmaşık IP adresleri yerine; bu IP adresleriyle eşleştirilen “www.marmara.edu.tr” gibi alan adları tercih edilmiştir. Alan Adı Sistemi (*Domain Name System (DNS)*) de özet olarak, bu unsurların ve eşleştirmelerin dağıtık şekilde tutulduğu bir veri tabanını ifade etmektedir.³⁹

Web sayesinde metin ve medya öğelerini barındıran sayfalar, yine barındırdıkları linklerle birbirine bağlanmış ve böylece internetin sağladığı fiziksel ağın üzerinde “yaşayan” bir soyut ağ ortaya çıkarmıştır. Web sayfalarının hiper metin sayesinde sahip olduğu bu özellikler sebebiyle, Web’in ilk yıllarından itibaren birçok yazar bu sistemi sanal bir uzay metaforu kullanarak tanımlamıştır.⁴⁰ Bu yöntem, *Gibson* tarafından kurgulanıp adlandırılan yapıya oldukça benzer vasıflarına binaen siber uzayı Web ile özdeşleştiren yaklaşımlara da kapı açmıştır. Gerçekten de internet ve Web’in insanlara

³⁴ Hiper metinler, salt yazıdan ibaret olmanın ötesinde, medya içeriği, diğer metinlere bağlantılar vs. özellikleri de içerisinde barındırabilen belgelerdir. Günümüzdeki “web sayfası” kavramının temeli, bu belge yönteminin ortaya çıkışıyla atılmıştır. Ayrıntılı bilgi için bkz. Roy Rada, “Writing and Reading Hypertext: An Overview”, *Journal of the American Society for Information Science*, Vol.40, Iss.3, (1989), s.164 vd.

³⁵ CERN, Tim Berners-Lee's Proposal, <http://info.cern.ch/Proposal.html> (31.12.2024).

³⁶ Tony Kippenberger, “How did We get to a World Wide Web?”, *The Antidote*, Vol.4, No.5, (1999), s.22.

³⁷ Berners-Lee, s.23; Eldeki çalışmanın devamında “Web” olarak ifade edilecektir.

³⁸ IPv4’ün 32 bitlik sisteminde adresler 193.140.143.43 gibi rakamlardan oluşurken; 128 bitlik gelişmiş versiyon IPv6 sistemine göre alınan adresler 2001:a98:a070:8c8f::2b gibi harf ve rakam kombinasyonlarından oluşabilmektedir.

³⁹ Milton L. Mueller, *Ruling the Root: Internet Governance and the Taming of Cyberspace*, The MIT Press, 2004, s.41.

⁴⁰ Rainer Bromme ve Elmar Stahl, “Is a Hypertext a Book or a Space? The Impact of Different Introductory Metaphors on Hypertext Construction”, *Computers & Education*, Vol.44, Iss.3, (2005), s.117.

sunduğu dijital ve mantıksal yapının, fiziksel uzaydakilere benzer fiillere imkân tanıyan yeni ve sanal bir alana benzetilerek yorumlanması makul bir zemine oturmaktadır. Fakat siber uzay, Web'i ve interneti de içermekle birlikte esasen daha geniş kapsama sahip bir olgudur.⁴¹ Bu konudaki görüşler ve siber uzayın mantıksal boyutunun detayları eldeki çalışmanın devamındaki başlıklarda hususen incelenecektir.

3. Tanımların Sınıflandırılması

Canlı organizmalar ve cansız varlıklar arasındaki (bilhassa insan ve makine) yönetim ve iletişim ilişkisinin bir ifade şekli olarak düşünülebilecek siber ön ekinin uzay ile birleşimi, günümüzde kökeninden farklı bağlamda ve müstakil bir anlamda kullanılmaktadır. Akademik literatürdeki çoğu kavramda olduğu gibi siber uzayın da üzerinde bütün paydaşların mutabık olduğu bir tanım bulunmamaktadır. Ansiklopedi ve sözlüklerin, devlet organlarının, sivil toplum kuruluşlarının ve yazarların farklı şekillerde yaptığı tanımlarla karşılaşmaktadır. Bu çalışmada, söz konusu kavramın mümkün olduğunca yüksek isabet oranıyla çerçevesinin çizilmesi ve özelliklerinin ortaya konması adına; çeşitli kaynaklar tarafından yapılmış belli başlı tanımlar seçilerek, aralarındaki benzerlik ve farklardan hareketle bir sonuca ulaşılması amaçlanmaktadır.

a. Ansiklopedik Sözlükler

Oxford Bilgisayar Bilimleri Sözlüğü'nde siber uzay için *“ilk olarak romancı William Gibson tarafından kullanıldığı düşünülen, dünyadaki tüm ağlarda bulunan bütün bilgisayarlardaki verilerin tamamına atıfta bulunan enformel bir kelime. Kelime, ağ üzerinden erişilebilen bilgisayar tabanlı verilerden oluşan geniş bir koleksiyona atıfta bulunmanın bir yolu olarak yaygın kullanıma geçmiştir”* ifadeleri kullanılmıştır.⁴² Britannica ise siber uzayı, *“belirli bir biçim sahibi olmayan, "sanal" olduğu kabul edilen, bilgisayarlar, internet özellikli cihazlar, sunucular, yönlendiriciler ve internet altyapısının diğer bileşenleri arasındaki bağlantılar tarafından oluşturulan dünya”*

⁴¹ Clemente, kümelerle şematize ederek internetin Web'i, siber uzayın da interneti kapsadığını belirtir; Dave Clemente, “Fundamentals of Cyber Security”, Larry MacFaul (Ed.), **Verification & Implementation – A biennial collection of analysis on international agreements for security and development** içinde (163-179), London: VERTIC, 2015, s.164.

⁴² Andrew Butterfield, Gerard Ekembe Ngondi ve Anne Kerr, “cyberspace”, **A Dictionary of Computer Science**, 7th Edition, Oxford University Press, 2016, s.130.

şeklinde tanımlamıştır.⁴³ Larousse Fransızca Sözlüğü’nde, siber uzay ile eşanlamlı olduğu belirtilen siber dünya (*cybermonde*), “*internet kullanıcıları topluluğunu ve bilgisayar ağları üzerinden erişilebilen dijital bilgi kaynaklarını bir araya getiren sanal alan*” ifadesiyle tanımlanmıştır.⁴⁴

Yukarıdaki tanımlarda farklı ifade biçimleri kullanılmakla birlikte aslında aynı sanal yapıya işaret edildiği görülmektedir. Oxford tanımında sanal yapının verilerden müteşekkil olma özelliği ön plana çıkarılmış; Britannica tanımında esas hareket noktası, yapının üzerinde yükseldiği fiziki altyapı olmuş; Larousse ise yapının kişiler ve verileri buluşturma özelliğini vurgulamıştır. Bu tanımlar üzerinden, söz konusu kaynaklarda siber uzayın mantıksal boyuttan ibaret görüldüğü sonucuna ulaşılabilecektir.

b. Devletler

Siber uzay söz konusu olduğunda yaklaşımı öncelikle incelenmesi gereken devlet, başta kavramın ve internetin kendi topraklarında doğması vesilesiyle konuyla ilgili en köklü literatüre sahip olan ABD’dir. ABD kurumları, kavram için farklı tanımlar yapmış ve bu tanımlar zaman içerisinde daha gelişkin hale gelmiştir. ABD Savunma Bakanlığı’nın yayımladığı terimler sözlüğünün erken dönemlerinde siber uzayın “*dijitalleştirilmiş bilginin, bilgisayar ağları üzerinden iletildiği kavramsal ortam*”⁴⁵ olduğu ifade edilirken; yakın dönemde “*internet, iletişim ağları, bilgisayar sistemleri, gömülü işlemciler ve kontrolörler dâhil olmak üzere bilgi teknolojisi altyapılarının ve yerleşik verilerin birbirine bağlı ağından oluşan bilgi ortamı içindeki küresel bir alan*”⁴⁶ şeklinde daha kapsayıcı bir tanıma gidilmiştir. Erken dönemde, yukarıdaki sözlük tanımlarına benzer bir yaklaşım söz konusuyken, son tanım ile siber uzayın verilerle oluşmuş kavramsal, soyut, varsayımsal bir alan mı yoksa çeşitli nitelikteki unsurları fiziki

⁴³ Jennifer Bussell, “cyberspace”, Britannica, <https://www.britannica.com/topic/cyberspace> (31.12.2024).

⁴⁴ Larousse, “cybermonde”, <https://www.larousse.fr/dictionnaires/francais/cybermonde> (31.12.2024).

⁴⁵ Joint Publication (JP) 1–02, DOD Dictionary of Military and Related Terms, Washington, DC: The Joint Staff, dated April 12, 2001, and amended through November 9, 2006.

⁴⁶ DOD Dictionary of Military and Related Terms, Washington, DC: The Joint Chiefs of Staff, March 2017, s.60; Joint Publication (JP) 3–12, Cyberspace Operations, Washington, DC: The Joint Chiefs of Staff, March 2017, GL-4. JP 1–02 ve JP 3–12 arasındaki ara dönemde, sözlüğün 2010 düzenlemesindeki tanım da büyük ölçüde aynı olmakla birlikte, tanıma sonradan “yerleşik veriler (*resident data*)” kavramının eklendiği görülmektedir. Bu ince değişiklik, siber uzayın boyut ve katmanlarını daha doğru ifade etmesi bakımından da kanaatimce isabetli niteliktedir.

unsurlarla birlikte bünyesinde barındıran çok boyutlu özel bir uzay mı olduğu sorunsalına farklı bir cevap verildiği görülmektedir.

Bilgi teknolojileri alanındaki yüksek kapasitesiyle ve özgün politikalarını uygulamadaki başarısıyla büyük yükseliş gösteren Çin Halk Cumhuriyeti'nin ve teknoloji çekişmesinde ABD ile uzun yıllar rekabet halinde olan Rusya Federasyonu'nun siber uzay konusundaki tutumları da büyük önem taşımaktadır. Öncelikle belirtilmelidir ki ABD ve İngiltere'nin başını çektiği Avro-Atlantik siber doktrin ile Çin ve Rusya'nın yaklaşımları, tanımlar bağlamında olduğu gibi kavramlar bağlamında da farklılık arz etmektedir. Bu farklılıkların da uluslararası hukukta ortak bir anlayışta buluşulmasını zorlaştırdığı ifade edilmiştir.⁴⁷

Çin ve Rusya'nın, siber uzaya ilişkin devlet politikalarında olduğu gibi, fonetik ve kavramsal olarak “siber” kelimesinin dillerine yerleşmemesi açısından da batılı devletlerden ayrıldıkları görülebilmektedir. Örnek olarak Çin, Birleşmiş Milletler (BM) bünyesindeki çalışmalara katılırken sunduğu güncel belgenin İngilizce versiyonunda *cyberspace* kavramını kullanmıştır.⁴⁸ Fakat Çince versiyonunda esasen “ağ uzayı” anlamına gelen “网络空间 (*Wǎngluò kōngjiān*)” ifadesinin kullanıldığı görülmektedir.⁴⁹ Akademik çalışmalarda da “网络” ifadesi yer yer “siber” şeklinde çevrilse de yerleşik olarak “ağ” anlamında kullanılmaktadır.⁵⁰ Eldeki çalışmada ayrıca incelenecek “siber egemenlik” politikasının da öncüsü olan Çin, bu yaklaşımını resmi olarak “bilgi egemenliği” ya da “internet (ağ) egemenliği” gibi kavramlarla ifade etmiştir.⁵¹

⁴⁷ Keir Giles ve William Hagestad II, “Divided by a Common Language: Cyber Definitions in Chinese, Russian and English”, K. Podins, J. Stinissen ve M. Maybaum (Ed.), **5th International Conference on Cyber Conflict** içinde (413-430), Tallinn: NATO CCDCOE Publications, 2013, s.413.

⁴⁸ UN/Open-ended Working Group on Information and Communication Technologies, China's Positions on International Rules-making in Cyberspace, Working Papers, 01.12.2021; <https://documents.unoda.org/wp-content/uploads/2021/12/Chinese-Position-Paper-on-International-Rules-making-in-Cyberspace-ENG.pdf> (31.12.2024).

⁴⁹ UN/Open-ended Working Group on Information and Communication Technologies, China's Positions on International Rules-making in Cyberspace, Working Papers, 01.12.2021; <https://documents.unoda.org/wp-content/uploads/2021/12/Chinese-Position-Paper-on-International-Rules-making-in-Cyberspace-CHN.pdf> (31.12.2024).

⁵⁰ Jinghan Zeng, Tim Stevens ve Yaru Chen, “China's Solution to Global Cyber Governance: Unpacking the Domestic Discourse of ‘Internet Sovereignty’”, **Politics & Policy**, Vol.45, No.3, (2017), ss.432-433; Xianwei Zhu ve Diğerleri, “Data Recommendation Algorithm of Network Security Event Based on Knowledge Graph”, **Chinese Journal of Network and Information Security**, Vol.9, No.6, (2023), s.116.

⁵¹ Zeng, Stevens ve Chen, s.446.

Rusya’da 2016 yılında kabul edilen “Rusya Federasyonu Bilgi Güvenliği Doktrini” metninde, siber uzay karşılığı olarak “bilgi küresi -alanı- (*informational sphere*)” ifadesi kullanılmıştır.⁵² Ayrıca bu ifade “*bilginin, bilgileştirme nesnelerinin, internet bilgi ve iletişim ağına dâhil bilgi sistemleri ve sitelerin (buradan itibaren “internet” olarak adlandırılacaktır), iletişim ağlarının, bilgi teknolojilerinin, bilgi üretme ve işleme, yukarıdaki teknolojileri ve bilgi güvenliği teminini geliştirme ve kullanma ile ilişkili kişi ve kurumların yanı sıra küredeki halkla ilişkileri düzenleyen bir dizi mekanizmanın birleşimi*” şeklinde tanımlanmıştır. Bu tanımın Rus idare geleneklerine uygun şekilde detaylı ve kapsayıcı yapısı dikkate değerdir. Ayrıca kapsamı daha geniş kabul edilmiş olsa da ABD’nin yaptığı tanım ile büyük ölçüde örtüşen bir sonuca ulaşıldığını söylemek de mümkündür.

Rusya’nın “siber” kavramına mesafeli duruşunun önemli bir sebebinin, ABD menşeli olması itibarıyla sibernetiğe ve kurucusu *Wiener*’e yönelik, Sovyet Sosyalist Cumhuriyetler Birliği’nin (SSCB) ilk döneminde yürütülen ret ve sansür politikası ile Stalin sonrası dönemde geçirilen tartışmalı süreçler olduğu da ileri sürülmüştür.⁵³ Dolayısıyla “siber”, Rusya’nın resmî belgelerinde tercih edilmezken; Rusça konuşan internet kullanıcıları ve yazarlar, oldukça yaygın olarak “кибер (kiber)” kelimesine teveccüh göstermektedir.⁵⁴ Bunun yanında, Rusya’da kullanılan “киберпространство (kiberprostranstvo)” ifadesine ve Çin’in tercih ettiği yukarıda bahsedilen karşılığa binaen; aslında bu devletlerin siber uzayı, kendi kapsayıcı “bilgi uzayı” tanımlarının bir alt kümesi ve mütemmim cüzü olarak gördükleri de belirtilmiştir.⁵⁵

Türkiye Cumhuriyeti Ulaştırma ve Altyapı Bakanlığı, periyodik olarak ulusal siber güvenlik stratejisine dair belgeler yayımlamaktadır. “2016-2019 Ulusal Siber Güvenlik Stratejisi” belgesi dâhilinde siber uzayın “*Tüm dünyaya ve uzaya yayılmış durumda bulunan bilişim sistemlerinden ve bunları birbirine bağlayan ağlardan oluşan*

⁵² Doctrine of Information Security of the Russian Federation, http://www.scrf.gov.ru/security/information/DIB_eng/ (31.12.2024).

⁵³ Süreçle ilgili detaylı bilgi için bkz. Benjamin Peters, **How Not to Network a Nation: The Uneasy History of the Soviet Internet**, Cambridge, MA: MIT Press, 2016, s.29 vd.

⁵⁴ Juha Kukkola, **Digital Soviet Union: The Russian National Segment of the Internet as a Closed National Network Shaped by Strategic Cultural Ideas**, Series 1, Research Publications No.40, Helsinki: National Defence University, 2020, s.59.

⁵⁵ Giles, s.419; Juha Kukkola ve Mari Ristolainen, “Projected Territoriality: A Case Study of the Infrastructure of Russian Digital Borders”, **Journal of Information Warfare**, Vol.17, No.2, (2018), s.83.

veya bağımsız bilgi sistemlerinden oluşan sayısal ortam” olduğu belirtilmiştir.⁵⁶ “Ulusal Siber Güvenlik Stratejisi ve Eylem Planı (2020-2023)” belgesinde ise aynı kavramın “doğrudan ya da dolaylı olarak internete, elektronik haberleşme ve bilgisayar ağlarına bağlı olan tüm sistem ve hizmetler” ifadeleriyle tanımlandığı görülmektedir.⁵⁷ Son yayımlanan “Ulusal Siber Güvenlik Stratejisi ve Eylem Planı (2024-2028)” belgesinin kamuya açık sunulan kısmında ise özel bir tanımlama yapılmamıştır.⁵⁸ “Sayısal ortam” tabirinden “sistem ve hizmetler” kapsamına geçilmesi; siber uzayın sadece sanal boyutuyla kabulünden, daha kapsayıcı ve sistematik bir yaklaşıma doğru olan pozisyon dönüşümünün göstergelerindendir. Yapılan değişiklik, bu yönüyle ABD’nin geçirdiği süreçle benzerlik arz etmektedir.

c. Uluslararası Örgütler ve Sivil Toplum Kuruluşları

Bilişim alanında uluslararası örgütler ve sivil toplum kuruluşları birçok farklı yönden belirleyici etkiye sahiptir. En köklü uluslararası örgütlerden olan ve günümüzde BM uzmanlık kuruluşu olarak faaliyetlerini sürdüren Uluslararası Telekomünikasyon Birliği (*International Telecommunication Union* (ITU)), devletlerin siber güvenlik stratejilerini belirlerken kullanabilmeleri amacıyla 2011’de yayımladığı rehberde siber uzayı “internet, iletişim ve bilgisayar ağlarına doğrudan veya dolaylı olarak bağlı sistemler ve hizmetler” şeklinde tanımlamıştır.⁵⁹ Türkiye’nin tercih ettiği tanım ile bu rehberde geçen tanımın büyük ölçüde örtüştüğü görülmektedir. Rehberin siber güvenliği konu edinmesinden ileri gelen bir sonuç olarak siber uzayın tanımı, siber güvenlik önlemlerinin ana konusunu ifade edecek şekilde kurgulanmıştır. İlgili metinde ayrıca ifade edildiği üzere, devletlerin bu sistem ve hizmetlerin yeterli ve güvenli şekilde çalışmasının devamını sağlamak üzere çaba sarf etmesi, ulusal siber güvenliğin temelini oluşturmaktadır. Sonuç itibarıyla ITU’nun, özel amaca dayalı tanımların isabetli bir örneğini ortaya koyduğu da söylenebilecektir.

BM’nin bir başka uzmanlık kuruluşu olan Birleşmiş Milletler Eğitim, Bilim ve Kültür Örgütü (*United Nations Educational, Scientific and Cultural Organization*

⁵⁶ T.C. Ulaştırma Denizcilik ve Haberleşme Bakanlığı, **2016-2019 Ulusal Siber Güvenlik Stratejisi**, s.7.

⁵⁷ T.C. Ulaştırma ve Altyapı Bakanlığı, **Ulusal Siber Güvenlik Stratejisi ve Eylem Planı (2020-2023)**, s.10.

⁵⁸ Belgenin büyük kısmı “hizmete özel” tasniflidir; T.C. Ulaştırma ve Altyapı Bakanlığı, **Ulusal Siber Güvenlik Stratejisi ve Eylem Planı (2024-2028)**, s.32.

⁵⁹ ITU, **The ITU National Cybersecurity Strategy Guide**, 2011, s.5.

(UNESCO)), “İnternet Yönetişimi Sözlüğü” içerisinde siber uzay için “*Vatandaşların ve kuruluşların, sosyal ve ticari etkileşimleri için bilgi ve iletişim teknolojisini kullanarak eriştikleri, birçok alt-topluluğun başta internet olmak üzere teknik ortam kullanılarak düzensiz dağılmış şekilde bulunduğu, gerçek uzaydan ayrı, dünya çapında sanal bir uzay*” tanımını yapmıştır.⁶⁰ Bu tanımın, siber uzayın mantıksal yapısını esas alan tanımlar kategorisine alınabileceği görülmektedir.

Çok sayıda sektörde tanımları ve standartları belirleyen Dünya Standardizasyon Örgütü (*International Organization for Standardization (ISO)*) ve elektrik elektronik sahasında önemli bir standart otoritesi olan Uluslararası Elektroteknik Komisyonu (*International Electrotechnical Commission (IEC)*) tarafından 2012’de yayımlanan standartta, siber uzay için “*herhangi bir fiziksel formda olmayan, teknolojik cihazlar ve buna bağlı ağlar vasıtasıyla internet üzerindeki insanların, yazılımların ve hizmetlerin etkileşiminden oluşan karmaşık bir ortam*” tanımı yapılmıştır.⁶¹ IEC’nin Uluslararası Elektroteknik Sözlüğü’ne (*International Electrotechnical Vocabulary*) 2019’da eklediği maddede ise “*internet de dahil olmak üzere birbirine bağlı bilgi işlem sistemlerinin ve işledikleri verilerin bütünü*” şeklinde bir tanım tercih edilmiştir.⁶² ISO ve IEC çok sayıda standardı ortak yayımlarıyla belirlemektedir. IEC tarafından yayımlanan sözlük maddeleri, ISO nezdinde de muteber görülmektedir.⁶³ Sonuç olarak, devletlerin tanımlarında görülen dönüşümün, söz konusu kurumlarca belirlenen tanımlarda da geçerli olduğu gözlemlenebilmektedir.

Son yıllarda yayımladığı makale ve stratejik analiz raporlarıyla dikkat çeken bir sivil toplum kuruluşu olarak Siber Barış Enstitüsü (*CyberPeace Institute*), düzenlediği Siber Terimler Sözlüğü’ndeki siber uzay başlığında “*dijital sistemler ve çevrimiçi dünya; bilgisayar ağları ve internet aracılığıyla erişilebilen her şeyi kapsayan siber uzayı oluşturmaktadır. Buna kurumsal ağlar ve sosyal medya platformlarından banka hesaplarına ve bulut hizmetlerine kadar her şey dâhildir. Ayrıca güvenlik kameraları,*

⁶⁰ UNESCO, Cyberspace, Internet Governance Glossary, <https://en.unesco.org/glossaries/igg> (31.12.2024).

⁶¹ ISO/IEC, Information technology — Security techniques — Guidelines for cybersecurity, International Standart, **ISO/IEC 2703:2012(E)**, 4.21, s.4.

⁶² IEC, Cyberspace, Electorpedia, <https://www.electropedia.org/iev/iev.nsf/display?openform&ievref=171-08-03> (31.12.2024).

⁶³ ISO/IEC, Cybersecurity — Guidelines for Internet Security, International Standart, **ISO/IEC 27032:2023(E)**, s.1.

*oyun konsolları, TV setleri veya robot elektrikli süpürgeler gibi tüm bağlı cihazları da içerir” ifadelerini kullanmıştır.*⁶⁴ Bu tanım, siber uzayın hem sanal özelliğine ve mantıksal boyutuna atıfta bulunmakta hem de fiziki unsurları da siber uzaya dahil etmektedir. Böylece devletlerin yukarıda arz edilen pozisyon değişiklikleri sonucunda bulundukları güncel konumlarla uyumlu bir kapsam seçildiği ifade edilebilir.

Uluslararası örgütler ve sivil toplum kuruluşlarının siber uzayı tanımlama biçiminin, ilgili yapının faaliyet sahasına ve amacına göre değiştiği görülmektedir. Yine de zamanla mezkûr tanımların daha kapsamlı ve gerçekçi bir hale geldiği, bu yönüyle de devletlerin tanımlarıyla paralellik taşıdığı söylenebilecektir.

d. Öğreti

Tanımlar ve kurallar söz konusu olduğunda en belirleyici etkiye sahip süjeler devletler ve onların oluşturduğu uluslararası örgütler olsa da hem süreç başlatıcı hem de sonuç verilerini toparlayıcı vasfıyla akademik literatür, en değerli kaynak olma özelliğini korumaktadır. Bilhassa günümüz teknolojisi gibi çok hızlı yön ve biçim değiştiren bir olgu hakkında en isabetli tespitlerin, ağır ve güvenli hareket etme eğilimindeki kurumlardan ziyade bu hıza yetişebilecek yazarlar ve bilim insanları tarafından yapılması daha olasıdır. Değişim ve beraberinde gelen esneklik ile üretkenliğin bir sonucu olarak da bu alandaki tanım, yaklaşım ve yorumların sayısını belirlemek imkânsız hale gelmiştir.

Siber uzayın teorik zemini genel olarak mekansallaştırılması (*spatialization*) ya da modellenmesi (*modelling*) üzerine yazarlarca yapılan tartışmalarla şekillenmiştir. Ortaya çıkan tanımların hemen hepsi de bu konuda alınan pozisyonların sonucudur. Devletler ve ilgili kurumsal yapılar, pratik ihtiyaçlar nedeniyle kendileri için geçerli bir tanım ve politika belirlemek mecburiyetinde kalmışlardır. Meselenin mutfağında ise tartışmalar hâlen sürmektedir. Resmi tanım ve pozisyonların kısa periyotlardaki değişimi de bu hareketliliğin doğal yansımasıdır. Öğreti, tanımlama faaliyetinin ötesinde, siber uzayın özüne ve kimliğine yönelik arayışın esas bağlamıdır.

⁶⁴ CyberPeace Institute, Cyberspace, Glossary of Cyber Terms, <https://cyberpeaceinstitute.org/glossary/> (31.12.2024).

1984'te Neuromancer'ın çıkışıyla “sanal gerçeklik (*virtual reality*)”, siber uzay adıyla kendine yeni bir isim ve kimlik bulmuştur.⁶⁵ “Klasik teori” de bu zemin üzerine inşa edilmiştir. *Benedikt*, 1991'de siber uzayın “fiilen mevcut, deneyimlenebilir” ancak “soyut” nitelikte olduğunu belirtmiş, fiziksel uzayın mekânsal olmayan “zaman” boyutuna da bu yönüyle bir örnek olarak işaret etmiştir.⁶⁶ Aynı dönemde siber uzayın fiziksel uzaydan ve coğrafi sınırlardan bağımsız olarak mevcut, bilgisayar ağlarının gelişimiyle ortaya çıkmış, bilgilerin elektronik olarak saklanması ve iletilmesini sağlayan alternatif bir evren olarak tanımlandığı da görülmektedir.⁶⁷ *Heim*, siber uzayın sonsuz ve soyut bir ikincil alem olduğu düşüncesinden hareketle, sanal gerçeklik sistemlerinin, fiziksel uzayı siber uzaya sunmak için kullanılabileceğini belirterek klasik teoriye katkıda bulunan yazarlardan olmuştur.⁶⁸ Yine dönemin yazarlarından olan *Tribe* ise sanal gerçeklik temalı veya siber uzayı bağımsız bir mekân olarak kabul eden tanımları reddederek, bilgisayar aracılı sesli ve görüntülü etkileşimlerin tamamını ifade edecek şekilde söz konusu kavramı kullanmıştır.⁶⁹ *Rheingold* da sentezleme yaparak, bilgisayarın bir iletişim aracına dönüşmesiyle birlikte ortaya çıkan “bilgisayar aracılı iletişim (*computer mediated communication*)” teknolojilerini kullanan insanlar tarafından bünyesinde toplulukların oluşturulduğu ve gündelik yaşam barındıran kavramsal bir uzay olarak siber uzayı değerlendirmiştir.⁷⁰ Klasik dönemdeki dikkate değer bir girişim de *Gozzi Jr.* tarafından siber fiber (*cyberfiber*) kavramının ortaya atılmasıdır. Yazar, sınırsız ve soyut siber uzay algısına karşı, kullanıcıların sanal boyutu tecrübe ederken fiziksel ağa olan bağımlılığının sürdüğüne dikkat çekerek siber uzayın çok yönlülüğü üzerinde durmuştur.⁷¹ *Dyson*, *Gilder*, *Keyworth* ve *Toffler* da ortak çalışmalarında siber uzayı “kelimenin tam anlamıyla evrensel olan biyoelektronik bir ortam” şeklinde

⁶⁵ Allucqu re Rosanne Stone, “Will the Real Body Please Stand Up?”, Michael Benedikt (Ed.), **Cyberspace: First Steps** içinde (81-118), The MIT Press, 1991, s.98; Howard Rheingold, **Virtual Reality: The Revolutionary Technology of Computer-Generated Artificial Worlds – and How It Promises and Threatens to Transform Business and Society**, New York: Summit Books, 1991, s.16.

⁶⁶ Michael Benedikt, “Cyberspace: Some Proposals”, Michael Benedikt (Ed.), **Cyberspace: First Steps** içinde (119-224), The MIT Press, 1991, s.120.

⁶⁷ Katie Hafner ve John Markoff, **Cyberpunk: Outlaws and Hackers on the Computer Frontier**, New York: Simon & Schuster, 1991, s.111 ve 150.

⁶⁸ Michael Heim, **The Metaphysics of Virtual Reality**, New York: Oxford University Press, 1993, ss.78-79.

⁶⁹ Laurence H. Tribe, “The Constitution in Cyberspace: Law and Liberty Beyond the Electronic Frontier”, Electronic Privacy Information Center, 1991, https://archive.epic.org/free_speech/tribe.html (31.12.2024).

⁷⁰ Howard Rheingold, **The Virtual Community: Homesteading on the Electronic Frontier**, Reading, Massachusetts: Addison-Wesley, 1993, s.6 vd.

⁷¹ Raymond Gozzi, Jr., “The Cyberspace Metaphor”, **ETC: A Review of General Semantics**, Vol.51, No.2, (1994), ss.221-222.

tanımlamışlardır. Yazarlar, “*telefon kablolarının, koaksiyel kabloların, fiber optik hatların veya elektromanyetik dalgaların olduğu her yerde*” bulunan ve elektronik formdaki bilgileri içeren bu ortamın, insanların erişimini mümkün kılan portallar vasıtasıyla fiziksel çevreye bağlandığını ifade etmişlerdir.⁷² Yapılan bu tanımlamalarda da insan ve fiziksel araçların durumlarından bahsedilse dahi nihai olarak sanal bir mekânın varlığına yönelik yaklaşımın kabul edildiği görülmektedir.

Barlow’un 1996’da Siber Uzak Bağımsızlık Bildirgesi’ni yayınlaması, literatürde bir mihenk taşı olmuştur. Özellikle internet teknolojisinin o dönem oluşturduğu atmosfer ile iletişim ve bilişim açısından oldukça özgürlükçü bir rüzgâr yakalanmıştır. *Barlow*, devletlere ve hükümetlere meydan okuyarak; siber uzayın onların egemenliğinden varestes, kontrol edilemez, haricen düzenleme getirilemez ve müdahale edilemez, ayrı bir evren olduğu iddiasını ileri sürmüştür.⁷³ Bu iddia o dönemde gördüğü yoğun ilgiyle siber uzayın teorik tarihinde klasik yaklaşımın zirve noktası olarak da değerlendirilebilir.

Strate, 1984’ten 1999’a kadarki süreçte literatürde karşılaşılan başlıca siber uzay tanımlarını bir araya getirerek kategorize etmiş ve bir taksonomi kurgulamıştır. Bu çalışmada, siber uzayın ontolojik zemininin klasik olarak soyut ve fizikötesi yönüyle inşa edildiği; bu zemin üzerinde fiziksel, algısal ve kavramsal yönlerin çeşitli yazarlarca vurgulandığı; nihayet sentez ile üçüncü basamağa geçildiği ifade edilmiştir.⁷⁴ Söz konusu eser, klasik teori adına önemli bir derleme ve tasnif çalışmasıdır. 2009’da yapılan bir başka çalışmada ise 28 farklı siber uzay tanımı ele alınmıştır.⁷⁵ Bu iki derleme incelendiğinde; 21. yy başında devletlerin siber güvenlik kaygılarının da artmasıyla beraber, siber uzayın fiziksel yönünün gittikçe daha çok ön plana çıkmaya başladığı gözlemlenebilmektedir. Son yıllarda ise bilgisayar teknolojilerinin ve ağların insan yaşamındaki etkinliğinin ivmelenerek artması (siberleşme (*cyberization*)), “genel siber uzay (*general cyberspace*)” teorisini de üreten önemli bir başka derleme çalışmasına kapı

⁷² Esther Dyson ve Diğerleri, “Cyberspace and the American Dream: A Magna Carta for the Knowledge Age (Release 1.2, August 22, 1994)”, **The Information Society**, Vol.12, Iss.3, (1996), s.296.

⁷³ John Perry Barlow, “A Declaration of the Independence of Cyberspace”, Electronic Frontier Foundation, <https://www.eff.org/tr/cyberspace-independence> (31.12.2024).

⁷⁴ Lance Strate, “The Varieties of Cyberspace: Problems in Definition and Delimitation”, **Western Journal of Communication**, Vol.63, No.3, (1999), ss.384-385.

⁷⁵ Daniel T. Kuehl, “From Cyberspace to Cyberpower: Defining the Problem”, Franklin D. Kramer, Stuart H. Starr ve Larry K. Wentz (Ed.), **Cyberpower and National Security** içinde (24-42), Washington: National Defense University Press, Potomac Books, 2009, s.26 vd.

açmıştır. Bu çalışmada siber uzayın sözlükler, devletler ve yazarlar nezdindeki tanımları arasındaki tutarsızlığa da değinilerek; yıllar içerisinde ortaya çıkan farklı amaç ve vurgulara göre tanımların şekillendiği ifade edilmiştir.⁷⁶ Ayrıca siber uzayın geleneksel tanımının “küresel olarak birbirine bağlı bilgisayar ağlarına ve ilgili tüm unsur ve altyapılara dayanan dijital, sanal, soyut ve zamandan bağımsız metaforik alanı” ifade ettiği; günümüzde geline nokta ise insanlığın fiziksel, sosyal ve düşünsel uzayları içerisinde siber-etkin (*cyber-enabled*) alanların oluştuğu ve bunların bütününe “genel siber uzay” olarak adlandırılabilceği düşüncesi aktarılmıştır.⁷⁷ Siber-etkin alanlar konsepti, siber uzayın çok boyutlu yapısının izahı adına değerli bir yaklaşım olmuştur. Bir uzay içerisindeki siber-etkin alandan bahsedilmesinin temelinde de yukarıda ilgili bölümde ele alınan sibernetik ve siber kavramları yatmaktadır. Modern siber uzay teorisinin kabul gören yazarlarından *Clark* da siber uzayın gerçek unsurlardan oluşan gerçek bir insan yapısı olduğunu, temelsiz ve fantastik bir kavram olmadığını ifade ederek siber uzay teorisinin modern dönemde geldiği nokta ile klasik yaklaşım arasındaki farkı ortaya koymuştur.⁷⁸

Rus doktrini, “bilgi” kavramından hareketle değerlendirdiği siber uzayı, Rusya’nın devlet politikasıyla uyumlu biçimde tanımlayagelmıştır. *Anokhin* ve *Baranov*, internete bağlı olmayan bir bilgisayarın da bilgiyi işleyebileceğinden ve kullanıcıya sanal bir alan oluşturabileceğinden bahisle, kullanıcının zihnini etkileyebileceğini; bir yazılım kullanıcısının, yazılımı yapan kişiyle dolaylı yoldan ilişki kurmuş olacağını ve üreticinin programladığı imge ve sembollerin tesiri altında kalacağını vurgulamıştır.⁷⁹ Böylece siber uzay, ağlardan ve sınır aşan iletişimden bağımsız olarak fertlerin zihin dünyasına etki edebilen tikel fiziksel ve mantıksal bilgi unsurlarının bütününe kapsayacaktır. Rusya’nın toplumun düşünce yapısına ve bilgi dünyasına özel ihtimam

⁷⁶ Huansheng Ning ve Diğerleri, “General Cyberspace: Cyberspace and Cyber-Enabled Spaces”, **IEEE Internet of Things Journal**, Vol.5, No.3, (2018), s.1844.

⁷⁷ Ibid. s.1845 vd.

⁷⁸ David D. Clark, “Characterizing Cyberspace: Past, Present and Future”, **ECIR Working Paper No.2010-3**, MIT Political Science Department, 2010, s.2.

⁷⁹ Yu. V. Anokhin ve M. P. Baranov, “Doctrinal Characteristic of the Ideological Function of the State in Virtual Space”, **Zhurnal Rossiyskogo Prava**, No.8, ss.14–24’ten aktaran Luidmila Terentieva, “The Issue of State Sovereignty in Cyberspace”, **Legal Issues in the Digital Age**, Vol.2, No.2, (2021), ss.62-63.

gösterdiği dikkate alındığında; batılı anlamda siber uzayın, Rus bilgi güvenliği politikasının teknolojik parçasından ibaret olduğu, bu yaklaşımdan da anlaşılabilecektir.

Siber uzay teorisinde alternatif ve karşıt görüşlere örnek olarak *Shapiro* gösterilebilir. Yazar öncelikle *Gibson*'ın sanal gerçeklik temalı konseptinin, 1990'da Elektronik Cephe Vakfı'nı (*Electronic Frontier Foundation* (EFF)) kuran *Kapor* ve *Barlow* tarafından yeniden ele alınarak "tüm çevrimiçi etkileşimlerin gerçekleştiği yeri" ifade edecek şekilde genişletildiğine dikkat çekmiştir.⁸⁰ *Shapiro*'ya göre siber uzaydan kasıt, en kadim örneklerden alfabe gibi yahut modern dönem için telefon ve televizyon gibi sadece bir iletişim aracıdır. Hissettirdikleri itibarıyla ayrı bir mekân gibi ele alınması genel kabul görmüş olsa da aslında tamamen kurgusal olan böyle bir uzayın gerçekliğinden bahsetmek mümkün değildir. Önemli olan, bu iletişim aracını oluşturan "kod" ve onunla ilgili hususlardır.⁸¹ Bir başka karşıt görüş yazarı *Dewar* ise *Neuromancer*'daki "*mutabakata dayalı halüsinasyon*" ifadesine ironiyle atıfta bulunup, siber uzayın kural dışı ve soyut bir sanal alem gibi kabul edilmesinin uyanılması gereken bir yanılgı olduğunu ileri sürerek; bu bağlamda karşılaşılan sorunların dijital olmasının "yeni" olduğu anlamına gelmediğini, sadece kullanılan araçların değiştiğini iddia etmiştir. *Dewar*'a göre siber uzay, gerçekte yoktur.⁸²

Siber uzayın tanımlanmasında öğretinin gelişim süreci -doğal olarak devletlerin resmi tanımlarında da görüldüğü üzere- gittikçe daha kapsayıcı olma ve somut öğeleri de siber uzay kapsamına dahil etme yönünde ilerlemiştir. Fakat hâlen uluslararası boyutta resmi kabul görmüş genel bir tanımdan söz edilemediğinden; kavram üzerinde hüküm inşa edileceği zaman, amaca yönelik bir seçimde bulunulması ve titiz bir çerçeve çizilmesi gerekliliği sürmektedir.

B. Bir Uzay Olarak Siber Uzay

Literatürdeki tanımlar arasında bir asgari müşteregin varlığından bahsedilebilse de siber uzayın aslında "ne" olduğuyla ilgili kesin mutabakata varılamamıştır. İnternet ile

⁸⁰ Andrew L. Shapiro, "The Disappearance of Cyberspace and the Rise of Code", *Seton Hall Constitutional Law Journal*, Vol.8, No.3, (1998), s.704.

⁸¹ Ibid., s.707 vd.

⁸² Robert Dewar, "Cyberspace is a Consensual Hallucination", *Policy Perspectives*, Vol.6, No.2, (2018), ss.2-4.

Web arasındaki farkta ve aralarındaki bağımlılık ilişkisinde de görülebilecek fiziksel unsurlar ile mantıksal unsurların birlikteliği, günümüzde “siber” başlığı altındaki hemen her alanda kendini gösteren özgün bir konsepttir. İnsanlık, teknolojiyle elde ettiği sanallığı, dünyadaki geçmişine kıyasla henüz çok kısa süredir tecrübe etmektedir. Yüzlerce yıldır halüsinatif maddelerle ve çeşitli zihinsel metotlarla sağlanan sanal gerçeklik algısı, *Gibson* tarafından da öngörüldüğü üzere artık iradi ve mutabakata dayalı, sistemli, kontrollü, istikrarlı ve erişilebilir bir yapıya dönüşmüştür. Böylece siber uzayın tanımlanması sürecinde bir kısım yazar bu sanallıktan hareket ederek, fiziksel altyapı üzerinde tecrübe edilebilen “sanal” boyuta “uzay” yakıştırması yapan klasik teoriyi oluşturmuşlardır.⁸³ Devamında ise gerek fiziksel altyapıyı gerek iki yapı arasında dolaşan veriyi gerekse bunları tecrübe eden insanı siber uzayın unsurları arasında kabul eden daha kapsayıcı yaklaşımlar görülecektir. Dolayısıyla siber uzayın, arayüzler vasıtasıyla erişilen bir sanallıktan mı ibaret olduğu yoksa bu sanallığın yanında insan dâhil fiziki unsurları da barındıran bir yapıdan mı bahsedildiği sorusu, yaklaşım farklılıklarının temelini teşkil etmektedir. Mahiyete yönelik bu ayrımın yanı sıra siber uzayın ayrı bir “yer” olarak mekânsallığına ve hukuki düzenlemelere konu olabilirliliğine dair tartışmalar da mevcuttur.⁸⁴ Fakat bu tartışmaları da siber uzayın mahiyetinden tamamen bağımsız düşünmek mümkün değildir.

Günlük dile astronomi bağlamındaki anlamıyla yerleşen “uzay”, esasen hem somut hem soyut karşılığı olan bir kavramdır. Dış uzay (*outer space*) ve insanın kendisi dahil olmak üzere bütün çevre, fiziki anlamdaki uzayı (uzay-zaman) oluşturmaktadır. Diğer taraftan uzay, matematik ve mantık bilimlerinin de konusudur. Bir problemi analiz etmek, bir teoriyi geliştirmek veya karmaşık kavramları açıklamak gibi amaçlar güden düşünce deneyleri ve modellemeler, soyut uzaylarda inşa edilmektedir.⁸⁵ Bu bakımdan “mantıksal uzay”⁸⁶ ve matematikte “kartezyen koordinat sistemi” gibi olgular, uzay

⁸³ Aaron Schwabach, **Internet and the Law: Technology, Society, and Compromises**, Santa Barbara, California: ABC-CLIO, 2006, s.66.

⁸⁴ Duygu Hatipoğlu Aydın, **Siber Alan ve Hukuk**, İstanbul: On İki Levha Yayıncılık, 2022, s.39 vd.

⁸⁵ Düşünce deneylerinin fiziksel uzay ile irtibatının, matematik örneği üzerinden anlatımı için bkz. Hans Christian Ørsted, “First Introduction to General Physics”, (1811), Karen Jelved, Andrew D. Jackson ve Ole Knudsen (Çev., Ed.), **Selected Scientific Works of Hans Christian Ørsted** içinde (282-309), Princeton: Princeton University Press, 1998, ss.296-297.

⁸⁶ *Wittgenstein*, transandantal gerçekliği olan kavramları hariç tuttuğu bir olgular bütünü olarak mantıksal uzayı ele almış ve gerçekliğin ancak mantıksal uzay içerisinde algılanıp kurulabileceğini, mantıksal önermelerin fonksiyonunun da bu uzay içindeki olguları ifade etmekle sınırlı olduğunu ileri sürmüştür; Neşe Aksoy, “Kant’tan Wittgenstein’a: Mantığın Sınırları”, **Felsefe Arkivi**, Sayı.51, (2019), s.24.

kavramının soyut karşılığını yansıtan örneklerdir. Uzak ayrıca sosyal bilimlerin çeşitli alanlarında da farklı yaklaşımlarla ele alınmıştır.⁸⁷

Uzak kelimesinin siber uzak içerisinde kullanımının, kavramın türetildiği dönem ve bağlam itibarıyla astronomik anlamdaki uzayın fiziksel varlığıyla bir analogi kurmak amacına dayandığı söylenebilecektir. Nitekim siber uzayın tıpkı fiziksel uzak gibi keşfedilmeye açık, akıl almaz büyüklükte bir kapsama ve kendine has yapılara sahip olduğu kabulü söz konusudur. Ayrıca bu ifade, siber uzayın sadece rastgele bir bilgi koleksiyonu değil, aynı zamanda fiziksel uzak gibi tutarlı, birbirine bağlı unsurlar barındıran ve kendi kanunlarına tabi olan bir sistem olduğu fikrini yansıtmaktadır. Böylece fiziksel uzaya paralel bir sanal aleme dair merak, keşif ve sınırsızlık duygusu uyandırmak amaçlanmıştır.

Yerli literatürde “*cyberspace*” kavramının Türkçe karşılığı için “siber uzak”, “siber alan” ve nadiren “siber mekân” çevirileri tercih edilmektedir.⁸⁸ Çevirilerin çeşitliliğinin, “*space*” kelimesinin Türkçe’de nasıl karşılanacağına dair çok erken zamanlardan bu yana süregelen bir karmaşadan kaynaklandığı görülmektedir.⁸⁹ Batı dillerinde “*cyberspace*” ifadesi ortak olarak kullanılırken,⁹⁰ kelimeyi bünyesinde bu

⁸⁷ Henri Lefebvre’in “La Production de l’espace” eserinde, uzayı boş bir barındırıcı ya da bir koordinat sistemi gibi gören soyut kartezyen yaklaşıma karşı, “aktif olarak üretilen tarihsel bir ürün ve bir toplumsal morfoloji” olarak ele alması, uzayın (bu bağlamdaki çevirilerde Türkçe karşılık olarak “mekân” tercih edilmekle birlikte) sosyal bilimlerdeki yansımalarına bir örnek olarak verilebilir; Henri Lefebvre, *Mekânın Üretimi*, Işık Ergüden (Çev.), 2. Baskı, İstanbul: Sel Yayıncılık, 2014, s.118.

⁸⁸ Alan çevirisini tercih eden yazarlardan Hatipoğlu Aydın, siber parantezinde “uzay” ve “dünya” gibi çevirilerin astronomik terimler olması sebebiyle, “alan” kavramının astronomik uzamdan farklı bir alanı ifade ettiğini belirterek tercihinin gerekçelendirmiştir; Hatipoğlu Aydın, s.3. *Küzeci* de incelenen kavramın mekânsallığa konu olabilmesi üzerinde yoğun şekilde durarak “alan” çevirisini tercih eden yazarlardandır; Elif Küzeci, *Sayısal Fil*, İstanbul: İnkılap Kitabevi, 2021, s.362 vd. Mekân çevirisine ise genellikle mimarlık merkezli çalışmalarda rastlanmaktadır; Evren Ülkeryıldız ve Nilay Özcan Uslu, “Hakikat Sonrası Bilincin Siber-Mekân Üzerinden Üretimi: Ağdaşın Kamusal Mekânı”, *Eskişehir Osmangazi Üniversitesi Sosyal Bilimler Dergisi*, Cilt.22, Sayı.1, (2021), s.293; Bülent Kaptanoğlu, “Bilgisayar Teknolojilerinin Gelişmesi ile Ortaya Çıkan Siber Mekan Kavramı ve Mimarlığa Olan Etkileri”, (*Yayınlanmamış Yüksek Lisans Tezi*, Yıldız Teknik Üniversitesi, Fen Bilimleri Enstitüsü, 2000).

⁸⁹ Şemseddin Sami, 19. Yüzyıl sonunda neşrettiği Kamûs-i Fransevî’de kelimeyi şöyle tanımlamaktadır: “*Mesafe, buud / Zaman aralığı, müddet / Saha, fezâ. // Buud-ı mücerret, fezâ // Cevv-i nâmütenâhi, fezâ-yı nâmütenâhi.*”; Şerif Eskin (Hzl.), *Resimli Kâmûs-ı Fransevî*, Cilt II, “Espace”, Ankara: Türkiye Bilimler Akademisi, 2018, s.728. 20. Yüzyıl başlarında ise *Mustafa Namık Çankı*, Büyük Felsefe Lugatı’nda şu karşılıkları saymış ve örneklerle incelemiştir: “*Mekân, Fezâ, Bu’dı Mücerred, Buud, Hayyiz, Tehayyüz, Mesafe*”. Ayrıca Dil İnkılabı (1932) sonrasında sunulan teklifleri ve karşılıkları; “*Alıs, Alışlık, Allek/Allık, Orun, Uzak*” şeklinde saymıştır; Recep Alpyağıl (Hzl.), *Büyük Felsefe Lugatı*, Cilt I, “Espace”, İstanbul: İz Yayıncılık, 2021, ss.1383-1387. Günümüzde geline nokta ise uzak, uzam, mekân, hayyiz (yer kaplama / fr. *Etendue* / ing. *Extent-Extension*) gibi kavramlar arasında girift bir ilişki söz konusudur. Yazarların kendi nüans tercihlerine göre ilerleyen literatürdeki karışıklığın detaylı incelemesi için bkz. Savaş Kılıç, “Uzam mı, Uzak mı? Peki Mekân ne?”, *Cogito*, Sayı.59, (2009), s.48 vd.

⁹⁰ Almanca’da uzak anlamındaki “*raum*” ile oluşan *cyberraum* kelimesi de ayrıca kullanılmaktadır; Norbert Pohlmann, “cyber-raum”, Institut für Internet-Sicherheit, <https://norbert-pohlmann.com/glossar-cyber-sicherheit/cyber-raum/> (31.12.2024).

haliyle bulundurmayan, Türkçe'nin de yoğun etkileşim içinde olduğu doğu dillerindeki çevirileri incelemek, kelimenin çok sayıdaki karşılığından hangisinin daha tercihe şayan olduğunu tespit etmeye yardımcı olabilecek bir yöntemdir. *Cyberspace* için Arapça karşılık olarak الفضاء السيبراني (*al-fada' al-siybiraniu*) ifadesinin kullanıldığı görülmektedir.⁹¹ Buradaki ifade aynı zamanda dilimize “fezâ” olarak geçmiştir ve yine uzay anlamına gelmektedir. Benzer şekilde Farsça'da da فضای مجازی (*fezâ-i mecâzi* (sanal uzay)) karşılığı kullanılmaktadır.⁹² Siber alan şeklindeki çevirinin de mekânsallığa (mekâniyet – *spatiality*) atıfta bulunan yönüyle muteber bir seçim olduğu kabul edilebilir olmakla birlikte, alan kelimesinin hem kültürel hem geometrik karşılıkları itibariyle iki boyutlu ve düzlemsel bir boşluğu ifade ettiği göz ardı edilmemelidir.⁹³ Sonuç itibariyle “uzay” kavramının yukarıda serdedilen çeşitli disiplinlerdeki özellikleri, çok boyutlu teorik yapılandırmaya müsait olması, kaynak dildeki tarihçesi ve diğer dillerde kullanılan karşılıkların bu kasıtlı uyumluluğu gibi sebeplerle eldeki çalışmada, yerli literatürde de en sık kullanılan karşılık olan “siber uzay” çevirisi tercih edilmiştir.

Siber uzay; belli boyutlara ve unsurlara sahip, kendi işleyişi içerisinde nedensellik ve tutarlılığı olan, içerisinde hem somut hem mantıksal unsurlar barındıran teorik bir uzaydır. Fakat bu tanımlama, yaygın kabul gördüğü üzere ve sadece, insanın teknolojik vasıtalar ile içine girip zihniyle algılayarak tecrübe ettiği bir sanal ortam şeklinde anlaşılmamalıdır.⁹⁴ Siber uzayın teorisi kurulurken boyutları, bu boyutlarda barınan bütün unsurların koordinatları, birbirleriyle ilişkileri ve bu ilişkilerin tabi olduğu doğa kanunları ile beşerî normlar sistematik şekilde ortaya konmalıdır. Söz konusu teorik uzayın ancak analitik izahı yapıldıktan sonra hukuka ve egemenliğe konu olabilirdiği tartışılabilecektir.

⁹¹ UNESCO, Cyberspace, Internet Governance Glossary, <https://en.unesco.org/glossaries/igg> (31.12.2024).

⁹² Glosbe, Cyberspace, <https://en.glosbe.com/en/fa/cyberspace> (31.12.2024).

⁹³ Divan-i Lugati't-Türk'te (1072-1074) dahi bulunan kadim bir sözcük olarak “alan” bu sözlükte: “Yazı, düz ova” şeklinde tanımlanmıştır. Dağlar arasındaki düzlüklerden mühlhem olduğu anlaşılmaktadır ve “açık kapı” anlamına gelen “anğıl” kelimesindeki harflerin yerlerinin değiştirilmesiyle ortaya çıktığı aktarılmıştır; Besim Atalay, **Divanü Lügat-it-Türk Tercümesi**, Ankara: Türk Tarih Kurumu Yayınları, 1985, s.135. Günümüzde de meydan, saha yahut iki boyut üzerinden yüz ölçümü gibi anlamlarda kullanılmakla birlikte “bir çalışma çevresi” (bilim dalı vs.) yahut “içinde birtakım kuvvet çizgilerinin yayılmış bulunduğu varsayılan uzay parçası” gibi karşılıkları da sağlamaktadır; **Güncel Türkçe Sözlük**, “alan”, Türk Dil Kurumu, <https://sozluk.gov.tr> (31.12.2024).

⁹⁴ Günlük dilde kullanılan “sanal alem” ifadesi bu ortamı tanımlamak için daha uygun bir seçenek olarak düşünülebilir.

C. Siber Uzayın Boyutları ve Unsurları

1. Analiz Yöntemleri

Mantık, matematik, fizik, coğrafya, felsefe, sosyoloji gibi çok sayıda farklı disipline dayalı yönleri olan bir teorik uzayın yapısının ve işleyiş kurallarının tespiti için sistemleştirme faaliyetine ihtiyaç duyulur. Siber uzayın da boyutları ve bünyesindeki unsurları arasındaki ilişkiler; uzayın katmanlara ayrılması, mekansallaştırılması, görselleştirilmesi, haritalandırılması, ağ analizi veya kümeleme analizi yapılması yahut matematiksel modellerle ifade edilmesi gibi metotlarla açıklanmaya çalışılmıştır.

Öğretide en sık karşılaşılan ve kabul gören yöntem, siber uzayı “katmanlar (*layer*)” ile analiz etmektir. Bu yaklaşımın arka planında, tasarım çalışmaları 1970’lerde başlayan⁹⁵ ve sonrasında ISO tarafından standart olarak kabul edilen OSI (*Open Systems Interconnection*) referans modeli⁹⁶ bulunmaktadır. OSI modeli, bilgisayar ağları üzerinden gerçekleşen iletişim sürecindeki unsurları tasnif etmek ve bir standart belirlemek amacıyla tasarlanmıştır. Bu modele göre bir açık ağ yapısı yedi katmandan oluşmaktadır. Katmanlar, fiziksel olarak birbirine bağlı iki cihazın varlığından başlayarak, veri iletimindeki protokollere ve transfer sürecinde verinin işlenmesi ile alıcı tarafından veriye erişilmesine kadar geçirilen süreçteki özellik ve rollerine göre aşağıdaki şekilde sıralanmıştır:⁹⁷

- Uygulama (*Application*) Katmanı
- Sunum (*Presentation*) Katmanı
- Oturum (*Session*) Katmanı
- Taşıma (*Transport*) Katmanı
- Ağ (*Network*) Katmanı
- Veri Bağlantısı (*Data Link*) Katmanı
- Fiziksel (*Physical*) Katman

Şekil.1: OSI referans modeli katmanları

Siber uzayı katmanlara ayıran yazarlar, kısmen OSI modeline benzer tasnifler yapmışlardır. Kurum ve yazarların konu üzerine eğilmesi, genel itibarıyla siber güvenlik

⁹⁵ John D. Day ve Hubert Zimmermann, “The OSI Reference Model”, **Proceedings of the IEEE**, Vol.71, No.12, (1983), s.1334.

⁹⁶ ISO/IEC, Information Technology – Open Systems Interconnection – Basic Reference Model: The Basic Model, **ISO/IEC 7498-1:1993(E)**.

⁹⁷ Ibid., s.28.

amaçlı olmuştur. Nitekim güvenliği sağlanmak istenen bir yapının mimarisinin ve unsurlarının doğru tespit ve analizi kesin bir gerekliliktir.

Bir devlet organı örneği olarak ABD Genel Kurmay Başkanlığı, siber uzay için üç katmanlı bir model öngörmüştür. Bu modele göre “fiziksel ağ katmanı”, “mantıksal ağ katmanı” ve “siber-kişilik (*cyber-persona*) katmanı” siber uzayı oluşturan üç katman olarak kabul edilmiştir.⁹⁸ Fiziksel ağ katmanı, benzer tasniflerde de görüleceği şekilde ortak bir tanım olarak; siber uzayda verilerin depolanmasını, taşınmasını ve işlenmesini sağlayan bilgi teknolojileri cihazlarından ve fiziksel altyapıdan oluşur (bilgi işlem cihazları, depolama cihazları, ağ cihazları ve kablolu ya da kablosuz bağlantılar gibi).⁹⁹ Mantıksal ağ katmanı, yine fiziksel katmana benzer şekilde yaygın kabul gördüğü üzere; veri aktarımını sağlayan protokoller, yazılım ve programlar, bağlantılar (*link*), erişim arayüzleri, web siteleri gibi fiziksel ortamdan soyutlanmış mantıksal yapılardan oluşur.¹⁰⁰ Modelde en özgün nitelendirilmiş katman ise siber-kişilik katmanıdır. Bu katmanın, insan veya bot¹⁰¹ fark etmeksizin ağ veya bilgi teknolojisi kullanıcı hesaplarından ve bunların birbirleriyle olan ilişkilerinden oluştuğu belirtilmiştir.¹⁰² Sonuç olarak siber uzayın, fiziksel ağ katmanı üzerinde işleyen mantıksal ağda insan kaynaklı faaliyet gösterilmesinden oluştuğu çıkarımı yapılabilecektir.

Üç katmanlı model öngören yazarlardan *Libicki*, ABD Hava Kuvvetleri için hazırlanan raporda bunları “fiziksel katman”, “sözdizimsel (*syntactic*) katman” ve “anlamsal (*semantic*) katman” şeklinde belirlemiştir. Bu modele göre siber uzay fiziksel katman üzerine kuruludur. Bilindik şekilde fiziksel altyapıyı ifade eden fiziksel katman üzerinde, tasarımcıların ve kullanıcıların makineye ve makinelerin birbirleriyle etkileşim kurdukları protokollere verdikleri talimatları (*instruction*) içeren sözdizimsel katman ve onun üzerinde de makinenin barındırdığı bilgiyi (*information*) içeren anlamsal katman oturmaktadır.¹⁰³ *Libicki*, bilgi ve talimat arasında her zaman kesin bir ayrım

⁹⁸ JP 3-12, I-3.

⁹⁹ Ibid.

¹⁰⁰ Ibid., I-4.

¹⁰¹ Fiziki uzayda faaliyet gösteren otomatik makineleri ifade eden “robot” kelimesinden türemiş, siber uzayda otomatik ve otonom şekilde çalışan yazılım; Ken Dunham ve Jim Melnick, **Malicious Bots: An Inside Look into the Cyber-Criminal Underground of the Internet**, Auerbach Publications, 2009, ss.1-2.

¹⁰² JP 3-12, I-4.

¹⁰³ Martin C. Libicki, **Cyberdeterrence and Cyberwarfare**, RAND Corporation, 2009, s.12.

yapılamayacağını, bazı talimatların bilgi formunda da bulunabileceğini ayrıca ifade etmiştir.¹⁰⁴ *Tabansky* de *Libicki*'ye atıfla üç katmana işaret etmiş fakat isimlendirmeyi “fiziksel”, “yazılım mantığı” ve “veri” şeklinde yapmıştır.¹⁰⁵ Böylece *Libicki*'nin sözdizimsel / anlamsal ayrımı, daha sade bir ifadeyle yazılım / veri denklemiyle ifade edilmiştir. Tallin El Kitabı'nda¹⁰⁶ da “fiziksel”, “mantıksal” ve “sosyal” isimlendirmesiyle üç katmanlı model kabul edilmiştir. Modelin ayırt edici özelliği olan sosyal katman, “siber faaliyetlerde bulunan bireyleri ve grupları” ifade etmektedir.¹⁰⁷

Siber uzayın katmanlarla açıklanması yöntemini izleyen yazarlardan *Clark*, dört katmanlı modeliyle siber uzayı; temelde “fiziksel katman” ve onun üzerinde kurulu “mantıksal katman” ile oluşan bir yapı, bu yapının içerisinde depolanan, aktarılan ve dönüştürülen verilerden müteşekkil “bilgi katmanı” ve nihayet siber-deneyime katılarak siber uzayın parçası haline gelen “insan katmanı” şeklinde unsurlarına ayırmıştır.¹⁰⁸ Bu modele öğretide sıkça başvurulduğu da görülmektedir.¹⁰⁹

Siber uzayın sunumunda “haritalandırılma (*mapping*)” da tercih edilen yöntemlerdendir. *Waldo Tobler*'in “*her şey diğer her şeyle ilişkilidir, ama yakın şeyler uzak şeylerden daha fazla ilişkilidir*” şeklinde ifade ettiği meşhur “coğrafyanın ilk yasası”,¹¹⁰ siber uzay unsurları söz konusu olduğunda yeniden yorumlanmaya ihtiyaç duyacaktır. Siber uzayda mekân algısının sanallaşması ve fiziksel unsurlarla mantıksal unsurların bir arada var olması ile mesafe, zaman ve maliyet arasındaki ilişki fiziksel uzaydakine göre farklılaşmıştır. Dolayısıyla siber uzayın haritalandırılması da kendi dinamikleri içinde gerçekleşmektedir. Bilişim teknolojilerinin, başta internet olmak üzere ağların ve bu ağlar üzerinden erişilen ortamın sosyal hayatla ilişkisini okumak adına, yukarıda sunulan katmanların her birinin ayrı ayrı ele alındığı yahut aralarındaki etkileşimin incelendiği görselleştirme girişimleri gerçekleşmektedir. 2011 sonu itibariyle

¹⁰⁴ Ibid., ss.12-13.

¹⁰⁵ Lior Tabansky, “Basic Concepts in Cyber Warfare”, *Military and Strategic Affairs*, Vol.3, No.1, (2011), s.77.

¹⁰⁶ Bkz. aşağıda “Tallin El Kitabı”; Michael N. Schmitt (ed.), **Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations**, 2nd Edition, Cambridge: Cambridge University Press, 2017.

¹⁰⁷ Tallin El Kitabı, s.12.

¹⁰⁸ Clark, ss.1-4.

¹⁰⁹ Doğrudan veya dolaylı olarak Clark'ın modeline başvuruda bulunan bazı yazarlar için bkz. Clemente, s.163; Hatipoğlu Aydın, s.27; Güzin Ulutaş, “Siber Güvenlik”, Şeref Sağıroğlu ve Mustafa Alkan (Ed.), **Siber Güvenlik ve Savunma – Farkındalık ve Caydırıcılık** içinde (87-101), Ankara: Grafiker Yayınları, 2018, s.87.

¹¹⁰ Daniel Z. Sui, “Tobler's First Law of Geography: A Big Idea for a Small World?”, *Annals of the Association of American Geographers*, Vol.94, No.2, (2004), s.269.

internet üzerinden erişilen web sitelerinin trafik yoğunluklarına ve kullanıcıların bu siteler aralarındaki geçişlerine göre tasarlanmış iki boyutlu bir harita bu çalışmalara örnektir.¹¹¹ Siber uzaydaki -somut ya da soyut- varlıkların (*entity*) katmanlar içerisinde birbiriyle ilişkilerini inceleyen ve matematiksel bir yaklaşımla haritalandıran çalışmalar olduğu gibi,¹¹² siber uzayı mekansallaştırarak mecazi ifadeyle coğrafi yapısını çıkarmaya ve barındırdığı unsurların bu coğrafyadaki konumlarını ve aralarındaki etkileşimleri görselleştirmeye yönelik daha geniş çaplı ve kartografya esaslarına dayalı haritalandırma çalışmaları da yapılmıştır.¹¹³

2. Egemenlik Amaçlı Siber Uzay Modellemesi

Başta üçlü olanlar olmak üzere katmanlı modellerin, temelde siber güvenlik odaklı üretildiğinden bahsedilmiştir. Bu modeller, siber uzaya yönelebilecek saldırı çeşitlerini, her bir katmanın kendine has yapısı ve zafiyetlerini göz önüne alarak tespit ve tasnif etmeyi; saldırıların bertaraf edilmesine ve gerekli önlemlerin tespitine yönelik siber güvenlik çalışmalarına da zemin oluşturmayı amaçlamaktadır. Önemli devlet kurumları ve yazarlarca tercih edilen modellemeler, yıllar içerisinde siber uzayın doğru şekilde sunumu açısından en olgun metot haline gelmiştir. Siber uzaya devlet egemenliği perspektifinden bakıldığında ise devletin egemenlik konusu haline getirebileceği somut veya soyut unsurların niteliklerinin ve birbirleriyle ilişkilerinin tespitine yönelik ihtiyaç daha çok ön plana çıkmaktadır. Dolayısıyla siber uzayın sanal bir dünya olarak kabulünün, egemenlik sorgulamasında belirsizliklere kapı açacağı aşikardır. Bu noktada, çok boyutlu bir teorik uzay olarak tanımlanan siber uzayın doğru şekilde analiz edilmesi, siber uzay dahilindeki bir unsurdan bahsedildiğinde koordinatlarının isabetle verilebilmesi, somut yahut soyut herhangi bir olgunun siber uzaya dahil olup olmadığının tespiti gibi temel gereklilikler önem arz edecektir.

Siber uzay, tabiatıta var olan bir fenomen değildir ve insan tarafından üretilmiştir. Bu üretim başta doğrudan değil; bilişim teknolojilerinin gelişiminin dolaylı bir

¹¹¹ The Internet Map, <http://internet-map.net>, (31.12.2024).

¹¹² Youjun Wang ve Diğerleri, “An Event-Based Method of Construction of Cyberspace Models”, Zuoyi Liang, Xiaoliang Li (Ed.), **4th International Conference on Mechatronics, Materials, Chemistry and Computer Engineering 2015** içinde (1674-1678), Atlantis Press, 2015, ss.1676-1678.

¹¹³ Martin Dodge ve Rob Kitchin, **Mapping Cyberspace**, New York: Routledge, 2001, s.69 vd.

sonucudur. Teorik bir uzay olarak siber uzayın kabulü ise zihinsel bir üretimin doğrudan sonucudur. İki sonuçta da siber uzayın varlığından bahsedilebilmesi için, insanın kendisi dışındaki fiziksel varlıkların zorunluluğu söz konusudur. Bu durum genel olarak siber uzayın fiziksel altyapıya mecburi bağımlılığı şeklinde kabul edilmektedir. Gerçekten de fiziksel altyapının zorunluluğu, siber uzay için bir hakikattir.

İlkel tarzda alet ve makine kullanımından farklı olarak “siber” eylemlerin gerçekleşmesini sağlayan unsur ise fiziksel varlıklar üzerinde kurulup işletilen mantıksal yapıdır. Bu yapı, elektriğin belli protokol ve prosedürler dahilinde kullanımıyla anlamlı sonuçlar ortaya çıkarmaktadır. İnsanın fiziksel ve mantıksal yapılar ile etkileşime girmesi, makine ve insan ilişkisinde “siber” noktasına gelmesini sağlar. “Veri (*data*)”, fiziksel ve mantıksal boyutlar içerisinde dolaşarak siber uzayın esaslı bir unsurunu teşkil eder. İnsan ise siber uzayın hem kurucusudur hem de boyutlarla girdiği etkileşime binaen bir başka esaslı unsurdur.

Siber uzayın yukarıdaki şekilde iki boyutlu ve iki unsurlu bir teorik uzay olarak ele alınması; siber eylem ve durumların, belirli bir “t” zamanında, uzaydaki konumunun analiz edilebilmesi ve bu konumun egemenlik ile ilişkilendirilmesi açısından kullanışlı bir yaklaşım olacaktır.

a. Fiziksel Boyut

Siber uzayın fiziksel boyutu, siber uzayı oluşturan fiziksel varlıkların varoluşlarını sergiledikleri alanı ifade etmektedir. İnsanlık, siber uzayı fiziksel altyapı üzerine inşa etmiştir ve yine fiziksel altyapı ile kurduğu etkileşimle siber uzayın bir parçası haline gelebilmiştir. Kastedilen fiziksellik ise sadece cihazlardan veya kablolar gibi bağlantı elemanlarından ibaret olmayıp; Wi-Fi, bluetooth, infrared, NFC, vb. sistemlerde kullanılan frekans dalgaları gibi, elle tutulur gözle görülür olmayan fakat fizik bilimi içerisinde var olan unsurları da kapsamaktadır.¹¹⁴ Bilgisayarlar, depolama araçları,

¹¹⁴ Bu noktada literatürde bir kavram karmaşası olduğu da görülmektedir. Bazı çalışmalarda kablosuz bağlantı sistemleri için “fiziksel olarak bağlı olmayan iki veya daha fazla nokta arasında” gibi ifadeler kullanılırken (bkz. Deepak Kataria, Amarpal Yadav ve Bhupender Pratap Singh, “Wireless Communication Systems: Bluetooth, Infrared, Zig bee, NFC and Wi-Fi Outline”, **International Journal of Innovative Research in Technology**, Vol.1, Iss.6, (2014), s.585.), siber uzay modellerine dair çalışmalarda fiziksel katman yapısı içerisine kablosuz bağlantıların da dahil edildiği görülmektedir; bkz. JP 3-12, I-3. Günlük dildeki kullanım alışkanlığının bir sonucu olarak fiziksellik; dış görünüş ve nesne ile ilişkilendirilmektedir. Siber uzayın fiziksel boyutundan/katmanından bahsedilirken ise kasıt, fizik bilimine göre var olan unsurlardır.

kablolar, kablosuz bağlantı sağlayan alıcı/vericiler ile dalgalar, yönlendiriciler (*router*), modemler, vb. birçok unsur fiziksel boyutu oluşturmaktadır.

Bir fiziksel varlığın siber uzayın parçası sayılması için hangi kriterlere sahip olması gerektiğinin tespiti, siber uzayın belirliliği açısından önemlidir. Bir cihazdan bahsedildiğinde; cihazın bilgiyi dijital formda depolaması ya da bilgi işleme / berim¹¹⁵ (*computing*) kabiliyetine sahip olması onu siber uzayın parçası haline getirecektir. Bu kabiliyetlere sahip cihazları birbirine bağlayan elemanlar için de aynı sonuç söz konusudur.

Literatürde genel kabul, siber uzayın temelinin “ağ” hatta “ağlar ağı” olduğuna yöneliktir. Nitekim çoğu çalışmada bulunan haliyle “fiziksel katman” da JP 3-12 belgesinde “fiziksel ağ katmanı” adıyla yer bulmuştur.¹¹⁶ Bu kabul büyük ölçüde isabetli olmakla birlikte belli noktalarda soru işareti doğurmaktadır. Her ne kadar siber uzay düşüncesi, ortaya çıkışını web ve internet gibi gelişmelere borçlu olsa da devlet ve egemenlik merkezli yaklaşıldığında; yukarıdaki kıstaslara sahip bir fiziksel varlığın, bir ağa bağlı ya da bağlanabilir olmasa dahi siber uzayın parçası olduğu söylenebilecektir. Örneğin; 5237 sayılı Türk Ceza Kanunu m.226(3-4)’te belirtilen içeriklerin dijital formda “depolanmasında” kullanılan bir harici disk, ağa bağlı olmasa da siber uzayın parçasıdır ve bu parça ile üzerinde taşıdığı verilerin devlet ile ilişkisi söz konusudur. Nitekim insanın siber-etkin hale geçmesi, zorunlu bir fiziksel zemin üzerinde dijital haldeki veriyle ve aracı protokollerle etkileşime girmesi sonucu gerçekleşmektedir. Farklı noktadan bir örnek olarak, berim kabiliyetine sahip bir fırın dahi siber uzayın parçasıdır. Hatta bu türden bir cihazın siber saldırıya maruz kalması durumunda fiziksel zararların doğması ihtimali de söz konusudur. Başka zaviyeden bir örnek de ağ kurulumunda kullanılan bağlantı elemanlarıdır. Bunlar da devletlerin kara, deniz ve hava ülkelerinde bulunmaları itibarıyla siber uzayın fiziksel boyutunun devlet ile irtibatlı noktalarındandır.

¹¹⁵ Halit Oğuztüzün, “Berimsel bir Deneme”, https://users.metu.edu.tr/bozsahin/berimsel_bir_deneme-ho.html (31.12.2024).

¹¹⁶ JP 3-12, I-3.

b. Mantıksal Boyut

Fiziksel boyuttaki varlıkların kabiliyetleri sayesinde, karmaşık işlemler çok hızlı bir şekilde gerçekleştirilebilmektedir. İnsanın fiziksel bir vasıta ile etkileşime geçtiği andan, elde etmek istediği sonuca ulaşmasına kadarki periyotta birtakım mantıksal süreçler işlemektedir. Bir dijital hesap makinesinin tuşuna basıldığında ekranda karşılığının gözlemlenmesinden, bir akıllı cihaza (*smart device*) sesli talimat verilmek suretiyle blok zinciri (*blockchain*) üzerinden kripto varlık aktarımı yapılmasına kadar tüm siber eylemlerde aynı durum söz konusudur.

Fizik kuralları, insanlara mantıksal yapılar oluşturma imkânı tanımaktadır. İnsanlık da tercihleriyle bu imkânı belirli kural, standart ve protokoller dahilinde kullanmıştır. Bir verinin bir cihazda nasıl depolanacağı ya da işleneceği; bir başka cihaza nasıl aktarılacağı veya farklı cihazlarda ortak bir verim sürecinin nasıl işletileceği gibi birçok sürecin şartları bu çerçevede belirlenmiştir. İşletim sistemleri, donanım sürücüler, depolama ve transfer protokolleri, yazılım, uygulama ve servisler, web siteleri, veri tabanları gibi çok sayıda yapı; hiyerarşik ve katmanlı şekilde birlikte çalışarak siber uzayın mantıksal boyutunu oluşturmaktadır. Mantıksal boyut, bu özelliği sayesinde üzerine sürekli yeni parçaların eklendiği, mevcut olanın da şekil değiştirebildiği, esnek ve özyinelemeli (*recursive*) bir yapıdadır; bu sebeple Clark da siber uzay hakkında “platformlar üstündeki platformlar üstündeki platformlar” tabirini kullanmıştır.¹¹⁷ İnsan – makine ilişkisinin, ilkel seviyeden “siber” seviyesine ulaşmasını sağlayan da yine mantıksal boyut olmuştur.

Klasik siber uzay teorisinde siber uzayın bizzat kendisi kavramsal bir uzay veya sanal bir gerçeklik olarak kabul edilmişti. Esasen bu kabul, fiziksel arayüzler vasıtasıyla etkileşime geçilen mantıksal boyutun insan zihnindeki karşılığının siber uzay olarak adlandırılmasından ileri gelmektedir. Halbuki yukarıda belirtildiği gibi siber uzay, fiziksel temellerden ve sanal algıyı oluşturan sözdizimlerinden bağımsız şekilde var olan bir bilim kurgu ürünü olmanın ötesinde, kapsamlı bir teoriye sahip hale gelmiştir.

¹¹⁷ Clark, s.3.

Mantıksal boyutta yer alan varlıklar, siber uzayın ilgili düzenleyicilerince belirlenen normlar çerçevesinde var olmakta ve işlemektedir. Söz konusu yapı; fikri mülkiyet, otonom sistemlerin işlemlerinden kaynaklanan sorumluluk, norm ve standartların tespiti, veri tabanı, web sitesi yahut uygulama/servis gibi platformlara erişim vb. birçok yönden devlet ile temas noktalarına sahiptir. Bunların bir kısmı fiziksel altyapı ile ayrılmaz bir bütün halinde ele alınırken bir kısmı da sadece mantıksal yapısı itibariyle bu ilişkinin konusu olmaktadır.

c. Veri / Bilgi Unsuru

Bilgi sistemlerinin bel kemiği konumundaki *data – information – knowledge – wisdom* (DIKW) hiyerarşisi üzerinde yoğun akademik tartışmalar süregelmektedir.¹¹⁸ Halihazırda birbirinin yerine dahi sıkça kullanılan bu kavramların Türkçe çevirilerinde *data* için “veri” ve *wisdom* için “irfan (ya da bilgelik)” tercihleri genel kabul görmüş olsa da “*information – knowledge*” ikilisi “bilgi – birikim”, “enformasyon (malûmat) – bilgi” gibi çeşitli kombinasyonlarda ve yine birbirinin yerine kullanılabilmektedir. Yerli literatürde -bu sahadaki pek çok kavramda olduğu gibi- çeviri problemiyle karşılaşılrsa da onlarca farklı tanımın bulunduğu uluslararası literatürde en azından anlam itibariyle genel geçer bir mutabakat bulunduğunu söylemek mümkündür.¹¹⁹

Siber uzay analiz edilirken, unsur olarak yukarıda katman isimlendirmelerinde örnekleri görüleceği üzere, literatürde *data* veya *information* kavramları tercih edilmektedir. Eldeki çalışmaya dahil disiplinler baz alındığında, *information* kavramının “*information technology* (IT)”, “*information system*” gibi ifadelerde dilimize bilgi/bilişim karşılığıyla yerleştiği görülmektedir. Özellikle 2016’da Avrupa Birliği’nin kabul ettiği “Genel Veri Koruma Tüzüğü (*General Data Protection Regulation* (GDPR))”¹²⁰ ve Türkiye’de yürürlüğe giren 6698 sayılı “Kişisel Verilerin Korunması Kanunu

¹¹⁸ Saša Baškarada ve Andy Koronios, “Data, Information, Knowledge, Wisdom (DIKW): A Semiotic Theoretical and Empirical Exploration of the Hierarchy and its Quality Dimension”, **Australasian Journal of Information Systems**, Vol.18, No.1, (2013), s.6.

¹¹⁹ 2007 yılında yayımlanan bir çalışmada, *data*, *information* ve *knowledge* kavramları için 45 yazardan toplam 130 farklı tanım alınmıştır. Tanımlar farklı şekillerde inşa edilmiş olsa da kavramsal karşılıklar açısından ortak bir zemin bulunduğu gözlemlenebilmektedir; Chaim Zins, “Conceptual Approaches for Defining Data, Information, and Knowledge”, **Journal of the Association for Information Science and Technology**, Vol.58, Iss.4, (2007), ss.479-493.

¹²⁰ Tüzük metni için bkz. <http://data.europa.eu/eli/reg/2016/679/oj> (31.12.2024).

(KVKK)”¹²¹ ile birlikte, veri ve kişisel veri kavramları da hukuk disiplininde ön plana çıkmıştır. İki metinde de paralel şekilde “kişisel veri (*personal data*)” kavramının, “kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgi (*information*)” anlamında kullanılması, iki kavram arasındaki geçişkenlik için önemli bir örnektir. Ayrıca 5651 sayılı “İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun”¹²² ile de veri için “bilgisayar tarafından üzerinde işlem yapılabilen her türlü değer”; bilgi için ise “verilerin anlam kazanmış biçimi” tanımları yapılmıştır. DIKW hiyerarşisindeki veri ise özetle; tek başına anlam ifade etmeyen, gözlem veya ölçüm sonucunda elde edilen semboller/değerler dizisi olarak ifade edilebilir.¹²³ Anlatılan bu durum, ilgili kelimelerin bilgisayar biliminde ve sosyal bilimlerde farklı şekilde algılanmasından ve tanımlanmasından kaynaklanmaktadır. Siber uzay söz konusu olduğunda ise veri için dijitallik esastır; bilgi de ham verinin işlenmesiyle ortaya çıkan sonuçtur. Bu bakımdan, siber uzay için ilgili unsurun hem veri (*data*) hem de bilgi (*information*) bağlamında değerlendirilmesi isabetli olacaktır.

Siber uzaydaki temel faaliyet konusu, fiziksel ve mantıksal boyutlar arasında işleme tabi tutulan dijital veridir. Bu işlem depolama, aktarma veya berim şeklinde olabilmektedir. Dijital formdaki her bir bit veri, siber uzayın birer parçası olmakla birlikte; geleneksel sistemlerle analiz edilemeyecek kadar büyük miktardaki veri topluğu olan “büyük veri (*big data*)”¹²⁴ veya verilerden zuhur eden (*emerge*) bilgi de yine siber uzaya dahil unsurlardır. İnsan, dijital veri üzerinde fiziksel ve mantıksal boyutlar vasıtasıyla tasarrufta bulunabilmektedir. Bu ilişki konsepti, siber uzayın en kısa ifadesi olarak dahi yorumlanabilir.

Siber uzayın hukuk ve egemenlikle ilişkilendirilmesinde, dijital verinin ve bundan zuhur eden bilginin tasnifi önem arz etmektedir. Bu noktada da inisiyatif daha çok sosyal bilimler alanına geçmektedir. Nitekim dijital veriyi konu alan bilgisayar biliminde veri ham haliyle ele alınmakta, veriye dair çalışmalar bu zemin üzerinde yürütülmektedir.

¹²¹ R. G., 24.03.2016, Sayı.29677.

¹²² R. G., 04.05.2007, Sayı.26530.

¹²³ Zins, ss.480-487.

¹²⁴ Korcan Doğan ve Sacit Arslantekin, “Büyük Veri: Önemi, Yapısı ve Günümüzdeki Durum”, **Ankara Üniversitesi Dil ve Tarih-Coğrafya Fakültesi Dergisi**, Cilt.56, Sayı.1, (2016), ss.22-23.

Verinin insan için “anlam” kazanması, zihinsel bir sonuçtur. Örneğin, 41°01'28.4"N, 29°00'49.4"E şeklindeki bir sayı, harf ve sembol dizisi, dijital olsun veya olmasın veri olarak kabul edilir. Bu verinin siber uzaya dahil oluşu, dijitalleşmesiyle gerçekleşir. Fakat dijital hale geldiğinde bilgisayar bilimi bu verinin depolanması, işlenmesi ve transferi gibi eylemlerin teknik kısmını esas almakta, veriyi de bu perspektiften ele alıp tasnif etmektedir. Söz konusu sayı ve sembol dizisinin coğrafi bir konumu ifade ettiği “bilgisi” ise beşeridir. Nitekim veri dijitalleşmiş olmasa dahi bu çıkarım insan tarafından yapılabilmektedir; öyle ki konum verilerinin formunu belirleyen de yine insandır. Diğer yandan bu konum verisi, bir X kişisine ait kimlik verisi ile eşleştğinde artık bir kişisel veriden bahsedilecek ve bu kişisel veriden zuhur eden “X kişinin mevcut konumu” bilgisine erişilecektir. Siber uzayın, dijital formdaki verileri bünyesinde barındırdığı gibi bunlardan zuhur eden ve insan zihniyle anlam kazanan bilgiyi de bünyesinde barındırdığı kabul edildiği takdirde, literatürdeki geçişkenlik ve karışıklık bu alana yansıtılmadan çözüme gidilebilecektir. Böylece yukarıdaki tüzük ve kanunda kurulan “kişisel veri = ...bilgi” denkleminin de sosyal bilimler bağlamında açıklaması yapılabilecektir.

Dijital verinin; üretildiği kaynağa göre, hak sahibinin tanıdığı erişim iznine göre, depolandığı veri tabanına göre, işlendiğindeki algılanış türüne göre (görsel, işitsel, yazılı vb.) gibi kriterlere dayalı sınıflandırılması mümkündür. Bu verilerin taşıdığı bilgiler ise; kime ve neye dair olduğu, gizlilik durumu, maddi değeri gibi özellikleri ile yine sosyal bilimler bağlamında sınıflandırılabilir.

d. İnsan Unsuru

Siber uzay, doğal bir fenomen değil; insanın fiziksel üretiminin sonucunda zihinsel olarak kurguladığı bir teorik uzaydır. İnsan siber uzayı kurar, kurallarını belirler ve işletir. Buradaki fiillerin hepsi insan kaynaklıdır. Yukarıda bahsedildiği üzere, JP 3-12 belgesinde varsayılan “siber-kişilik katmanı”, insan veya bot (otomatikleştirilmiş) fark etmeksizin ağ veya bilgi teknolojisi kullanıcı hesaplarını ve bunların birbirleriyle olan ilişkilerini kapsamaktaydı.¹²⁵ Oysa botlar ve kullanıcı hesapları esasen mantıksal yapılardır. Özellikle botlar her ne kadar fiillerinde bağımsız görünse de netice itibarıyla insan yapımı algoritmalar dahilinde işleyen mantıksal süreçlerden ibarettir. Dolayısıyla

¹²⁵ JP 3-12, I-3.

siber uzayda esas olanlar; insan, insan fiilleri ve insanın siber uzayın diğer unsurları üzerindeki hak ve yetkileridir.

II. EGEMENLİK

Uluslararası (milletlerarası) hukuk, adlandırma itibariyle “ulusların (milletlerin)” aralarındaki bir hukukun varlığına işaret etmektedir. Modern uluslararası hukukun klasik yaklaşımı, bilhassa 2. Dünya Savaşı’na ve BM’nin kuruluşuna kadarki süreçte -hukuki pozitivizmin de etkisiyle- devletleri, uluslararası hukukun tek süjesi olarak ele almış; uluslararası hukuku, devletler arası ilişkileri düzenleyen bir hukuk dalı olarak kabul etmiştir.¹²⁶ Bir disiplinin “devletlerarası” ya da “uluslararası” adıyla anılması arasında temelde fark olduğu açıktır. Fakat modern devletin (*state*) doğuşu ve egemenliğin ulusa (*nation*) atfedilmesi gibi gelişmeler sonucunda devlet, ulus egemenliğinin kullanıcısı ve görünen yüzü haline gelmiştir. Dolayısıyla, kurgusal yapılar olan ulusların birbirleriyle ilişki biçimleri, ancak somutlaşmış devlet yapılanmaları vasıtasıyla gözlemlenebilir olmaktadır. Hatta ulusun politik yönünün, dini, etnik, tarihi, kültürel ortaklıklardan çok daha ön planda olması,¹²⁷ kurumsallaşmış devlet yapılarının ulusları biçimlendirdiği sonucuna da götürmektedir. Bugün “uluslar”arası hukuktan bahsedilmesi de bu şekilde mümkündür. Söz konusu ilişki biçimlerini görünür hale getiren bir diğer yapı olan ve bu hukuk sisteminde aldığı rol vasıtasıyla “uluslararası hukuk süjesi” unvanını elde eden uluslararası örgütlerin de esaslı unsurları sivil yapılar değil, bizzat yine devletlerdir. Devlet ise belirli ülke parçaları (kara-deniz-hava) ve üzerindeki insan toplulukları üstüne mutlak olarak hukuk vazeden ve bunları tatbik eden yapıdır. Bu kabiliyeti de “egemenlik” kavramı ile kazanmıştır.

İnsan algısına temas eden bütün varlık ve kavramlar bir hukuki “durum” sahibidir. Hukuk ise mevcut uluslararası sistemde devlet egemenliği ile doğrudan ilgilidir. Siber uzay gibi mahiyeti yeni tespit edilmekte olan yarı soyut ve küresel bir yapının da hukuki durumu kaçınılmaz olarak uluslararası hukukun ve tabii olarak devletin ilgi ve etki alanına girecektir. Siber uzaya ilişkin hukuki kuralların belirlenmesi, icra edilmesi ve

¹²⁶ Yusuf Aksar, *Teoride ve Uygulamada Uluslararası Hukuk – 1*, 6. Baskı, Ankara: Seçkin Yayıncılık, 2021, s.225.

¹²⁷ Paul James, *Nation Formation: Towards a Theory of Abstract Community*, Cambridge: SAGE Publications, 1996, s.5 vd.

devletler arasındaki yetki paylaşımının yapılması gibi modern meydan okumaların çözümü, “egemenlik” kavramının ve uluslararası hukukun egemenliği ele alış biçiminin doğru analiz edilmesinde saklıdır.

A. Tarihsel ve Teorik Düzlem

1. İktidar

Canlı veya cansız bütün varlıklar, tabiat kanunlarına bağlı olarak bir güç ilişkisi içerisindedir. İnsanı farklı kılan ise, yine bu kanunlara tabi olsa dahi güç ilişkilerini iradi olarak şekillendirebilmesidir. Bir şeyi yapma kudretine sahip olmak şeklindeki ferdi güç sahipliği bir tarafa; kural koymak, uygulamak, değiştirmek, başka bir süreyi bir eyleme ya da duruma icbar etmek gibi fiiller, irade sahibi canlının güç ilişkilerinin sonucudur. İktidar kavramı bu sebeple; “*aktörlerin kendi durumlarını ve geleceklerini tayin etme kapasitelerini şekillendiren etkilerin sosyal ilişkiler vasıtasıyla üretimi*” şeklinde tanımlanmıştır.¹²⁸ Bu ürün “toplumsal iktidar” şeklinde de ifade edilir. Bir yönetim ilişkisinden bağımsız olarak, sosyal yapının olduğu her durumda toplumsal iktidarın doğal olarak varlığının kabulü mümkündür.¹²⁹ Toplumsal iktidarın kullanımı için gerekli gücün “ekonomik, ideolojik ve siyasal” olarak üç farklı kaynaktan sağlandığı belirtilmiştir.¹³⁰ Bu tasnif aynı sırayla “ekonomik, sembolik ve fiziksel” şeklinde de yapılabilmektedir.¹³¹

Devlet, Akal’a göre “*siyasal iktidar tiplerinden bir tip*” olarak kabul edilebilir ve hiyerarşik olarak diğer tiplerin üstünde veya altında değildir.¹³² Nitekim toplumun olduğu her yerde toplumsal iktidar ilişkisi ve toplumsal iktidarın söz konusu olduğu her yerde de siyasal iktidar olacaktır. Siyasal iktidar ilişkisi de toplumun kurallarını belirleyen “Yasa” ve bunun toplumda uygulanması arasında kurulan bağın sonucu olarak görülmüştür.¹³³

¹²⁸ Michael Barnett ve Raymond Duvall, “Power in International Politics”, **International Organization**, Vol.50, Iss.1, (2005), s.42.

¹²⁹ Mehmet Emin Büyük, “Machiavelli’den Grotius’e Egemenlik Kuramının ve Modern Devletler Hukukunun Gelişimi”, **İstanbul Hukuk Mecmuası**, Cilt.80, Sayı.1, (2022), s.305.

¹³⁰ Gianfranco Poggi, **Devlet: Doğası, Gelişimi ve Geleceği**, Aysun Babacan (Çev.), 4. Baskı, İstanbul: İstanbul Bilgi Üniversitesi Yayınları, 2014, s.4.

¹³¹ Ahmet Kemal Bayram, “Siyasetin Dili: Kavramlar, Kurumlar”, Davut Dursun ve Mustafa Altunoğlu (Ed.), **Siyaset Bilimi** içinde (28-57), Eskişehir: Anadolu Üniversitesi Yayınları, 2012, s.31.

¹³² Cemal Bali Akal, **İktidarın Üç Yüzü**, Birinci Baskı, Ankara: Dost Kitabevi, 1998, s.324.

¹³³ Ibid., s.323.

Vakıa odur ki söz konusu ilişkiye bütün sosyal yapılarda rastlamak mümkündür. Siyasal iktidar kavramı, her zaman olduğu gibi günümüzde de hayattadır ve modern devlet biçiminde görünmektedir. Siyasal iktidardan farklı olarak “egemenlik” ise siyaset bilimine ancak modern devleti doğuran süreç ile dahil olacaktır.

2. Kabuller ve Meşruiyet

Yöneten ve yönetilen ilişkisinin kurulduğu sosyal yapılarda yasa ve uygulama kurgusu oluşur. “Kurallar nelerdir” sorusundan önce “kurallar nasıl belirlenir” ve dolayısıyla “kuralları kim belirler” soruları her toplum için cevaplanması zorunlu ve öncelikli sorulardır. Daha sonra zincirleme şekilde “kuralları kim uygular”, “kural uygulayıcı nasıl belirlenir” ve dolayısıyla “kural uygulayıcıyı kim belirler” soruları gündeme gelecektir. Devamında ise “kurallar nasıl uygulanır” gibi usule ilişkin hususlar ve bunların nasıl belirleneceği gibi süregiden sorularla içtimai hayat inşa edilmiştir. Cevaplama faaliyetine girildiğinde ise “kabul” olgusuyla karşılaşılacaktır. Tarih boyunca insanlar isteyerek veya istemeyerek bazı cevapları kabul etmiştir. Kabuller, fiili mecburiyetler dışında genellikle “inanç” ile oluşmuş ve “meşruiyet” ile sonuçlanmıştır.

Vurgulamak gerekir ki; iktidarın Tanrı ile ilişkilendirilmesi, kayıt altındaki ve erişilebilir siyasi tarihin neredeyse tamamında görülebilen bir olgudur. Bu ilişki, iktidar sahibinin meşruiyetini Tanrı’dan alması şeklinde olabildiği gibi vahiyle gelen şer’î hükümlerin muktediri bağlaması şeklinde de teşekkül edebilir. Ayrıca Hristiyanlığın Avrupa’ya ulaşmasından sonraki süreçte Kilise’nin ve Papalık makamının ortaya çıkması; bu kurumların Roma İmparatorluğu’nun dağılmasıyla Avrupa’nın siyasi birliği açısından tek bir evrensel otorite olarak kalması ve *Respublica Christiana* ideolojisinin doğuşu¹³⁴ ile iktidar sahipliğinin dünyevi ve dinî iki farklı otorite arasında paylaşım konusu haline gelmesi, yine söz konusu ilişkinin siyasi tarih açısından büyük önem taşıyan bir başka görünüş biçimidir.

¹³⁴ Hakkı Hakan Erkiner, “Grotius Öncesinde İlk Modern Uluslararası Hukuk Düşüncesinin Oluştugu Tarihsel Koşullar ve Erken Klâsik Dönemdeki Öğreti”, **Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi**, Cilt.18, Sayı.1, (2012), s.59.

M.Ö. 3000'e kadar uzanan dönemlerde Mısır'da firavunların Tanrı'nın oğlu olduğu ve dolayısıyla tanrı olduğu kabul edilmiştir.¹³⁵ Hatta Mısır'daki siyasi gidişata göre öne çıkan tanrıların değiştiği ve dolayısıyla firavunların izaf edildiği tanrının da bu değişen kabullere göre tayin edildiği görülmektedir.¹³⁶ Kralların tanrısallığına dair benzer inanış aynı dönemlerde Mezopotamya uygarlıkları için de söz konusu olmuştur.¹³⁷ Antik Yunan site devletlerinde (polis) ise her sitenin bir koruyucu tanrısı olduğuna inanılmıştır. Dolayısıyla yurttaşların da tanrılarına ve yasalarına bağlılık gösterdikleri aktarılmaktadır.¹³⁸ Siteye karşı işlenmiş suçların Tanrı'ya karşı işlenmiş sayılacağı da bu durumun sonucu olarak kabul görmüştür.¹³⁹ Antik Yunan siyaset düşünürleri ise genellikle erdem ve bilgi temelinde siyasal iktidarı kullanacakların nasıl belirlenmesi gerektiği, yöneticinin vasıfları ve siteye nasıl hükmedilmesi gerektiği gibi konular üzerine eğilmişlerdir.¹⁴⁰ Eski Çin düşüncesinde odak doğaya dönüktür ve doğanın halkı sevdiği, idarecinin de doğaya uymak zorunda olduğu kabulü ifade edilmiştir.¹⁴¹ Türk tarihine gelindiğinde “kut” anlayışıyla karşılaşmaktadır. İslamiyet öncesinde Gök Tanrı inancına sahip olan Türklerde, kağanların devleti idare etme hak ve salahiyetine sahip olmalarının ancak Tanrı tarafından kendilerine verilen “kut” (hâkimiyet kudreti), “ülüg” (nasip ve kismet) ve “yarlıg” (Tanrı'nın izni ve kader) ile mümkün olacağı kabul görmüştür. Bu bakımdan hükümdarlık, Tanrı buyruklarını yerine getirmek için “Tanrı'nın yeryüzündeki gölgesi” sıfatıyla “görevli” olma hali olarak değerlendirilmiştir.¹⁴²

Hristiyanlığın doğuşundan hemen sonraki süreçte, Pavlus'un “*iktidar yalnızca Tanrı'dan gelir ve iktidardakiler Tanrı tarafından atanmışlardır*”¹⁴³ ifadesinde karşılık bulan meşruiyet inancı Avrupa'ya yayılmaya başlayacak ve zaman içinde yukarıda da

¹³⁵ Ömer Faruk Harman, “Firavun”, **Türkiye Diyanet Vakfı İslam Ansiklopedisi**, Cilt.13, İstanbul: Türkiye Diyanet Vakfı Yayınları, 1996, s.118

¹³⁶ Mürüvvet Kurhan, “İmparatorluk Tanrısı Amon”, **Belleken**, Cilt.59, Sayı.226, (1995), s.501.

¹³⁷ Ercüment Yıldırım, “Türklerdeki Kut Anlayışı ile Mezopotamya'daki Kralın Kutsallığı İnancının Karşılaştırılması”, **Atatürk Üniversitesi Türkiyat Araştırmaları Enstitüsü Dergisi**, Sayı.70, (2021), ss.333-335.

¹³⁸ Hüseyin Sevinç, “Antik Yunan'da Siyasal Yapı ve Aristo ile Platon Özelinde Siyasal Düşünüş”, **Ekonomi İşletme Siyaset ve Uluslararası İlişkiler Dergisi**, Cilt.7, Sayı.2, (2021), s.210.

¹³⁹ İlhan F. Akın, **Devlet Doktrinleri**, 3. Baskı, İstanbul: Beta, 2016, s.1.

¹⁴⁰ Halil İbrahim Aydın ve Veysel Ayhan, “Egemenlik Kavramının Tarihsel Gelişimi Perspektifinden İktidarın Sınırlandırılması Tartışması”, **Cumhuriyet Üniversitesi İktisadi ve İdari Bilimler Dergisi**, Cilt.5, Sayı.1, (2004), ss.69-70.

¹⁴¹ Ibid. s.69.

¹⁴² Kayhan Atik, “Türklerdeki Kut Anlayışına Karşılaştırmalı Tarih Açısından Bakış”, **Akademik Sosyal Araştırmalar Dergisi**, Yıl.5, Sayı.60, (2017), ss.210-211.

¹⁴³ Gérard Mairet, “Padovalı Marsilius'dan Louis XIV'e Laik Devletin Doğuşu”, Cemal Bali Akal (Ed), **Devlet Kuramı** içinde (215-244), 4. Bası, Ankara: Dost Kitabevi Yayınları, 2013, s.217.

değinilen iktidar bölünmesinin temelleri atılacaktır. İslam toplumlarında ise devlet başkanlığı (imamet), meşruiyetini “şeriata ittiba” kıstası üzerinden kazanmaktadır.¹⁴⁴ Bu noktada Hristiyan siyaset düşüncesine göre temel fark, bir iktidar bölünmesinin söz konusu olmamasıdır. Nitekim Hristiyanlık orijin itibariyle siyasi nitelikte değildir ve ancak Roma’ya ulaşmasından sonra “devletleşip” iktidara ilişkin fonksiyonlarda belirleyici konuma gelmiştir.¹⁴⁵ İslamiyet ise Hz. Muhammed’in hem peygamber hem de siyasi iktidar sahibi olmasının sonucu olarak devlet fonksiyonlarıyla birlikte doğmuştur. İmâmetin söz konusu niteliğini Cüveynî şu ifadelerle açıklamıştır:¹⁴⁶

“İmâmet, din ve dünya önderliğidir. Nasıl ki, imamın dünyevî işleri idare edişinde (tedbîr) kendi kendine yeten biri olması gerekliyse; dinî işlerde de böyle olması gerekir. Çünkü dünya işleri şeriatın belirlediği çerçeve üzere cereyan eder. İmam, ahkâmın tüm sahasında imamdır, kendisine tâbi olunan biridir. [Onun] re’yunin şeriatın muktezasınca olması gerekir. [Zira] şeriatın gerekli kılmadığı hiçbir şeye itimad edilmez.”

3. Avrupa’nın İki Kılıcı

Siyasal iktidarın modern anlamda devlet egemenliğine geçişini anlamlandırmak için, egemenlik kavramının ortaya çıktığı topraklarda uzun soluklu bir çekişmenin nüvesini taşıyan İki Kılıç Kuramı’nın ve devamındaki sürecin üzerine eğilmek gerekir. Modern anlamda egemenlik kavramı ortaya çıkana dek Orta Çağ Avrupası’nın sahne olduğu bu süreçte şüphesiz, sayısız olay ve düşünürün büyük etkisi söz konusudur. Eldeki çalışmada yalnızca önemli kilometre taşlarından bahsedilerek ilgili süreç kısaca özetlenecektir.

Batı Roma’nın çöküşüyle ortaya çıkan otorite boşluğunda Doğu Roma’nın olası tahakkümünden azade kalmak isteyen *Papa I. Gelasius*, dünyanın yönetiminde biri piskoposların kutsanmış otoritesi (*auctoritas*), biri de kral iktidarı (*potestas*) olmak üzere

¹⁴⁴ Kavak, bu esası şöyle izah etmiştir: “Başa gelen yönetici “din ve dünya işleri konusunda Hz. Peygamber’in halifesi olması hasebiyle genel lider” görüldüğünden ve “tayin edilmesi pek çok şer’î yükümlülüğün gerçekleşmesinin kendisine bağlı olması hasebiyle farz olduğundan” vazifeleri de “şeriata ittiba” ilkesinin doğal bir uzantısı olarak “Allah’ın kullarının gözetilmesi/yönetilmesi (ri’âyetü ibâdillâh)” ile “Allah’ın hükümlerinin muhafazası (hıfzu ahkâmillâh)” olarak belirlenir.”, Özgür Kavak, “Hal’, İstifa ve İhtilal: İslam Devletlerinde İktidarın El Değiştirmesi Üzerine Bazı Tespitler”, *Dîvân Disiplinlerarası Çalışmalar Dergisi*, Cilt.24, Sayı.47, (2019), s.145.

¹⁴⁵ Haşim Özpolat, “Tanrının Siyasetinden Siyasetin Tanrısına Egemenlik Kuramının Dönüşümü”, *Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi*, Cilt.23, Sayı.2, (2017), s.147.

¹⁴⁶ İmâmü’l-Haremeyn el-Cüveynî, el-Gıyâsî: Gıyâsü’l-ümem fi’l-tiyâsî’z-zulem, nşr. Abdülazim ed-Dîb, 2. bsk., Mektebâtü’l-kübra, [y.y.] 1981, s.85, Aktaran: Özgür Kavak, “Siyasî-Fıkhî Ahkâmın’ Fıkıh Usûlü Zemininde Temellendirilmesi: Cüveynî’nin el-Gıyâsî’sinde Kat’iyyât-Zanniyyât Ayrımı ve Modern Yorumları”, *Dîvân Disiplinlerarası Çalışmalar Dergisi*, Cilt.14, Sayı.27, (2009), s.22.

iki iktidar olduğunu ileri sürdüğü bir mektup kaleme almıştır.¹⁴⁷ Kutsal otoriteyi ve dünyevi iktidarı temsil eden bu ayrım, “iki kılıç” metaforu olarak sonradan *Gelasius*’a atfedilmiştir.¹⁴⁸ Söz konusu ayrım, yukarıda üzerinde durulan yasa ve uygulama kurgusunun bölünerek iki farklı iktidar odağının ortaya çıkmasına kapı açmıştır. Oysa yine yukarıda görüldüğü üzere iktidarın meşruiyetini tanrısal kaynaktan aldığı birçok farklı örnekte böyle bir durum söz konusu olmamıştır. Tarih boyunca, hangi inanç olursa olsun, inancının gereklerine ve Tanrı buyruğuna hâkim kişi ve grupların varlığı ve bunların hükümdara etkide bulunması doğal bir sonuçtur. Fakat dönemin siyasi boşluk atmosferinde kurumsal yapısı ve kitleler üzerindeki kuvvetli etkisiyle Kilise zamanla büyük güç kazanmış, siyasal iktidarla rekabete girmiş ve nihayet 11. Yüzyıla gelindiğinde, iki kılıca birden sahip olma girişiminin *Papa VII. Gregorius* tarafından aşağıdaki seçili ilkelerle deklare edildiği noktaya ulaşılmıştır.¹⁴⁹

“*Md. I. Roma Kilisesi yalnızca Tanrı tarafından kuruldu.*
Md. VII. Yalnızca Papa emperyal simgeler kullanabilir.
Md. IX. Papa hükümdarların ayaklarını öptüğü tek insandır.
Md. XII. Papa imparatorları tahtından indirebilir.
Md. XIII. Papa'nın kararını kimse gözden geçiremez, ama o herkesin kararını gözden geçirebilir.
Md. XIX. Papa'yı kimse yargılayamazdır.”

Kilise’nin hakimiyetinin zirveyi görmesinden sonraki süreçte meydana gelen siyasi, askeri ve ekonomik gelişmeleri takiben, Batı düşüncesinin Orta Çağ’daki serüveni, yasa ve iktidarın meşruiyet kaynağının yeniden belirlenmesi ve dünyevi iktidardan Kilise’nin uzaklaştırılması yönünde seyretmiştir.

Padovalı Marsilius, insanların ancak yaşamsal ihtiyaçlarını karşılamak için bir araya gelip toplumu oluşturduklarını ileri sürerek din dışı bir sivil toplum tanımı yapmıştır.¹⁵⁰ Toplumun varoluş amacının dünyevileşmesi, pek tabii bu toplumun yönetiminin dayandığı ilkenin de dünyevileşmesini gerektirecektir. Dolayısıyla iki kılıçtan biri (*auctoritas*) tanrısal iradedden uzaklaştırılmıştır. Batı siyaset düşüncesinde temel ilkenin dini referanslardan soyutlanmasını takip eden süreçte *Machiavelli* bir adım

¹⁴⁷ Ayhan Yalçınkaya, “İlahi Siyaset”, Mehmet Ali Ağaoğulları (Ed.), *Sokrates'ten Jakobenlere Batı'da Siyasal Düşünceler* içinde (197-234), 6. Baskı, İstanbul: İletişim Yayınları, 2015, ss.225-226.

¹⁴⁸ *Ibid.*, s.226.

¹⁴⁹ Mairer, s.217.

¹⁵⁰ *Ibid.*, s.221.

ileri giderek; iktidarın meşruiyetinin, toplumun amacından bağımsız olarak bizzat iktidarın varlığından kaynaklandığını iddia etmiştir.¹⁵¹ Bu noktada *auctoritas*, iktidara sahip olma durumuna bağlanmış ve siyasal iktidar, hükümdarın fiziksel varlığıyla özdeşleşmiştir. İktidar sahibi öldüğünde yahut iktidarı yitirdiğinde, boşluğu dolduracak olan kişi sahip olduğu iktidar sayesinde yine meşruiyet kazanacaktır. Bu durum da modern egemenlik anlayışının süreklilik özelliğine aykırılık teşkil etmiştir.¹⁵²

4. Egemenliğin doğuşu

Egemenlik kavramının siyaset bilimi literatürüne girişinin *Jean Bodin* ile olduğu kabul edilir.¹⁵³ *Bodin*'in devlet düşüncesi, 1576'da yayınladığı “Devletin Altı Kitabı (*Les six livres de la République*)” eseri üzerinden ele alınmaktadır. Yazar, toplumun temelinde aileye büyük önem vermiş; iyi yönetilen bir ailenin, devletin gerçek bir görüntüsü olduğunu ifade etmiştir.¹⁵⁴ Ailenin devletten çok daha köklü bir müessese olması, aile idaresinin devlet idaresine benzer özellikler taşıması ve en önemlisi de kral iktidarının temelinde baba iktidarının bulunması gibi faktörler, *Bodin*'nin devlet düşüncesinde aileyi temel yapı taşı yapmıştır.¹⁵⁵ Nitekim eserinin hemen başında devlet (*République* (Fr.) – *Commonwealth* (İng.)) için “*birden fazla ailenin ve onların ortak çıkarlarının egemen bir güç tarafından adil bir şekilde yönetilmesi*” tanımını yapmıştır.¹⁵⁶ Tanımda ilgi çekici husus; devletin bir güç değil, bir sistem/süreç olarak ele alınmasıdır. İktidar sahibi, “egemen” bir güç olmalıdır. Devlet ise egemen gücün “yönetimidir”. İktidar sahibi zamanla değişecek ancak yönetim hali devam edecektir. Bu yaklaşım, *Machiavelli*'nin düşüncesinde atlanan esaslı noktayı tamamlamaktadır. Zira *Bodin*'e göre egemenlik mutlak, sürekli ve bölünmezdir.¹⁵⁷ Yazar, egemenlik anlayışına en uygun sistemin monarşi olduğunu düşünse de kralı egemenliğin kendisinde somutlaştığı iktidar sahibi olarak görür. Kral egemendir fakat egemenliğin bizzat kendisi değildir; *auctoritas* egemenlikte mündemiçtir ve *potestas* siyasal iktidar sahipleri arasında el

¹⁵¹ Ibid., s.233.

¹⁵² Büyük, s.312.

¹⁵³ Mehmet Ali Ağaoğulları, “Bodin'den Hobbes'a Doğru: Jean Bodin”, Mehmet Ali Ağaoğulları (Ed.), **Sokrates'ten Jakobenlere Batı'da Siyasal Düşünceler** içinde (401-415), 6. Baskı, İstanbul: İletişim Yayınları, 2015, s.401.

¹⁵⁴ Jean Bodin, **On Sovereignty: Six Books Of The Commonwealth**, M. J. Tooley (Çev., Ed.), Oxford: Basil Blackwell, 1955, s.6.

¹⁵⁵ Akın, s.82.

¹⁵⁶ Bodin, s.1.

¹⁵⁷ Ibid., s.24 vd.

değiştirmektedir.¹⁵⁸ *Auctoritas*ın yeni sahibini bulmasıyla, devletin tanrılaştırılması sürecinin de kapısı açılmıştır. *Schmitt*, “modern devlet kuramının bütün önemli kavramları, dünyevileştirilmiş ilahiyat kavramlarıdır”¹⁵⁹ derken esasen bu duruma işaret eder. *Bodin*’den sonra gelen bazı yazarlar da egemenlik düşüncesini “sözleşme” temeline oturtarak günümüz devlet anlayışının kurucuları arasında anılacaktır.

5. Sözleşmecî Düşünürler ve Modern Devletin Doğuşu

Bodin, her ne kadar temelde tanrısal özellikler taşıyan bir egemenlik düsturu ortaya koymuş olsa da yasanın amacı olarak adaleti görmesi ve hükümdarın bunu sağlamak adına tabii yasalara uyması gerektiğini ileri sürmesi, kendisinin egemenliği tam anlamıyla Tanrı’dan bağımsız olarak ele almadığını göstermektedir. Öyle ki hükümdar nihayetinde Tanrı’nın temsilcisidir ve sonunda Tanrı’ya hesap verecektir.¹⁶⁰

Bodin’den hemen sonra İspanyol Cizvit teolog ve filozof *Francisco Suárez*, yükselen laikliğe bir tepki olarak Papalık savunusuna girişmiştir. Fakat siyasal iktidarın doğal olarak var olduğunu ve tanrısal kökeni olduğunu, savunu gereği kabul etmiş olmasına rağmen; iktidarın kullanımını, toplum arasındaki açık veya gizli bir sözleşmeye dayalı olarak insanların iradesine bağlamıştır. İktidarın kaynağı Tanrı’dır fakat onu kullanana iktidarı teslim eden halktır.¹⁶¹ *Suárez* her ne kadar rejim olarak monarşiyi öngörse de düşüncesinde kralın gücünü sözleşmeyle yani ortak fayda ile sınırlamıştır. Ayrıca Papa’yı da sınırlandırarak dünyevi alana el atmaktan alıkoymuştur.¹⁶² Bu girişimi ile de *Bodin*’in getirdiği süreci devam ettirerek, egemenliği tanrısal temelden sosyal temele taşımıştır.

İnsan insanın kurdudur (*homo homini lupus*) söylemiyle maruf *Hobbes*, insanın devlet yokluğu kurgusundaki (doğa durumu) kötücül doğasından toplumu korumak adına, toplum sözleşmesi sonucu var olan ve *Leviathan* ismiyle sembolize ettiği bir egemen güç kurgulamıştır. Bu egemenlik anlayışında esas maksat, güvenliği sağlayacak

¹⁵⁸ Ağaoğulları, s.408.

¹⁵⁹ Carl Schmitt, **Siyasi İlahiyat: Egemenlik Kuramı Üzerine Dört Bölüm**, Emre Zeybekoğlu (Çev.), 2. Baskı, Ankara: Dost Kitabevi Yayınları, 2005, s.41.

¹⁶⁰ Akal, s.75.

¹⁶¹ Cemal Bali Akal, **Modern Düşüncenin Doğuşu: İspanyol Altın Çağı**, 2. Baskı, Ankara: Dost Kitabevi Yayınları, 1997, ss.206-207.

¹⁶² Ibid., s.213.

ve bir iç savaşa mahal bırakmayacak mutlak kudretin siyasal iktidara verilmesidir.¹⁶³ Toplum bütün yetkileri egemene devretmiştir zira buna mecburdur. Egemen ise sözleşmenin taraflarından biri olmadığı için kendisini bağlayan hiçbir ilke söz konusu değildir. Siyasal rejim ne olursa olsun egemenlik birdir, mutlak ve üzerinde hiçbir güç yoktur.¹⁶⁴ Görüldüğü üzere gerek Orta Çağ Avrupası siyaset düşüncesinin seyri gerekse de bölgedeki fiili koşullar sonucunda *Hobbes* tamamen ilahi nitelikler taşıyan bir devlet tasavvurunda bulunmuştur.

Hobbes'tan 124 yıl sonra doğan bir başka sözleşmeci düşünür *Rousseau*, nispeten benzer şekilde doğa durumunun kötülüğü üzerinden bir toplum sözleşmesi kurgulamış; fakat *Hobbes*'un radikal teorisine göre önemli bir farkla devleti totaliter yapıdan çıkarıp, insanların sahip olduğu hak ve özgürlükler ile devlet otoritesi arasında bir denge gözetmeye çalışmıştır.¹⁶⁵ *Rousseau* ve hemen sonrasında gelen diğer Fransız *Sieyes*, yukarıda özetlenen uzun sürecin sonunda “ulusal egemenlik” düşüncesinin temellerini atmışlardır. Hatta Fransız İhtilali'nin *Sieyes* ile başlayıp *Sieyes* ile bittiği bazı yazarlarca belirtilmiştir.¹⁶⁶ *Sieyes*, milleti “bir müşterek kanun altında yaşayan ve aynı yasa koyucu tarafından temsil edilen fertler topluluğu” olarak tanımlamıştır.¹⁶⁷ Günümüzde Türkiye Cumhuriyeti Anayasası'nda bulunan “*Türk Devletine vatandaşlık bağı ile bağlı olan herkes Türktür*”¹⁶⁸ hükmü dahi; Türk Milleti'ne dahil olmak için inanç, etnik köken, dil, kültür, tarihsel bağ vs. fark etmeksizin sadece anayasal vatandaşlık bağına yeterli sayması bakımından, *Sieyes*'in millet tanımında görülen yaklaşımı taşımaktadır. Aynı uyum, Anayasa'nın “*yasama yetkisi Türk Milleti adına Türkiye Büyük Millet Meclisinindir. Bu yetki devredilemez*”¹⁶⁹ hükmü için de söz konusudur. Sonuç itibarıyla milletin bir ferdi olma koşulu olarak vatandaşlık, kişiye devletin yasasıyla tanınan bir nitelik ve haktır. Vatandaş olan kişi, ilgili devletin yasasına tabidir ve dahil olduğu millet de vatandaşı olduğu devletçe temsil edilmektedir. Günümüzde adı ve yönetim şekli fark etmeksizin

¹⁶³ Mehmet Ali Ağaoğulları, Cemal Bali Akal ve Levent Köker, **Kral Devlet ya da Ölümlü Tanrı**, Ankara: İmge Kitabevi Yayıncılık, 1994, s.224.

¹⁶⁴ Ibid., s.228.

¹⁶⁵ Mehmet Ali Ağaoğulları, “Jean-Jacques Rousseau: Halk Kendini Yaratıyor”, Mehmet Ali Ağaoğulları (Ed.), **Sokrates'ten Jakobenlere Batı'da Siyasal Düşünceler** içinde (569-596), 6. Baskı, İstanbul: İletişim Yayınları, 2015, s.591.

¹⁶⁶ Akın, s.151.

¹⁶⁷ Emmanuel Sieyes, “Tiers Etat Nedir”, Süheyp Derbil (Çev.), **Ankara Üniversitesi Hukuk Fakültesi Dergisi**, Cilt.8, Sayı.1, (1951), s.152.

¹⁶⁸ T. C. Anayasası, m.66.

¹⁶⁹ T.C. Anayasası, m.7.

bütün devletler için literatüre ve günlük kullanıma yerleşmiş olan “milli yetki”, “milli marş”, “milli takım”, “milli menfaat” gibi sayısız örnek, modern ulus devletin bu yönünün yansımasıdır.

Günümüzde muhtelif tanımlar yapılabilse de modern anlamda egemenlik, özetle; devletin münhasır alanında salahiyyet sahibi en üst otorite olmasını ve diğer devletlerle birlikte bulunduğu uluslararası sistemde bu otoritesini bağımsız şekilde kullanmasını ifade etmektedir.¹⁷⁰ Egemenlik modern anlamına kavuşurken ulus, hükmi bir şahıs olarak doğmuş, ona irade atfedilmiş ve *auctoritas*ın Tanrı’dan uzaklaştırılması süreci, ulusa teslim edilmesiyle sona ermiştir. *Potestas* ise ulusun takdir ettiği şekilde kullanılmak üzere, yine ulusun takdir ettiği kişilere verilecektir.

6. Modern Egemenliğe Eleştiriler

İlahi özellikler taşıyan ve kaynağını ulustan alan egemen devlet düşüncesi, günümüz gerçekliğinde genel kabul görmüş olmasına karşın çeşitli açılardan eleştirilmiş ve çok farklı yönleriyle yorumlanmıştır. Sosyal bilimlerin üzerinde spekülasyon yapılması en mümkün kavramlarından olan devlet egemenliği hakkında, literatürde sayısı tespit edilemeyecek kadar fazla çeşitte eleştiri ve yorum bulunduğu şüphe götürmeyecektir. Yine de öğretilerdeki belli başlı örnekler, çalışmada ele alınan kavrama teorik hakkaniyetle yaklaşma adına kısaca aktarılacaktır.

Pozitivizm rüzgarının kuvvetli estiği dönemlerde, devletin varlığına sosyolojik açıdan yaklaşan *Duguit* gibi realist yazarlar, devletin ortaya çıkışı için, fiili üstünlüğün getirdiği yönetim kabiliyetinin varlığını yeterli görmüştür.¹⁷¹ Dolayısıyla *Duguit*, insan topluluklarının kişilik sahibi olamayacağını ileri sürdüğü için devletin de kişiliğinin varlığını reddetmektedir.¹⁷² Salt güç ilişkisinin varlığına dayalı bu yaklaşımın, modern devlet olgusunun diğer iktidar yapılarından farkını ortaya koymak açısından yetersiz kaldığı söylenmiştir -ki esasen *Duguit* tabii olarak buna ihtiyaç da duymamıştır-. *Mairet*,

¹⁷⁰ Tanım örnekleri ve çeşitli tartışmalar için bkz. Richard B. Bilder, “Perspectives on Sovereignty in the Current Context: An American Viewpoint”, *Canada-United States Law Journal*, Vol.20, (1994), s.10 vd.

¹⁷¹ Aydan Ömür Surlu, “Leon Duguit’in Devlet ve Hukuk Anlayışı”, *Erzincan Binali Yıldırım Üniversitesi Hukuk Fakültesi Dergisi*, Cilt.13, Sayı.3-4, (2009), s.117.

¹⁷² Leon Duguit, *Kamu Hukuku Dersleri*, Süheyye Derbil (Çev.), Ankara: Ankara Üniversitesi Hukuk Fakültesi Yayınları, 1954, s.46 vd.

devletten bahsetmek için, bir toprak parçasında bulunan insan topluluğunun iktidar ve dolayısıyla itaat ilişkisi kurmasının yeterli olduğu görüşüne karşı çıkarak; söz konusu farkın “egemenlik” kavramında vücut bulduğunu ileri sürmüş ve kastettiği egemenliğin, iktidarın tamamen din dışı bağlamda kendi meşruiyetini kendisinden bulması ile ortaya çıkacağını belirtmiştir.¹⁷³ Duguit ise aşkınlık gerektirdiği için egemenlik kavramını reddetmektedir. Zira aşkınlık, pozitivizme göre söz konusu olamaz. Kendisi bu konudaki düşüncesini aşağıdaki şekilde ifade etmiştir.¹⁷⁴

“Teokratik doktrinlerin hareket noktalarının anti-bilimsel olduğu meydandadır ve bundan dolayı tartışmağa bile değmez. Ama bu doktrinlerin de mantıklı olduğu apaçıktır. Gerçekten, eğer egemenlik var ise, o ancak insan iradelerine üstün bir iradenin kudreti olabilir; o halde bu kudret, tabiat üstü ve sonsuz kudrette bir varlık tarafından verilmedikçe mevcut olamaz.”

Konuya pozitivist çerçevede yaklaşan yazarlardan Kelsen, uluslararası hukukun ve devletlerin iç hukuklarının mevcut olduğu bir düzende -monizm teorisine dayanarak- egemenliğin ancak en yüksekteki sisteme atfedilebileceğini ileri sürmüş, hangi sistemin daha üstün olduğuna dair ise nesnel bir hükme varılamayacağını, bunun dünya görüşlerine göre değişeceğini ifade etmiştir.¹⁷⁵ Monist düşüncede bir toprak üzerinde hakim olan hukuk tek parça olarak kabul edildiğinde, bu hususun ulusların öznel tercihlerine bırakılması da doğal olacaktır. Uluslararası hukukun var olduğu bir dünyada ise egemenliğin klasik anlamda mutlak ve ilahi nitelikte ele alınması da soru işaretleri doğuracaktır. Konunun bu boyutuna uluslararası hukuk ve egemenlik bağlamında aşağıda ayrıca değinilecektir.

Schmitt, genel geçer egemenlik tanımını eleştiren yazarlardandır. Schmitt’e göre bir toprak üzerindeki “en üstün, hukuken bağımsız ve asli güç” ifadesi gerçekçilikten uzaktır. Ayrıca “güç”, hukukta hiçbir şeyi kanıtlamayacağı için egemenlik kavramının temel sorunu, fiili ve hukuki “en üstün güç” arasındaki bağlantıdır.¹⁷⁶ Yazara göre egemenlik kavramını doğuran süreç, yapılan tanımlar, kurulan soyut teoriler önemsiz ve anlamsızdır. Önemli olan somut durumdur ve devleti ancak, kendini korumak için hukuku

¹⁷³ Mairat, ss.217-218.

¹⁷⁴ Duguit, s.63.

¹⁷⁵ Hidemi Suganami, “Understanding Sovereignty Through Kelsen/Schmitt”, **Review of International Studies**, Vol.33, No.3, (2007), s.518.

¹⁷⁶ Schmitt, ss.24-25.

askıya alabileceği olağanüstü hale karar verebilmesi egemen kılacaktır.¹⁷⁷ Nitekim hukuk, egemenin vazettiğidir. Egemenin tehlikede olduğu durumlarda dahi bunu askıya alamayacağını düşünmek kavramın doğasına aykırı olacaktır.

Modern devletin, Tanrı iradesi – insan iradesi bağlamında eleştirisi, literatürde karşılaşılan ilgi çekici bir başka yaklaşımdır. Avrupa Orta Çağına hâkim olan Augustine’ci teodise, Hz. Âdem’den tevarüs eden “aslî günahı (*original sin*)” doğuştan insana yüklemiştir. Dünyadaki bütün kötülüğün kaynağı da Tanrı’nın özgür bıraktığı insandır.¹⁷⁸ İnsan iradesinin “zararlı” olduğu kabulü ile herkesin iyiliği için iktidar ve iradenin tamamen Kilise’ye hasredilmesi noktasına gelinmiştir. Sonradan insan iradesinin itibar kazanmasıyla devam eden gidişat, Avrupa siyaset düşüncesinin gelişimiyle paralellik içindedir. İnsanın hür iradesinin yok sayılmasına tepki olarak yükselen ve insan akli ile iradesini merkeze koyan hümanizm, Orta Çağ sonunda skolastisizme karşı akademik üstünlük sağlamıştır.¹⁷⁹ Kilise de Rönesans sürecinde nispeten “orta yolcu” bir konuma gelip, insan iradesinin tamamen yok sayılamayacağını ve insanların günahlarından arınma adına ilahi lütufla iş birliği yapabileceğini kabul etse de sonuçta aslî günah konusundaki inanç sabit kalmıştır.¹⁸⁰ İrade sahibi olmak aynı zamanda fail olmak demektir ve yukarıdaki teodise düşüncesine göre özünde “şer” olan bir fail de potansiyel olarak “şer faili”; kendisine mutlak irade tanınması durumunda da “mutlak şer faili” olacaktır.¹⁸¹ Her ne kadar modern düşünce, siyasal iktidarı ve meşruiyeti Tanrı iradesinden ayırmış olsa da bunları ulus iradesine atfetmesinin felsefi arka planında, insanın özü ile ilgili bu kabulün izlerinin bulunduğu düşüncesi serdedilmiştir. Öyle ki Tanrı hakimiyetinin yok sayıldığı bir dünyada, insanların özünde taşıdığı kötülük üretimini kontrol atında tutup düzeni sağlayacak bir iradeye ihtiyaç olacaktı. Bu ihtiyaca verilen cevabın kökenini, yukarıda bahsedilen sözleşmecî düşünürlerin devlet

¹⁷⁷ Ibid., ss.13-14; yazar ayrıca olağanüstü hali tanrısallık bakımından mucizeye benzetmiştir.

¹⁷⁸ Cafer Sadık Yaran, **Kötülük ve Teodise: Batı ve İslâm Din Felsefesinde “Kötülük Problemi” ve Teistik Çözümler**, Ankara: Vadi Yayınları, 1997, s.92.

¹⁷⁹ Ullrich Langer, **Divine and Poetic Freedom in the Renaissance: Nominalist Theology and Literature in France and Italy**, Princeton: Princeton University Press, 2014, ss.11-19

¹⁸⁰ Joseph M. Shaw ve Diğerleri (Ed.), **Readings in Christian Humanism**, Minneapolis: Fortress Press, 2009, s.308.

¹⁸¹ Bu denklem, *Lord Acton*’ın ünlü “*iktidar yozlaştırır, mutlak iktidar mutlaka yozlaştırır*” sözüyle özetlediği nedensellik ilişkisine benzetilmiştir; Bedri Gencer, “Keşf-i Kadimin Altı Kapısı”, Şanlıurfa Valiliği, **Uluslararası İslam Bilgeleri Zirvesi: Tebliğler** içinde (118-125), İstanbul: Marmara Matbaası, 2017, s.120.

tasavvurlarında bulmak mümkündür. Söz konusu durumu *Gencer* şu ifadelerle eleştirmektedir:¹⁸²

“Teodise zihniyeti için ilahî veya beşerî, küllî iradenin her türü tehlikeliydi. Çözüm, bir bütün olarak irade ve failiyyetin gayr-i iradî, mekanistik bir “görünmez el”e atfıydı. Hobbes’un Leviathan’ı, Adam Smith’in “görünmez el”i, hep bu görünmez canavarları, iradesiz failleri temsil ederler. Sonuçta adeta okulların imhasıyla eğitim probleminin de imhasının sanılması gibi, bizzat insanın ortadan kaldırılmasıyla şer probleminin de ortadan kaldırılacağı varsayılmıştır.”

Tanrı iradesinin dünyaya hâkim olduğu dönemlerin ardından gelen ve devletin kendisine tanınan egemenlik vasfıyla birlikte Tanrılaşması olarak bahsedilen süreç, bir bakıma olası otorite boşluğunun aslen dünyevi olan ama tanımı ilahi vasıflarla yapılan bir müessese ile doldurulmasını ifade etmektedir. İktidar, bir irade meselesidir ve bu sahadan “egemen” Tanrı iradesi çıkarıldığında geriye sadece insanların iradeleri kalmaktadır. Her bir ferdin iradesi ayrı ayrı egemen kabul edildiğinde sosyal düzenin inşası mümkün olamayacağından, fertlerin üzerinde yeni bir irade gerekliliği doğacaktır. Ulus, laik siyaset düşüncesinin bir ürünü olarak doğmuş ve yüksek irade yükünü yüklenmiştir. Egemen devlet ise başta değinildiği üzere ulus egemenliğinin kullanıcısı ve görünen yüzü olmuştur.

Günümüzde ulusun küllî bir iradenin boşluğunu doldurmaktaki, devletin de ulus iradesini yansıtmaktaki yeterlilikleri bilhassa tartışılmaya devam etmektedir.¹⁸³ Ayrıca klasik anlamıyla kendinden başka hiçbir ilkeyle bağlı olmayan ve ancak kendi kendini sınırlandırabilen egemen devlet modeli, özellikle insanlığın 2. Dünya Savaşı sürecinden çıkardığı dersler üzerinde yükselen doğal hukuk anlayışı -dolayısıyla insan hakları- ve faaliyete geçen BM sistemi ile bir derece törpülenmiştir. Egemenlik düşüncesi zirveye ulaşana kadarki dönemde bunalımlar egemenliği güçlendirirken, postmodernizm sürecindeki bunalımlar yeni meşruiyet arayışlarını ve egemen devlete karşı çizilmeye çalışılan yeni sınır çizgilerini doğurmaktadır.¹⁸⁴ *Kulick* bu eğilimin devletsizleşme (*de-etatization*) olduğu fikrinden hareketle, bireyin ve insan haklarının yükselişinden ayrı

¹⁸² Ibid.

¹⁸³ Fatih Ertugay, “Potestas ve Populus Arasındaki Mesafe Darılırken Auctoritas’ı Yeniden Ele Almak”, **Muhafazakâr Düşünce Dergisi**, Cilt.8, Sayı.31, (2012), s.209.

¹⁸⁴ Ibid., ss.220-221.

olarak siber uzay özelinde çok uluslu şirketlerin oynadığı düzenleyici rolü de mahut süreçle ilişkilendirmiştir.¹⁸⁵ Hal böyle olsa da mer’i hukuk düzenlerinde cari olan siyasal iktidar anlayışının “egemen devlet” olduğu küresel kabul görmüş sayılmaktadır. Modern anlamda “uluslar-arası” hukukun doğuşu da egemen devleti oluşturan sürecin bir sonucudur.

B. Uluslararası Hukuk ve Egemenlik

1. Uluslararası Hukukun Doğuşu

Bir ülke üzerindeki siyasal iktidarın doğasına dair cevap arayışlarının yanı sıra farklı ülkelerin iktidar sahipleri arasındaki iktidar ilişkine dair cevap arayışları da daima siyasi düşüncenin içerisinde yer almıştır. Modern devletin ortaya çıkışından önceki dönemlerde, siyasal iktidar yapıları arasındaki veya başta inanç olmak üzere belli farklılıklara sahip topluluklar arasındaki ilişkileri düzenleyen hukuk sistemlerinin işlediği görülmektedir. Tarihte bilinen ilk örnek olan Kadeş Antlaşması gibi antik metinler krallık şeklinde vücut bulan iktidar yapıları arasında hukuk tesis etmiştir. Antik Yunan’da site ve yurttaşlık müesseselerinin doğal sonucu “yabancılık” olmuştur. Yabancıların yabancılarla ve yurttaşlarla arasındaki hukuk ayrıca ele alınmıştır.¹⁸⁶ Roma’da benzer sistemin gelişmiş hali *jus gentium* ve *jus fetiale* ile inşa edilmiş; böylece gerek savaş, barış, anlaşma gibi konularda gerekse fethedilen yerlerdeki yabancıların devlet ve yurttaşlarla olan ilişkilerinde uyulacak hukuk normlarına rastlanabilmıştır.¹⁸⁷ İslam devletlerinin gayrimüslim devletlerle olan ilişkilerini “siyer” ilmi konu edinmiştir. Bu konudaki ilk ve temel klasik eser, *İmam Muhammed* tarafından yazılmış fakat orijinali bugüne erişemediği için *İmam Serahsî*’nin şerhi ile temsil edilen es-Siyerü’l-kebîr’dir.¹⁸⁸ Eser, tabii olarak zamanı itibarıyla modern anlamda uluslararası hukuk eseri olmasa da devletler hukuku açısından öncü ve kurucu niteliktedir.¹⁸⁹

¹⁸⁵ Andreas Kulick, “Regulating Cyberspace between Grotius, Lotus and Strasbourg”, **Heidelberg Journal of International Law**, Vol.80, Heft.2, (2020), s.560.

¹⁸⁶ Aristoteles, **Politika**, Mete Tuncay (Çev.), 16. Basım, İstanbul: Remzi Kitabevi, 2010, s.140.

¹⁸⁷ Erkiner, Grotius Öncesinde..., 2012, s.98.

¹⁸⁸ Oğuzhan Tan, “İslam Hukuk Literatüründe Bir Müşterek Metin İnşası Örneği Olarak Şerhu’s Siyeri’l-Kebîr”, **Turkish Studies**, Vol.13, Iss.17, (2018), s.289.

¹⁸⁹ Ahmet Yaman, “es-Siyerü’l-kebîr”, **Türkiye Diyanet Vakfı İslam Ansiklopedisi**, Cilt.37, İstanbul: Türkiye Diyanet Vakfı Yayınları, 2009, s.327.

Modern devletler hukuku sistemi, Orta Çağ sonrası Avrupa'daki siyasi gelişmelerle nedensellik ilişkisi içerisinde ortaya çıkmıştır. Dönemin düşünsel öncüsü ise İspanyol ekolü olmuştur.

Akılcı çıkarımları ve mantıksal tutarlılığı esas almış *Akinolu Tommaso*'yu izleyen Dominiken Tarikatı mensubu düşünürlerden *Francisco de Vitoria*, Roma'dan gelen *jus gentium* (kavimler hukuku) kavramını *jus inter gentes* kavramına dönüştürerek “kavimler arası” hukuku gündeme getirmiştir.¹⁹⁰ Bunun yanı sıra Papa'nın yargılama hakkını dini alanla ve dolayısıyla Hristiyan dünyasıyla sınırlı tutmuş; Hristiyanlıktaki haklı savaş (*bellum justum*) öğretisine de dokunarak, doğrudan emperyal yahut dini amaçlarla açılan savaşları reddetmiştir.¹⁹¹ Yeni keşfedilen yerlerin işgali sürecinde yerlilerin haklarını hukuk genel ilkeleri bağlamında değerlendiren *Vitoria*, bölgedeki uygulamaların haksız olduğunu da dile getirmiştir.

Vitoria'nın dönem ve ekol itibarıyla ardılı olan ve yukarıda siyaset düşüncesine kısaca değinilen *Suárez*, doğal hukuktan farklı olarak *jus gentium*un iradi nitelikte olduğunu ve değişen koşullara göre şekillenebileceğini ifade ederek onu “*tüm dünya milletleri arasında, yayılma ve karşılıklı taklitle gelişen adet ve geleneklerin ürünü*” olarak görmüştür.¹⁹² Görüldüğü üzere bu yaklaşım, Roma'daki anlayıştan çok farklı ve modern uluslararası hukuka çok benzer bir şekilde *jus gentium*un yeniden yorumlanması anlamına gelmektedir. *Suárez*'in, uluslararası uygulama ve akli normlar arasındaki farkı tespit etmesiyle pozitivizm geleneğinin başında durduğu ve tarihçi ekol için de bir eşik oluşturduğu belirtilmektedir.¹⁹³

İspanyol ekolünün bir diğer önemli üyesi de *Suárez*'in çağdaşı olmakla birlikte, teolog değil, asker kökenli bir hukukçu olmasıyla ayrılan *Alberico Gentilis*'dir. *Gentilis*, hukuk kurallarının dini hükümlerin etkisinden kurtarılması gerektiğini düşünmüş; haklı savaş kavramına seküler, enternasyonalist ve meşru müdafaa esaslı yaklaşmış; ayrıca savaş dışındaki birçok uluslararası hukuk konusunu da ele alarak, somut olaylardan

¹⁹⁰ Erkiner, Grotius Öncesinde..., 2012, s.99.

¹⁹¹ Akal, 1997, s.49.

¹⁹² Büyük, s.342.

¹⁹³ Erkiner, Grotius Öncesinde..., 2012, s.125.

kurama geiř yapmaya alıřmıřtır.¹⁹⁴ Sonu olarak *Gentilis* uluslararası hukukta seküler ekolün bařlangıcı olarak grlmřtr.¹⁹⁵

İřpanyol ekolnn Avrupa hukuk dřnesi zerindeki etkisi, “uluslararası hukukun babası” unvanına sahip bir *Hugo Grotius*’u doęurmuřtur. Nitekim *Grotius*’un İřpanyol olmamakla birlikte ilkesel olarak İřpanyol ekolne ait olduęu sylenmiřtir.¹⁹⁶ 1625 tarihli meřhur eseri *De Jure Belli ac Pacis* (Savař ve Barıř Hukuku), uluslararası hukuku ayrı bir disiplin halinde ele alan ilk alıřma olarak kabul edilmektedir.¹⁹⁷ *Grotius*, btn insanlar zerinde bir doęal hukukun varlıęını kabul etmekle birlikte bu hukuku, dini hkmlerden baęımsız, insan doęası ve mantıęa dayalı řekilde kurgulamıřtır.¹⁹⁸ yle ki *Grotius*’a gre Tanrı iki kere ikinin drt etmesini engelleyemez, dolayısıyla doęal hukuka da mdahale edemezdi.¹⁹⁹ *Grotius* dięer taraftan hukukun iradi ynn de *jus gentium* zerinden kabul etmiřtir. Roma Hukuku’ndaki *jus gentium*, *Grotius* ęretisinde *jus naturae* ile karřılanırken; Grotien anlamda *jus gentium*, devletlerin karřılıklı iliřkilerini dzenleyen ve zerinde mutabakata vardıkları bir kamu hukuku biimi olarak ele alınmıřtır.²⁰⁰ Modern uluslararası hukuk adına teorik baęlamda kurucu rol stlenen *Grotius*, biraz da yařadıęı dnem itibariyle egemenlięin devlete “insanlık hukuku” tarafından verilen bir yetki olduęunu dřndę iin, devletler hukukunu doęrudan devletlerin egemenlięine dayandırmamıřtır.²⁰¹

2. Vestfalya Barıřı ve Modern Uluslararası Hukuk İliřkisi

Uluslararası hukuk, babasını topraęa verdikten  yıl sonra; Avrupa devletler sistemini derinden etkileyecek Vestfalya Barıřı tesis edilmiřtir. Barıř ncesi sre ise

¹⁹⁴ Ibid., s.136.

¹⁹⁵ Ibid., s.137.

¹⁹⁶ James Brown Scott, *The Catholic Conception of International Law*, New Jersey: The Lawbook Exchange, 2007, s.128.

¹⁹⁷ Byk, s.344.

¹⁹⁸ Walter Simons, *The Evolution of International Public Law in Europe since Grotius*, New York: William S Hein & Co, 2004, s.5.

¹⁹⁹ Hugo Grotius, *On the Law of War and Peace*, Archibald Colin Campbell (ev.), Kitchener: Batoche Books, 2001, s.10.

²⁰⁰ Vladimir Đuro Degan, *Sources of International Law*, The Hague: Martinus Nijhoff Publishers, 1997, s.28.

²⁰¹ Mehmet Aydoęan zman, “Devletlerin Egemenlięi ve Milletlerarası Teřekkller”, *Ankara niversitesi Hukuk Fakltesi Dergisi*, Cilt.21, Sayı.1, (1964), s.63.

dünya tarihinin en uzun ve kanlı savaşlarından sayılan Otuz Yıl Savaşları'na sahne olmuştur.

Reform hareketi sonrasında Protestanlığın yükseliş ve yayılışı, halihazırda siyaseten dağınık olan Avrupa'yı dini temelde de bölünmeye götürmüştür. Bugünkü Almanya ve çevresine hâkim olan Katolik Kutsal Roma İmparatorluğu bünyesindeki prensliklerde yükselen Protestanlıkla mücadele bir iç savaşa dönüşmüş; üstüne üstlük İmparatorluk karşısında bağımsızlık isteyen Katolik prenslikler de iç savaşa farklı açıdan dahil olmuştur. Tüm bu karışıklık, Fransızların ve İsveçlilerin de katıldığı İmparatorluk karşıtı bir ittifak ve başta İspanyollar ile Kilise'nin İmparatorluk safında yer aldığı diğer bir ittifak arasında büyük ve umumi bir savaşa dönüşmüştür.²⁰² Oldukça girift ve çok değişkenli gelişmelerden müteşekkil savaşın esas önemi, modern uluslararası hukuk açısından doğurduğu sonuçtan kaynaklanır.

Esasen Osnabrück ve Münster'de aynı yıl içinde imzalanan iki antlaşmanın bütününe ifade eden Vestfalya Antlaşması, usule ilişkin iki yıl süren öncü tartışmalar ve üzerine dört yıl süren müzakerelerin ardından 1648'de akdedilmiştir.²⁰³ Henüz ilk maddelerinde “*Hristiyan, evrensel ve daimî barış; gerçek ve samimi bir dostluk ve kardeşlik*”²⁰⁴ ifadesi bulunan iki antlaşma, reel siyasi durumun yanında esasen din temeli üzerinde inşa edilmiş bir hoşgörü mutabakatı olarak da görülebilir. Papalık, müzakereler için aracı rol oynamakla birlikte ne müzakerelere katılmış ne de hükümlerini kesin bir dille kınayarak reddettiği antlaşmaya taraf olmuştur.²⁰⁵ Papalıkla ilgili bu durumun sonucunda, Antlaşma'nın en önemli özelliklerinden birinin laik nitelik taşıması olduğu literatürde belirtilmekle birlikte; aksine Papalığın sürece dahil edilmemesinin de dini kaygıların neticesi olduğu ve Antlaşma'nın, bahsi geçen ilk maddede işaret edildiği üzere bizatihi dini bir antlaşma olduğu da ileri sürülmüştür.²⁰⁶ Bu görüşe ilk bakışta metnin lafzı bağlamında hak vermek mümkündür. Gelgelelim dönemin hâkim düşünce yapısı ve

²⁰² Oral Sander, **Siyasi Tarih: İlkçağlardan 1918'e**, 12. Baskı, Ankara: İmge Kitabevi Yayınları, 2003, ss.99-100.

²⁰³ Stephen C. Neff, **Justice Among Nations: A History of International Law**, Massachusetts: Harward University Press, 2014, s.139.

²⁰⁴ Vestfalya Antlaşma'sının İngilizce metni için bkz. http://www.pax-westphalica.de/ipmipo/pdf/o_1732en-treatys.pdf (31.12.2024)

²⁰⁵ Neff, s.139.

²⁰⁶ Yaşar Salihpaşaoğlu ve Özgem Tuğçe Gümüş Boyacı, “Bir Modern Devlet ve Egemenlik Miti: Westphalia Barışı”, **Erciyes Üniversitesi Hukuk Fakültesi Dergisi**, Cilt.15, Sayı.1, (2020), ss.205-206.

paradigma gereği, bu tür metinlerin inşasında aksi bir tutumun imkânı tartışmaya açıktır. Zira benzer bir örnek olarak; Tanzimat Fermanı adıyla bilinen 1839 tarihli Gülhane Hatt-ı Hümayunu’nda da “*ahkâm-ı celîle-i Kur’âniyye ve kavânîn-i şer’iyyeye kemâliyle riâyet*” esasının devletin kudreti ve halkın refahı için önemi vurgulanmış, bu esasa bağlılığın tekrar sağlanması amacının taşındığı belirtilmiştir.²⁰⁷ Ancak metnin fehvasının, devletin kendisine tüzel kişilik kazandırılmak suretiyle modern devletler sistemine (Avrupa Kamu Hukuku’na) dahil edilmesi maksadını ve dolayısıyla laik modern devlet nosyonunun ilk izlerini taşıdığı görülmektedir.²⁰⁸ Dolayısıyla bu tür politik metinlerde, ortaya çıktıkları dönemin şartları gereği tercih edilen lafızlar ve metinlerin tarihteki konumları arasında bir nüansın varlığından bahsedilebilecektir.

Vestfalya Barışı ile ilgili genel kabul, egemen devletlerin ilişkilerinden müteşekkil laik modern uluslararası sistemin doğuşu olduğu yönündedir.²⁰⁹ Diğer taraftan Antlaşma’nın ancak savaş öncesi feodal düzene barış ve hoşgörü şartlarında geri dönüşü ifade ettiği görüşü de söz konusudur.²¹⁰ Yine de ortaya çıkan sonuç; Almanya topraklarında İmparatorluk’a karşı egemenliğe çok yakın yetkiler kazanan 300 civarı prenslik (devlet) ve zaferle mutlak monarşilerini güçlendirmiş krallıklar şeklinde görülmüştür.²¹¹

Vestfalya düzeninin başlangıcından sonra gelen ve aynı zamanda uluslararası hukukta klasik dönemin son yazarı olarak kabul edilen²¹² *Emerich de Vattel*, egemenliğe dair kendisine kalan mirası, mevcut siyasi duruma uygun şekilde ele almıştır. Yazar, “Uluslar Hukuku” olarak adlandırdığı disiplini, “*milletler veya devletler arasında var olan hakları ve bu haklara karşılık gelen yükümlülükleri öğreten bilim*” şeklinde

²⁰⁷ A. Şeref Gözübüyük ve Suna Kili, **Türk Anayasa Metinleri: Senedi İttifaktan Günümüze**, Ankara: Türkiye İş Bankası Kültür Yayınları, 1985, s.11.

²⁰⁸ Bedri Gencer, **Gelenekten Modernliğe Osmanlı**, İstanbul: Ketebe Yayınları, 2019, ss.527-533; *Zürcher* de söz konusu fermanın “*niteliğine ve bilhassa da içtenliğine ve ona dayalı Tanzimat politikalarına*” yönelik şiddetli tartışmaların varlığını hatırlatarak aslında bu gerçeği işaret eder; Erik Jan Zürcher, **Modernleşen Türkiye’nin Tarihi**, 28. Baskı, İstanbul: İletişim Yayınları, 2013, s.85.

²⁰⁹ Sander, s.101; Neff, s.140; Malcolm Shaw, **International Law**, Eighth Edition, Cambridge: Cambridge University Press, 2017, s.982.

²¹⁰ Vestfalya Barışı’nın genel kabul gören özelliklerine yönelik eleştirilerin detaylarına dair bkz. Salihpaşaoğlu ve Gümüş Boyacı, s.191 vd.

²¹¹ Sander, s.100.

²¹² Hakkı Hakan Erkiner, “Uluslararası Hukuk Düşüncesinde Klâsik Öğretinin Kuruluşu: Hugo Grotius ve Postgrotien Yazarlar Samuel Von Pufendorf, Richard Zouche, Cornelius Van Bynkershoek ve Samuel Rachel’e İlişkin İnceleme ve Değerlendirme”, **Marmara Üniversitesi Hukuk Fakültesi Dergisi**, Cilt.18, Sayı.3, (2012), s.5.

tanımlamıştır.²¹³ *Vattel*'in uluslararası hukuk anlayışı, ulus devletin egemenliğini ve bağımsızlığını merkezine almıştır.²¹⁴ Yazara göre ulus (devlet) egemenliği -başka devletlerin egemenliğini etkilememek kaydıyla- ancak içsel olarak sınırlanabilir ve hiçbir başka dış kuvvet tarafından sınırlanamaz; yani “*her devlet kendi eylemlerinin efendisidir*”.²¹⁵ Eğer bir devlet bu özgürlüğünü kötüye kullanırsa, “görevi ihlal (*breach of duty*)” suçu işlemiş sayılır; ancak diğer devletler, o devleti zorlama hakları olmadığından, ilgili davranışa razı olmak zorundadırlar.²¹⁶ Ayrıca tıpkı insanların eşit olması gibi devletler de güç, zayıflık veya büyüklük fark etmeksizin hukuk önünde eşittir.²¹⁷ Görüldüğü üzere *Vattel* henüz doğal hukuku reddetmemiş, devletlerin uyması gereken kaideler (görevler) olduğunu kabul etmiştir. Fakat geline nokta bir anlamda pozitivizmin eşiğidir. Bununla birlikte yazarın görüşleri gerek modern anlamda egemenlik ve “devletlerin egemen eşitliği” kavramlarına yaklaşma derecesi gerekse uluslararası hukuku devletlerin arasındaki egemenlik ilişkisi üzerinden yorumlaması açısından klasik dönem için etkileyici bir son katkı olarak değerlendirilebilecektir.

Avrupa’da tebaanın din tercihlerinin nispeten özgürleşmesi, siyasal iktidar yapılarının kendi topraklarındaki tasarruf hak ve kabiliyetlerinin bilhassa dini iktidardan soyutlanması, siyasal iktidar yapıları arasındaki ilişkinin daha eşitlikçi bir düzeyde düzenlenmesi gibi gelişmeler; “egemenlik” ve “ulus devlet” kavramlarının siyaset düşüncesinde ortaya çıkışıyla paralellik arz etmektedir. Söz konusu gidişat, doğal bir sonuç olarak hukuk sahasında pozitivizm hakimiyetini getirmiştir.

3. Uluslararası Hukukta Egemenliğe Pozitivist Bakış

Tanrı iradesini zamanla dünyevi düzenden uzaklaştıran Avrupa siyaset düşüncesi, insan akıl ve iradesini önce çıkardıkça, ampirik yöntem önem kazanmıştır. İdea ve ilkelerin doğal olarak var olmayıp deney ve gözlemden türediği önermesi ile *Locke*’un yaptığı çıkış ve devamında *Hume*’un tabiattaki nedenselliği reddedecek ölçüdeki

²¹³ Emer de Vattel, *The Law of Nations*, Thomas Nugent (Çev.), Béla Kapossy ve Richard Whatmore (Ed.), Indianapolis: Liberty Fund, 2008, s.67.

²¹⁴ Özman, s.63.

²¹⁵ Vattel, s.75.

²¹⁶ Ibid.

²¹⁷ Ibid.

düşüncesi ampirizmi yükseltmiştir.²¹⁸ Doğrudan Tanrı buyruğu olmasa da -yine Tanrı tarafından yaratılmış yahut tabiatta kendiliğinden oluşmuş- doğal kuralların varlığına yönelik kabul, aslında dünyevi düzen üzerinden kaldırılmak istenen Tanrı iradesinin ikamesini sağlama niyetinin bir göstergesi olarak görülebilirdi. Ampirik yöntemle uluslararası hukuka yaklaşıldığında ise artık devletlerin doğal kurallara göre “ne yapması gerektiği” değil yalnızca gerçekte “ne yönde irade gösterdiği” önem arz etmeye başlamıştır.²¹⁹

Devlet iradesi doktrininin ilk olarak *Hegel* tarafından ortaya konulduğu aktarılmıştır.²²⁰ *Hegel*, ulusun (dolayısıyla ulus-devletin) esaslı rasyonelliği ve doğrudan gerçekliği ile dünyadaki mutlak güç olduğunu, dolayısıyla her devletin diğer devletlerle ilişkilerinde bağımsız ve egemen olduğunu vurgulamıştır.²²¹ Nihayetinde *Hegel*’e göre egemenlerin birbiri üzerinde otoritesi olmadığı gibi aralarında nesnel ve evrensel bir hak alanı da yoktur: ilişkiler sürekli değişmektedir ve nihai çözüm savaş ile olmaktadır.²²²

Haenel’in, devletin yetkilerini bizzat tayin etme yetkisine (*kompetenez-kompetenz*) sahip olduğu düşüncesi ve *Jellinek*’in, devletin ancak kendi kendini sınırlayabileceği düşüncesi gibi göstergelerle ilerleyen pozitivist egemenlik yaklaşımının uygulamaya yansımaları, devletin herhangi bir üst ilkeyle bağlı kalmaksızın keyfi icraatlarına kapı açmıştır.²²³ Uluslararası sistemde süjelerin uymakla yükümlü olduğu doğal kuralların olmadığı, fiili durumda mevcut şartlar neyi hukuk olarak doğurduysa onun meşru kabul edildiği görüşlerin hakimiyetiyle geçen 19. yy, sonraki yüzyıla, ilk yarısını etkisi altına alacak üst üste iki dünya savaşı armağan etmiştir.

4. Birleşmiş Milletler Düzeni ve Self Determinasyon Hakkı

Dünya savaşları, özellikle II. Dünya Savaşı, uluslararası topluluk için dönüm noktası olmuştur. Öncelikle bir devletin kendi ülkesinde hiçbir ilkeyle bağlı kalmaksızın

²¹⁸ Wolfgang Friedmann, **Legal Theory**, Fifth Edition, New York: Columbia University Press, 1967, s.254.

²¹⁹ Shaw, s.19.

²²⁰ Ibid. s.21.

²²¹ Georg Wilhelm Friedrich Hegel, **Elements of the Philosophy of Right**, Hugh Barr Nisbet (Çev.), Allen W. Wood (Ed.), 18th Printing, Cambridge: Cambridge University Press, 2014, s.366.

²²² Friedmann, s.170.

²²³ Seha Lütü Meray, **Devletler Hukukuna Giriş – Birinci Cilt**, Üçüncü Bası, Ankara: Ankara Üniversitesi Siyasal Bilgiler Fakültesi Yayınları, 1968, s.299.

mutlak irade sahibi olmasının nasıl sonuçlar doğurabildiği görülmüştür. *Hegel*'in “nihai çözüm”ünün ülkeler ve milletler üzerindeki yıkıcı etkisinin, önceki dönemlere göre dramatik şekilde arttığı anlaşılmıştır. Belki en önemli sonuç olarak da nükleer silahların insanlık adına yeni ve geri dönülemez bir durum oluşturduğu gerçeğiyle yüzleşilmiştir. Oluşan zaruri farkındalığın sonucu olarak 1945 yılında imzalanan BM Şartı'nın giriş kısmı, “*Bir insan yaşamı içinde iki kez insanlığa tarif olunmaz acılar getiren savaş felaketinden gelecek kuşakları korumaya, temel insan haklarına, insan kişiliğinin onur ve değerine, erkeklerle kadınların ve büyük uluslarla küçük ulusların hak eşitliğine olan inancımızı yeniden ilan etmeye, adaletin korunması...*” ifadeleriyle başlamıştır.²²⁴ Günümüzde halen varlığını sürdüren “BM Düzeni”, bu ifadelerden anlaşılacağı üzere “insan hakları” ve ilkeler zemini üzerinde doğal hukukun yeniden yükselişinin göstergesidir.

BM Düzeni, egemen eşit devletlere²²⁵, birbirlerinin egemenliklerini tanıma, iç işlerine karışmama²²⁶, meşru müdafaa hakkı dışında kuvvet kullanmama²²⁷ gibi birtakım yükümlülükler yüklemiştir. Ayrıca uluslararası barış ve güvenliğin korunması adına BM bünyesinde Güvenlik Konseyi ihdas edilmiş; gerekli durumlarda (beş daimî üyeye tanınan veto hakkı ile birlikte) devletlere yönelik askeri müdahalede bulunulmasına imkân tanınmıştır.²²⁸

BM Düzeni'nin bir getirisi de Uluslararası Adalet Divanı'nın (UAD) kurulmasıdır.²²⁹ Divan'ın, Birleşmiş Milletler Hizmetinde Uğranılan Zararın Tazmini hakkında verdiği 1949 tarihli danışma görüşü ile BM zatında, uluslararası örgütlerin de kendilerini kuran antlaşmalarda belirlenen amaçlar dahilinde uluslararası hukuk kişiliğine sahip oldukları kabul edilmiştir.²³⁰

²²⁴ Şart'ın İngilizce metni için bkz. United Nations, United Nations Charter, <https://www.un.org/en/about-us/un-charter/full-text> (31.12.2024); Türkçe çeviri için bkz. Selami Kuran ve Diğerleri, **Uluslararası Hukuk Temel Metinler**, İkinci Baskı, İstanbul: Türkmen Kitabevi, 2011, s.3.

²²⁵ BM Şartı, m.2/1.

²²⁶ BM Şartı, m.2/7.

²²⁷ BM Şartı, m.2/4.

²²⁸ BM Şartı, m.24, m.42.

²²⁹ BM Şartı, m.92.

²³⁰ Reparation for Injuries Suffered in the Service of the United Nations, **Advisory Opinion**, ICJ Reports, 1949, s.8.

BM Düzeni'nin bugünkü halini alması, self determinasyon hakkına dayalı olarak sömürge durumundaki ulusların bağımsızlıklarını elde etmeleriyle gerçekleşmiştir.²³¹ Self determinasyon; halkların, yönetim esaslarını ve işleyişini kendilerinin belirlediği bir devlete sahip olma ve bu devleti idame ettirme hakkını ifade etmektedir. Köklerini ulus devletin serüveniyle paylaşan self determinasyon teorisi, 1851'de *Mancini*'nin "milliyetler prensibi" ile kendisine temel bulmuştur. Bu yaklaşımda, "*her milli topluluğun bağımsız bir devlet hale geline gelmesi*" "*meşru ve zaruri*" görülmüştür.²³² Her ne kadar sonrasındaki süreçte self determinasyonun uluslararası hukuka yerleşmesi zaman alacak olsa da Fransız İhtilali sonrasında imparatorlukların dağılıp ulus devletlerin ortaya çıkması, bu prensibin bir görünümü olarak kabul edilebilecektir. 20. yy başlarında hem SSCB'nin kurucusu *Lenin* hem de dönemin ABD başkanı *Wilson*, self determinasyon ilkesini bugünkü anlamıyla ele almışlardır.²³³ BM Şartı m. 55 ve m. 76 hükümleriyle uluslararası hukukun genel kabul görmüş bir ilkesi haline gelen self determinasyon, 1966'da BM bünyesinde akdedilen ve ikiz sözleşmeler olarak bilinen "Medeni ve Siyasi Haklara İlişkin Uluslararası Sözleşme" ve "Ekonomik, Sosyal ve Kültürel Haklara İlişkin Uluslararası Sözleşme" dahilinde bir "hak" olarak hükme bağlanmıştır.²³⁴ 1970 yılında BM Genel Kurulu kararıyla ilan edilen ve kısaca "Dostça İlişkiler Bildirgesi" olarak da bilinen "Birleşmiş Milletler Antlaşması Doğrultusunda Devletler Arasında Dostça İlişkiler ve İşbirliğine İlişkin Uluslararası Hukuk İlkeleri Konusundaki Bildirge" ile de devletlerin; halkları self determinasyon, özgürlük ve bağımsızlık haklarından mahrum bırakacak her türlü eylemden kaçınması gerekliliği tanınmıştır.²³⁵

Özellikle sömürge durumundaki Afrika ile Latin Amerika ülkelerinin ve eski SSCB ile Yugoslavya üyesi ülkelerin bağımsızlıklarını kazanmalarının temelinde self determinasyon hakkı ve *uti possidetis* ilkesi bulunmaktadır. *Uti possidetis* ilkesi, self

²³¹ Dekolonizasyon sürecine ve sürecin modern uluslararası sistemdeki sonuçlarına dair detaylı bilgi için bkz. Raymond F. Betts, **Decolonization: The Making of the Contemporary World**, Second Edition, Cornwall: Routledge, 2004.

²³² Meray, s.138.

²³³ Özlem Yücel, "Halkların Ekonomik (İktisadi) Self Determinasyon Hakkı ve Afrika'daki Halklar", **Adam Akademi Sosyal Bilimler Dergisi**, Cilt.4, Sayı.1, (2014), s.91.

²³⁴ Ibid., ss.91-92.

²³⁵ UN/General Assembly, Declaration on Principles of International Law concerning Friendly Relations and Cooperation among States in accordance with the Charter of the United Nations, A/RES/2625(XXV), 24.10.1970, s.123, https://treaties.un.org/doc/source/docs/A_RES_2625-Eng.pdf (31.12.2024).

determinasyon hakkının kullanımında, önceki durumda mevcut olan sınırların korunmasını öngörerek makul bir çerçeve çizmeyi amaçlamıştır. Self determinasyon hakkının ancak dekolonizasyon amacıyla ve *uti possidetis* ilkesine dayalı olarak öngörülen sınırlar içerisinde kullanılabileceği ve bunun dışında egemen devletlerin bünyesinden ayrılma yasağı olduğu belirtilir.²³⁶ Ayrıca, mevcut egemen devletler içerisindeki toprak bütünlüğü ilkesine aykırı ayrılıkçı hareketler meşruiyet dışı bırakılarak; self determinasyon hakkının sömürge idaresi, yabancı işgali, ve ırkçı yönetim biçimi (*apartheid*) gibi şartlar altındaki milletlere, mevcut durumlarından kurtuluş amacıyla tanındığı söylenebilecektir.²³⁷

Sonuç olarak özetlemek gerekirse BM Düzeni; devletlerin egemen ve eşit kabul edildiği fakat bazı devletlere Güvenlik Konseyi marifetiyle diğerlerinden farklı haklar tanındığı, devletlerin iradi olarak birtakım hususlarda egemenliklerinin kullanımını sınırlamakta mutabakata vardığı, dekolonizasyon süreci sonunda sömürge durumundaki halklarca kurulan bağımsız devletlerin işleyişe dahil olduğu, klasik uluslararası hukuk mantığından farklı bir şekilde uluslararası örgütlere de hukuk kişiliğinin tanındığı modern uluslararası hukuk sistemini simgelemektedir. Aşağıda bu sistemin devlet egemenliği telakkisine dair incelemelerde bulunulacaktır.

C. Modern Uluslararası Hukukta Devlet Egemenliğine Hâkim İlkeler

1. Egemenlik ve Bağımsızlık İlişkisi

Devletin, ülkesinde en üstün buyurma yetkisine sahip olması, teorik olarak onun üzerinde bir başka hukukun söz konusu olamayacağı anlamını taşımaktadır. Fakat uluslararası hukukun varlığı kabul edildiği takdirde devletin aynı zamanda bir hukuk süjesine dönüşmesi, mutlak anlamdaki egemenlik kavramı ile tenakuz doğurmuştur.²³⁸ Tanrısal vasıflar taşıyan bir varlık için sınırlamalardan ve sorumluluktan bahsedilemezken; uluslararası hukuk, devletleri fiillerinden sorumlu tutmaktadır.

²³⁶ Jörg Fisch, “Peoples and Nations”, Bardo Fassbender ve Anne Peters (Ed.), **The Oxford Handbook of the History of International Law** içinde (27-48), Oxford: Oxford University Press, 2012, s.47.

²³⁷ Hakkı Hakan Erkiner, **Uluslararası Terörizme Karşı Meşrû Müdâfaa**, 2. Baskı, Ankara: Seçkin Yayıncılık, 2021, s.68.

²³⁸ Meray, s.300; Hüseyin Pazarcı, **Uluslararası Hukuk**, 14. Bası, Ankara: Turhan Kitabevi Yayınları, 2015, s.148.

Egemen yapıların bir arada olmasıyla ortaya çıkan ilişki biçimi, modern dönemde mutlak egemenlik düşüncesini yıpratmıştır. Hal böyle olunca bazı yazarlar, uluslararası hukukta devletin esaslı vasfının “bağımsızlık” olduğunu kabul etmek suretiyle egemenlik ile bağımsızlığı eş anlamlı şekilde kullanmayı tercih etmişlerdir. *Brownlie*, iki kavramın eş anlamlı olarak kullanılabileceğini, bu açıdan dış ilişkilerini başka bir devletin yönetmesine izin veren veya başka bir devlete geniş kapsamlı sınır ötesi haklar tanıyan bir siyasi yapının egemen olamayacağını belirtmiştir.²³⁹ Bir başka görüşe göre ise egemenlik hukuki bir durumu ifade ederken bağımsızlığın fiili bir durumu ifade etmesi nedeniyle, egemenliği bağımsızlıkla eş anlamlı olarak kullanmanın doğruluğu tartışmalıdır. Ayrıca egemenlik devredilebilir niteliktedir, fakat bunun bağımsızlık kavramına uygulanması mümkün değildir.²⁴⁰ *Talmon*, bu düşüncesini Baltık devletleri, Vietnam, Kamboçya ve Laos örnekleriyle desteklemiştir. Yazara göre bir dönem Sovyet kontrolüne giren Baltık devletleri bağımsızlıklarını geçici olarak kaybetmiş olsalar da bu devletlerin egemenlikleri saklı kalmıştır. Vietnam, Kamboçya ve Laos ise fiili bağımsızlıklarını elde etmeden çok önce hukuken egemenlik sahibi olmuşlardır.²⁴¹ *Meray* da söz konusu meseleden yola çıkarak, modern uluslararası hukuk düzeni ile artık devlet egemenliğinin, “devletler hukukunca devletlere tanınmış ‘yetkiler’ manzumesi” ve “devletin devletler hukukunca çizilen sınırlar içinde ve tespit ettiği şekilde, geniş yetkiler kullanması” olarak kabul gördüğü bir noktaya geldiğini tespit etmiştir.²⁴²

2. İç Egemenlik – Dış Egemenlik Ayrımı

Egemenlik – bağımsızlık ilişkisinin sorgulanması ile bu kavramlar arasında bir anlamdaşlık arayışından farklı olarak, bağımsızlığı egemenliğin bir yönü olarak kabul eden ikili bir ayrım ortaya çıkmıştır.

Devletin, kendi ülkesi içinde en üstün buyurma yetkisine sahip olması ve ülke içinde bu yetkiyle rekabet edecek başka bir güç odağının bulunmaması durumu “iç

²³⁹ Ian Brownlie, *Principles of Public International Law*, Seventh Edition, New York: Oxford University Press, 2008, s.76.

²⁴⁰ Stefan Talmon, *Recognition of Governments in International Law: With Particular Reference to Governments in Exile*, Oxford, New York: Clarendon Press, 1998, s.50

²⁴¹ Ibid.

²⁴² Meray, s.300.

egemenlik” kavramı ile ifade edilmiştir.²⁴³ Bodin’in kanun yapma, savaş ve barış kararı alma, devlet memurlarını atama ve görevden alma, her tür mahkeme kararı için temyiz mercii olma, vergilendirme ya da muafiyetler sağlama, paranın değerini belirleme (para basma) örnekleriyle anlattığı yetkiler,²⁴⁴ devletin iç egemenliğinin sonuçlarıdır.

Dış egemenlik tamamen uluslararası sistemin ürünüdür. Devletlerin, diğer devletlerle ilişkilerini başka bir iktidar yapısının müdahalesi olmaksızın, serbest ve iradi şekilde belirleyip yürütmelerini ifade etmektedir.²⁴⁵ Tanımdan anlaşılacağı üzere dış egemenlikten kasıt, devletin bağımsızlığıdır. Egemenlik ve bağımsızlığın ayrı ayrı ele alınmasının aksine bu tasnifte bağımsızlık kavramı dış egemenlik ifadesiyle karşılık bulmuştur.

İç egemenlik ve dış egemenlik ayrımına gidilmesinin yanlış olduğu, hakikatte bunların tek bir egemenliğin farklı belirtilerinden ibaret olduğu görüşü de literatürde dile getirilmiştir.²⁴⁶ Yine de her durumda modern devletin, ülke sınırları içerisinde ve uyrukları üzerinde “egemen”, diğer devletlerle olan hukukunda “bağımsız” bir yapı olarak tanımlanması sonucuna ulaşılabilir. Devletin uluslararası hukuktaki bağımsızlığı, kendi iç egemenliğinin kullanımını sınırlandıracak uluslararası hukuk normları ile bağlanmasının iradi şekilde gerçekleşmesini sağlamaktadır. Tarih boyunca olduğu gibi mevcut durumda da ekonomik, askeri, politik birçok faktör sonucunda, özellikle zayıf devletlerin bağımsızlığının fiilen önemli ölçüde kaybolduğu örneklerle rastlansa da en azından mer’i uluslararası hukuk mekanizması bu şekilde işlemektedir. Söz konusu mekanizmanın tabii sonuçları olarak aşağıda incelenecek birtakım uluslararası hukuk ilkeleri ortaya çıkmıştır.

3. Devletlerin Egemen Eşitliği İlkesi

Modern uluslararası hukuk düzenini açıklamak için, devletlerin “egemen” ve “bağımsız” olma vasıflarının yanına, diğer devletlerle “eşit” olmalarını da eklemek gerekir. BM Şartı m.2/1’deki “*örgüt, tüm üyelerinin egemen eşitliği ilkesi üzerine*

²⁴³ Özman, s.59.

²⁴⁴ Bodin, s.44.

²⁴⁵ Meray, s.300.

²⁴⁶ Özman, s.60.

kurulmuştur” hükmü, esasen yukarıda incelendiği üzere daha önceki dönemlerde teorik olarak öngörülmüş bir yaklaşımın küresel kabule dönüşmesini ifade etmektedir. Şüphesiz ki egemen devletler için, taşıdıkları nicel özellikler bakımından bir eşitlik söz konusu değildir. Egemen eşitlik, devletlerin hukuk kişileri olarak süjesi oldukları hukuk önünde eşitliklerini ifade etmektedir. Eşitliğin devlet egemenliğinin doğal sonucu olarak görülmesi yaygın kabul olsa da normatif pozitivist bir örnek olarak *Kelsen*, ekolün önceki temsilcilerinden *Duguit*’e benzer şekilde egemenlik kavramının müphemliğini hatırlatmış; eşitliği ve eşitliğin pratik sonuçlarını doğuranın, egemenliğin kendisi değil, devlet iradeleriyle şekillenen normlar olduğunu ifade etmiştir.²⁴⁷

Egemen eşitliğin tanımı, Dostça İlişkiler Bildirgesi içerisinde yapılmıştır. Bildirgede egemen eşitlik şu şekilde izah edilmiştir:²⁴⁸

“Bütün devletler egemen eşitlikten yararlanırlar. Ekonomik, sosyal, siyasi veya diğer farklılıklara rağmen eşit hak ve yükümlülüklerle sahiptirler ve uluslararası topluluğun eşit üyeleridirler.

Egemenlik eşitlik hususen aşağıdaki unsurları içerir:

(a) Devletler hukuken eşittirler;

(b) Her devlet, tam egemenliğin doğasında bulunan haklardan yararlanır;

(c) Her devletin, diğer devletlerin kişiliklerine saygı gösterme yükümlülüğü vardır;

(d) Devletin ülkesel bütünlüğü ve siyasal bağımsızlığı dokunulmazdır;

(e) Her devlet, kendi politik, sosyal, ekonomik ve kültürel sistemini özgürce seçme ve geliştirme hakkına sahiptir;

(f) Her devlet, uluslararası yükümlülüklerine tamamen ve iyi niyetle uymak ve diğer devletlerle barış içinde yaşamakla yükümlüdür.”

²⁴⁷ Hans Kelsen, “The Principle of Sovereign Equality of States as a Basis for International Organization”, *The Yale Law Journal*, Vol.53, No.2, (1944), ss.207-208.

²⁴⁸ A/RES/2625(XXV), s.124.

Uluslararası hukukun emredici kurallarından (*jus cogens*) biri olduğu da kabul edilen²⁴⁹ egemen eşitlik ilkesinin işlerliğine ilişkin çok sayıda farklı görüş söz konusudur. Genel olarak BM Güvenlik Konseyi mekanizmasından hareket eden bu görüşlerden birkaçına dahi değinilmesi, ilkenin mahiyetinin izahı açısından faydalı olacaktır. Özman, BM Güvenlik Konseyi'nde beş üyenin daimî, diğerlerinin geçici olmasını fiili yönden; daimî üyelerin münhasıran veto yetkisine sahip olmalarını da hukuki yönden egemen eşitlik ilkesinin ihlali olarak görmüştür.²⁵⁰ Anand, Güvenlik Konseyi'nin doğurduğu eşitsizliğin savaş sonrası şartların ürünü olduğuna dikkat çekmiş ve galip devletlerin mevcut sistemi inşa sürecini ele almıştır.²⁵¹ Cassese ise devletlerin hukuken kısıtlanmasının ancak ilgili devlet tarafından tamamen özgürce kabul edilmesiyle mümkün olabileceğini belirtip, aksi duruma Güvenlik Konseyi'nin daimi üyeleri dışındaki BM üyesi devletleri örnek göstermiştir.²⁵² Sonuç itibarıyla BM Güvenlik Konseyi yapısının, beş devlete verilen imtiyaz ile egemenler arası ilişkide eşitsizlik doğurduğu kabul görmekle birlikte; üye devletlerin bu kısıtlamayı özgürce ve iradi olarak kabul ettikleri varsayımında, kuralın doğuş noktasında egemen eşitlik ilkesine yönelik bir ihlalden bahsedilemeyecektir. Bu konuda belirleyici kriter, ilgili normların kabulünde diğer devletlerin iradelerini gerçekten özgür şartlarda ortaya koyup koymadıklarıdır. II. Dünya Savaşı ve devamındaki süreç dikkate alındığında, bu kriterin gerçekten sağlandığını düşünmek kanaatimce fazla iyimser bir yorum olacaktır.

Egemen eşitlik ilkesi, bilhassa devletlerin ülkeleri dışında uluslararası topluluğu ilgilendiren meselelerde uluslararası hukuk yapımı için temel taşıdır. Bu meseleler, milli yetkiye tabi olmayan deniz alanları ya da uzay gibi mekânsal olabildiği gibi nükleer denemeler ya da iklim gidişatı gibi konularda politika belirlemeye yönelik de olabilmektedir. Siber uzay gibi hemen hemen bütün insanlığın temas kurduğu bir olgudan bahsedildiğinde de uluslararası hukuk açısından esaslı hareket noktası yine devletlerin

²⁴⁹ Devletlerin egemen eşitliği ilkesinin *jus cogens* norm niteliği hakkında çalışma için bkz. Yasin Öztürk, "Uluslararası Hukukta Devletlerin Egemen Eşitliği Kavramının *Jus Cogens* Niteliği", **Erciyes Üniversitesi Sosyal Bilimler Enstitüsü Dergisi**, Cilt.31, Sayı.42, (2017), s.37. Diğer yandan kural-ilke ilişkisinin tartışmaya açık yönünü de hatırlatmak gerekir; bkz. aşağıda "İlke Olarak Egemenlik ve Kural Olarak Egemenlik".

²⁵⁰ Özman, s.90.

²⁵¹ Ram Prakash Anand, "Sovereign Equality of States in International Law – I", **International Studies**, Vol.8, Iss.3, (1966), s.240.

²⁵² Antoino Cassese, **International Law**, Second Edition, New York: Oxford University Press, 2005, s.53.

egemen eşitliği ilkesi olacaktır. Eldeki çalışmanın ilgili bölümlerinde bu ilkeye mükerreren temas edilecektir.

4. Müdahale Etmeme ve Karışmama İlkesi

Devletlerin egemen yapılar olduklarının kabulü, onları uluslararası hukuk süjesi oluşlarında yatay hiyerarşiye yerleştirmiştir. Bu yerleşim de egemen eşitlik ilkesiyle ifade edilmektedir. Yatay hiyerarşinin eşitlik dışında diğer sonucu da devletlerin birbirlerinin iç işlerine karışmalarının ve müdahale etmelerinin²⁵³ uluslararası hukuka aykırılığıdır.

Devletin “iç işleri” ifadesinin temelinde “münhasır salahiyet” ve “milli yetki” kavramları yatmaktadır.²⁵⁴ Literatürde Fransızca “*domaine réservé*” terimiyle de anılan bu alan,²⁵⁵ BM Şartı’nda “iç yetki alanı (*domestic jurisdiction*)” şeklinde karşılık bulmuş ve konu hakkındaki hüküm şu şekilde düzenlenmiştir:²⁵⁶

“İşbu Şart’ın hiçbir hükmü, Birleşmiş Milletler’e, esas olarak herhangi bir devletin iç yetki alanına giren konulara müdahale etme yetkisi vermez veya üyelerin bu tür konuları işbu Şart kapsamında çözüme kavuşturmasını zorunlu kılmaz; ancak bu ilke VII. Bölüm’de öngörülen zorlayıcı önlemlerin uygulanmasına hâlel getirmez.”

Uluslararası hukuk, süjeleri arasındaki ilişkileri düzenler fakat devletler egemen yapılar oldukları için uluslararası hukukun etki alanı, devletlerin kendi iradeleriyle belirledikleri kadardır. Nitekim egemenlik, teorik olarak muktedire mutlak bir kudret tanıdığı için sınırlanması da esasen ancak yine muktedirin kendi iradesiyle olabilir. Bu denklem, uluslararası antlaşmaların iradi niteliğinin yanı sıra uluslararası örf ve âdet

²⁵³ Müdahale (*intervention*) ve karışma (*interference*) kavramları, anlam ve önem bakımından farklılık arz etmekle birlikte; uluslararası hukukta aynı derecede emredici ve yasaklayıcı kuralların konusu olup olmadıkları hususunda evrensel bir mutabakatın yokluğunda, sıklıkla birbirlerinin yerine kullanılmaktadır; Denitsa Raynova, “Towards a Common Understanding of the Non-Intervention Principle”, **European Leadership Network Post-Workshop Report**, 2017, s.2. İki kavram arasındaki ayrım aşağıda ayrıca ele alınacaktır.

²⁵⁴ Meray, s.306.

²⁵⁵ Helmut Rumpf, “Çağdaş Devletler Hukukunda Müdahale”, Rona Serozan (Çev.), **Hıfzı Timur’un Anısına Armağan** içinde (709-727), İstanbul: İstanbul Üniversitesi Yayınları, 1979, s.721; Tallin El Kitabı, s.314.

²⁵⁶ BM Şartı, m.2/7.

hukuku kurallarının ısrarlı itirazcı (*persistent objector*) konumdaki devlet için uygulanmaması ile de kendini teyit ettirmektedir.²⁵⁷

Tıpkı devletlerin egemen eşitliği ilkesinde olduğu gibi, iç işlerine karışmama ilkesinde de BM Şartı'nda bir genel kabule ve sonrasında doğrudan ilkeyle ilgili BM Genel Kurulu kararına rastlanmaktadır. 1965 yılında BM Genel Kurulu kararıyla ilan edilen “Devletlerin İçişlerine Müdahale Edilmesinin Reddi ve Bağımsızlıkları ile Egemenliklerinin Korunması Hakkında Bildiri” ile devletlerin, birbirlerinin iç veya dış işlerine doğrudan veya dolaylı olarak herhangi bir sebeple müdahale etme hakkı olmadığını belirtmiş; devletin kişiliğine veya siyasi, ekonomik ve kültürel unsurlarına karşı silahlı müdahale (*armed intervention*) ve karışmanın diğer her türü (*all other forms of interference*) veya tehdit girişimi kınanmıştır.²⁵⁸

“Hiçbir devlet, egemenlik haklarının kullanımının kendisine tabi kılınmasını sağlamak ya da herhangi bir avantaj elde etmek amacıyla başka bir devleti zorlamak için ekonomik, siyasi ya da başka türden önlemlere başvuramaz ya da başvurulmasını teşvik edemez. Ayrıca, hiçbir Devlet, başka bir Devletin rejimini şiddet yoluyla devirmeye yönelik yıkıcı, terörist veya silahlı faaliyetleri organize edemez, destekleyemez, teşvik edemez, finanse edemez, kışkırtamaz veya hoş göremez ya da başka bir Devletteki iç çatışmalara karışamaz.”

İlke aynı zamanda yukarıda bahsedilen Dostça İlişkiler Bildirgesi'nde de egemen eşitlik ilkesiyle birlikte tekrar edilmiştir.

Müdahale ve karışma kavramlarının literatürdeki kullanımında genel bir tutarsızlık ve belirsizlik söz konusudur. İkisini birbirinin yerine kullanan metinler olduğu

²⁵⁷ İsrarlı itiraz müessesesine ilişkin detaylı bilgi için bkz. Emre Öktem, **Uluslararası Teamül Hukuku**, İstanbul: Beta Basım Yayım Dağıtım, 2013, s.455 vd. Bu noktada “uluslararası hukukun emredici kuralları” olan *jus cogens* normlar için ayrı bir parantez açılması gereklidir. Zira *jus cogens* normların dahi nihayetinde iradi nitelikte olduğu ve bu sebeple ayırt edici değerini kaynağından değil devletlerce kendisine tanınan nitelikten aldığı söylenmektedir. 1969 Viyana Antlaşmalar Hukuku Sözleşmesi m. 53 hükmünde geçen “...devletlerin uluslararası topluluğunun bütünü tarafından...kabul edilen ve tanınan bir normdur” ifadesi, *jus cogens* normların bu özelliğine işaret etmektedir (Antlaşma metni için bkz. United Nations Treaty Series (UNTS), Vol.1155, No.18232, 1987, s.331 vd.). Fakat diğer taraftan uluslararası örf ve âdet hukuku kurallarından farklı şekilde *jus cogens* normların, baştan itibaren ısrarlı itirazcı konumda olsa dahi bütün devletler için bağlayıcı olduğunun kabulü, iradiliğin bir istisnası gibi görünmektedir. 1969 Viyana Sözleşmesi'ni onaylamayan Fransa'nın tek olmasa da en önemli gerekçesinin *jus cogens* normlara ilişkin hükümler olduğu bilinmektedir. Fransa'nın temel kaygısının *jus cogens* normların varlığı değil; devletlerin egemenlik haklarını tehdit edecek şekilde düzenlendiği yönündeki düşüncesi olduğu aktarılmıştır; bkz. Maurizio Ragazzi, **The Concept of International Obligations Erga Omnes**, Oxford: Clarendon Press, 2002, ss.67-72. Sonuç olarak uluslararası hukukta *jus cogens* norm kavramının hâkim görüşün kabul ettiği şekilde gerçekten iradeci pozitivist düşüncüyü mi yansıttığı yoksa iradeci görüntüsüne rağmen aslında tekil devlet iradesinin üstüne çıkabilecek doğal hukuk eğilimli bir kurum mu olduğu konusunun tartışmaya açık olduğunu söylemek mümkündür.

²⁵⁸ UN/General Assembly, Declaration on the Inadmissibility of Intervention in the Domestic Affairs of States and the Protection of Their Independence and Sovereignty, A/RES/20/2131(XX), 21.12.1965.

gibi ayrı kavramlar olarak kabul eden metinler de bulunmaktadır. Dolayısıyla kavramların içeriği ve uluslararası ilişkilerin tabiatı gereği ortaya çıkabilecek sayısız fiili durumdan hangilerinin bu bağlamda uluslararası hukuka aykırılık teşkil edeceği konusunda belirsizlik sorunu doğmaktadır.

UAD, Nikaragua Davası'na ilişkin 1986 yılındaki kararında, ilkeyle yasaklanan müdahale (*prohibited intervention*) eylemini “*politik, ekonomik, sosyal ve kültürel sistemin seçilmesi ve dış politikanın ifade edilmesi*” gibi devletlerin münhasır salahiyet alanlarına giren konularda zorlamada bulunulması şeklinde yorumlayarak, “zorlamanın (*coercion*)”²⁵⁹ yasağın esaslı unsuru olduğunu ifade etmiştir.²⁶⁰ Vincent -birçok yazarın müdahale ile karışmayı eş anlamlı kullandığını hatırlatarak- Oppenheim tarafından hukuka aykırı hususu ifade etmek için kullanılan “diktatörce karışma (*dictatorial interference*)” kavramına işaret etmiştir.²⁶¹ Devamında, hukuka aykırılıkta belirleyici faktörün “zorlama” olmasına binaen “zorlayıcı karışma (*coercive interference*)” ifadesini “müdahale” anlamına gelecek şekilde yorumlamıştır.²⁶² Roscini de teorisini aynı metot üzerine oturtmuştur.²⁶³ 1965 tarihli A/RES/20/2131(XX) sayılı bildiri lafzından öncelikle silahlı müdahalenin, karışmanın türlerinden biri olduğu ve diğer her tür karışma ile birlikte reddedildiği anlaşılmaktadır. Devamında ise yukarıda alıntılanan kısmında görüleceği üzere, yasaklanan eylemler için zorlama unsuru merkeze alınmıştır. Yerli literatürde sıklıkla referans gösterilen yazarlardan Keskin, çeviride kesin bir ayrıma gitmeksizin “karışma” ifadesini kullanmayı tercih etmiştir. Yazar, kuvvet kullanarak yapılan karışmalara ilişkin kuralların “kuvvet kullanma yasağı” ile daha muhkem hale geldiğini fakat kuvvet kullanma içermeyen bir karışmanın -ilkesel olarak hukuka aykırı

²⁵⁹ Zorlamaya dair birtakım mülahazalara Üçüncü Bölüm'de ayrıca yer verilmiştir; bkz. aşağıda “Uzaktan Siber Faaliyet ile Siyasi Bağımsızlığa Müdahale Edilmesi”.

²⁶⁰ Military and Paramilitary Activities in and Against Nicaragua (Nicaragua v. United States of America), Merits, **Judgment**, ICJ Reports, 1986, ss.107-108, para.205; Türkçe çeviri için bkz. Sertaç Hami Başeren, **Uluslararası Hukukta Devletlerin Münferiden Kuvvet Kullanmalarının Sınırları**, Ankara: Ankara Üniversitesi Basımevi, 2003, ss.96-97.

²⁶¹ Raymond John Vincent, **Nonintervention and International Order**. New Jersey: Princeton University Press, 1974, s.7.

²⁶² Ibid., s.8.

²⁶³ Marco Roscini, **International Law and the Principle of Non-Intervention: History, Theory, and Interactions with Other Principles**, Oxford: Oxford University Press, 2024, s.3.

olduğu kabul görmekle birlikte- tanım ve kapsamı konusunda bir mutabakatın olmadığını belirtmiştir.²⁶⁴

Müdahale ve karışmayı, müdahale etmeme (*non-intervention*) ve karışmama (*non-interference*) ilkeleri bağlamında iki ayrı hukuka aykırılık olarak kabul eden yazarlardan *Aloupi*, müdahalenin “ülkesel dokunulmazlık ve bütünlüğe” karşı; karışmanın ise devletin “bağımsızlık ve özyönetimine” karşı nitelikte olması üzerinden ayrımı ele almıştır.²⁶⁵ Tallin El Kitabı’nda izlenen yaklaşım da benzer niteliktedir. Eserde, devletin siyasi yapısı iki unsura ayrılmıştır. Bunlardan biri “*domaine réservé*” terimiyle anılan, devletin münhasır yetki alanıdır. Nikaragua Davası’nda, Dostça İlişkiler Bildirgesi’nde ve A/RES/20/2131(XX) sayılı bildiride vurgulandığı üzere; siyasi, ekonomik, sosyal ve kültürel sistemlerin seçilmesi ve dış politikanın oluşturulması, münhasır yetki alanının başlıca unsurlarıdır.²⁶⁶ Tallin El Kitabı yazarlarına göre siyasi yapının diğer unsuru da devletin bu alanlarda kullandığı ve doğası itibariyle hükümete ait olan fonksiyonlardır (*inherently governmental functions*). Bu kapsamda asıl olan, fonksiyonun doğası itibariyle devlet egemenliğinden kaynaklanması ve dolayısıyla devletin münhasır salahiyyet alanına giren konulara ilişkin olmasıdır. Zira fonksiyonların özelleştirilmesi de bu vasıflarını değiştirmeyecektir.²⁶⁷ Uluslararası hukukta söz konusu fonksiyonların fiile dönüşmüş hali de *acta jure imperii* olarak kabul edilir ve devletler bu işlemleri bakımından diğer devlet mahkemelerine karşı yargı bağımsızlığına sahiptir.²⁶⁸

Tallin El Kitabı’nda yapılan ayrımın özgün sonucu, *Aloupi*’nin ayrımına da yansıdığı üzere müdahaleyi münhasır yetki alanıyla; karışmayı ve gaspı (*usurpation*) ise doğası itibariyle hükümete ait olan fonksiyonlarla ilişkilendirmesidir. Tallin El Kitabı’nın genel editörü *Schmitt*, eserde yapılan ayrımı bir yazısında aşağıdaki şekilde gerekçelendirmiştir:²⁶⁹

“Domaine réservé bazen, seçimlerin yürütülmesinde olduğu gibi, doğası itibariyle hükümete ait olan fonksiyonlarla örtüşür. Ancak durum her zaman böyle değildir. Örneğin, eğitim faaliyetleri domaine réservé

²⁶⁴ Funda Keskin, *Uluslararası Hukukta Kuvvet Kullanma: Savaş, Karışma ve Birleşmiş Milletler*, Ankara: Mülkiyeliler Birliği Vakfı Yayınları, 1998, s.103.

²⁶⁵ Niki Aloupi, “The Right to Non-intervention and Non-interference”, *Cambridge Journal of International and Comparative Law*, Vol.4, Iss.3, (2015), s.572.

²⁶⁶ Tallin El Kitabı, s.315.

²⁶⁷ Tallin El Kitabı, ss.22-24

²⁶⁸ Wallace ve Ortega, ss.143-145.

²⁶⁹ Michael Schmitt, “Canada Takes on International Law in Cyberspace”, *EJIL:Talk!*, 14.07.2022, <https://www.ejiltalk.org/canada-takes-on-international-law-in-cyberspace/> (31.12.2024).

kapsamına girer ancak doğası itibariyle hükümete ait olan bir fonksiyon değildir; zira birçok devlette özel kuruluşlar eğitim sağlar. Benzer şekilde, kolluk doğası itibariyle hükümete ait olan bir fonksiyondur çünkü tevkif gibi fonksiyonları yerine getirmeye yalnızca devletler yetkilidir. Ancak kolluğun tüm yönleri domaine réservé kapsamına girmez. Bilakis, tevkif gibi birçoğu, uluslararası insan hakları hukukuna tabidir.”

Böyle bir tasnifin pratik kaygılarla yapılmış olması bir nebze anlaşılabilir olsa da ilkesel olarak münhasır yetki alanının, bir yetkinin/fonksiyonun hangi süljelerce kullanıldığından veya uluslararası hukuk normlarıyla iradi olarak söz konusu alanda devleti sınırlayıcı bir hüküm altına girilmesinden bağımsız ele alınması gerektiği kanaatindeyim. Bir devletin, münhasır yetki alanına giren bir hususta uluslararası hukuk normuyla bağlanması ve bu norma ulusal hukuk düzeninde yürürlük tanınması yine kendi münhasır yetkisine tabidir. Dolayısıyla bu tür bir bağlanmanın ilgili hususu münhasır yetki alanından çıkardığı düşünülemez. Ayrıca yukarıdaki örnekte görülen, eğitim hizmetinin özel kuruluşlarca verilebiliyor olması, Tallin El Kitabı’nda da vurgulandığı üzere fonksiyonun niteliğini değiştirmeyecektir.²⁷⁰ Neyin doğası itibariyle hükümete ait olduğunu tespit etmek doğal hukuk temalı bir süreçtir. Oysa egemen devletler arasında kurulmuş olan bir hukuk sisteminde asıl olan, devletin hangi konuları münhasır yetki alanında kabul ettiği ve ilgili fonksiyonların icra usulünü nasıl belirlediğidir. İfade ettiğim yaklaşıma karşı literatürde sıkça rastlanan görüş ise küreselleşmeyle birlikte devletlerin münhasır yetki alanında kalan hususların gittikçe azaldığını yönündedir. *Kunig*, bu durumun müdahale etmeme ilkesi ile korunan devlet menfaatlerinin tam olarak tespitini zorlaştırdığını; ayrıca dolaylı, sade ve basit bir karışma ile ilkeyi ihlal eden müdahale arasındaki sınırın tespiti adına da belirsizlik olduğunu ileri sürmüştür.²⁷¹

Yukarıda serdedilen görüşler ışığında, *Vincent*’in “bir devletin başka bir devlet içinde şiddetli bir çatışmaya girmesi kadar önemli veya bir devlet adamının yabancı bir devletin işleri hakkında söylediği kötü seçilmiş bir söz kadar önemsiz”²⁷² şeklinde betimlediği geniş yelpazenin esasen “karışma” eylemini ifade ettiği sonucuna varılabilir. Zorlama unsuru (devletin münhasır yetki alanındaki irade hürriyetine zarar verilmesi) ile

²⁷⁰ Ayrıca bkz. Frédéric Mégret, “Are There ‘Inherently Sovereign Functions’ in International Law?”, *American Journal of International Law*, Vol.115, No.3, (2021), s.452 vd.

²⁷¹ Philip Kunig, “Prohibition of Intervention”, *Max Planck Encyclopedia of Public International Law*, Oxford University Press, 2015, ss.1-2.

²⁷² Vincent, s.3.

ortaya çıkan “zorlayıcı karışma”, müdahale yasağının konusunu oluşturmaktadır. “Yasaklanmış müdahale” kavramı da bunu ifade etmektedir. Bu durumda, “‘karışma’ kavramını saf dışı bırakarak yukarıdaki yelpazenin tamamını ‘müdahale’ kapsamında ele alıp, zorlama unsurunun varlığı halini ‘yasaklanmış müdahale’ olarak adlandırmak” ile “yelpazenin tamamını ‘karışma’ kapsamında değerlendirip, zorlama içeren karışmayı bir alt küme olarak ‘müdahale’ başlığında ele almak” arasında gerçek bir fark olmayacaktır. İkinci yöntem seçildiğinde genellikle, “zorlama unsuru içermeyen karışma” yalnızca ve yine (üçüncü bir terime ihtiyaç duyulmaksızın) “karışma” terimi ile ifade edilmektedir. Ortaya çıkan karışıklığın nedeni de budur. En azından eldeki çalışmada terminolojik sarahatin sağlanması açısından, ikinci yöntemdeki küme ilişkisini tasdik ile “karışma” kavramını, “zorlama unsuru içermeyen karışma” anlamında kullanmayı tercih ediyorum.

Müdahale etmeme ilkesinin mutlak görünüşüne rağmen, müdahale eyleminin belirli durumlarda uluslararası hukuka uygun sayılabileceği görüşü gerek uygulamada gerek öğretide kabul görmeye başlamıştır. Devletler, ilkeden ayrılmanın doğuracağı olası istikrarsızlıklardan kaçınmak adına ilkenin mutlak niteliğini muhafaza etmiş olsalar da özellikle insani kaygıların çok yükseldiği durumlarda gerçekleşecek bir müdahalenin ahlakiliği de göz ardı edilemeyecektir.²⁷³ Keskin, literatürde müdahalenin hukuka uygun hale geldiği ileri sürülen durumları “*yurt dışındaki vatandaşlarını korumak amacıyla karışma, devlet kendi ülkesinde vatandaşlarının temel insan haklarını çiğniyorsa bu devlete karışma, meşru savunma hakkının kullanılması bir ölçüde karışmayı gerektiriyorsa meşru savunma çerçevesinde karışma, self-determinasyon hakkını kullanan bir halka yardım için karışma ve bir antlaşmaya dayanarak ya da ilgili devletin çağrısı üzerine karışma*” şeklinde saymıştır.²⁷⁴ Gerçekten de bilhassa BM Güvenlik Konseyi sisteminin işlerliğinin sorgulandığı şartlarda, bir devlet ülkesinde insan haklarına yönelik ağır ihlaller gerçekleştiğinde, uluslararası topluluğun buna göz yummasının çoğu zaman ağır sonuçlar doğurduğu görülmüştür.²⁷⁵ Mahiyet ve kapsamına dair tartışmaların devam ettiği ve henüz üzerinde kesin mutabakat sağlanan bir uluslararası hukuk normuna

²⁷³ Vaughan Lowe, “The Principle of Non-intervention: Use of Force”, Vaughan Lowe ve Colin Warbrick (Ed.), **The United Nations and the Principles of International Law: Essays in Memory of Michael Akehurst** içinde (66-84), London, New York: Routledge, 1994, ss.79-80.

²⁷⁴ Keskin, s.107.

²⁷⁵ Özellikle 1990’lı yıllarda Somali, Ruanda, Srebrenitsa ve Haiti’de yaşanan tecrübeler, ilgili durumun en bilinen örnekleridir.

dönüşmemiş “insani müdahale (*humanitarian intervention*)” ve onun geliştirilmiş modeli “koruma sorumluluğu (*responsibility to protect*)” konseptleri, söz konusu sürecin ürünleri olarak ortaya çıkmıştır.²⁷⁶ Uluslararası hukukta insan hakları ve devlet egemenliği arasındaki menfaatler dengesini sağlama çabaları, bu bağlam içerisinde de devam etmektedir.

Müdahale etmeme ilkesine eldeki çalışmanın konusu açısından yaklaşıldığında; 21. yüzyılın başından itibaren küreselleşmenin birincil enstrümanı haline gelmiş olan başta internet olmak üzere bütün siber uzay bileşenlerinin, devletlerin bu bağlamdaki münhasır yetki alanlarının ve müdahale eşiklerinin tespitini zorlaştırdığı söylenebilir. Bazı devletlerce ileri sürülen “siber egemenlik” konseptleri temelde yine bu ilkeye dayalı kaygılar üzerine inşa edilmiş; ayrıca siber uzayda gerçekleşen birçok faaliyetin de ilkeyi ihlal ettiği görüşü savunulmuştur. Söz konusu hususlar, çalışmanın ilerleyen bölümlerinde ayrı ayrı ele alınacaktır.

5. Doğal Kaynaklar Üzerinde Sürekli Egemenlik İlkesi

Dekolonizasyon sürecinde eski sömürgecilerin, bağımsızlıklarını kazanan ülkelerde sömürge düzenini fiilen devam ettirebilmek maksatlı ekonomik düzenler inşa ettikleri görülmüştür.²⁷⁷ Sömürge durumundayken bağımsızlık kazanan devletlerin bu duruma çözüm bulmak için başlattığı girişimler sonucunda, “ekonomik self determinasyon hakkı” şeklinde adlandırılabilir “doğal kaynaklar üzerinde sürekli egemenlik ilkesi” uluslararası hukukta kabul görmüştür.²⁷⁸ Bu ilke self determinasyon hakkının doğal bir sonucu ve “*ekonomik içerikli egemenlik hakkının özel bir ilke olarak kabulü*” şeklinde de yorumlanmıştır.²⁷⁹ İlkeyi konu alan veya içeren çok sayıda antlaşma ve uluslararası örgüt kararı bulunmakla birlikte, 1962 tarihinde kabul edilen “Doğal Kaynaklar Üzerinde Daimi Egemenlik” başlıklı BM Genel Kurulu kararı, ilkenin muhtevasını tespit açısından özel önem taşımaktadır. Kararda özetle doğal kaynaklar

²⁷⁶ Detaylı bilgi için bkz. Gareth Evans, “From Humanitarian Intervention to the Responsibility to Protect”, **Wisconsin International Law Journal**, Vol.24, Iss.3, (2006), s.706; Birsan Erdoğan, **Humanitarian Intervention and the Responsibility to Protect: Turkish Foreign Policy Discourse**, Palgrave Macmillan, 2017; Ümmühan Elçin Ertuğrul, “Koruma Sorumluluğu: İnsani Müdahaleyi Makyajlamak”, **Gazi Üniversitesi Hukuk Fakültesi Dergisi**, Cilt.20, Sayı.2, (2016), s.441 vd.

²⁷⁷ Yücel, s.98.

²⁷⁸ Ibid.

²⁷⁹ Pazarcı, s.151.

üzerinde sürekli egemenliğin, ilgili devlet halkının refahı yararına kullanılması; kaynakların kullanımı için gerekli olan yabancı yatırımın, ilgili halkın ihdas ettiği normlara uygun şekilde gerçekleşmesi; elde edilen kârın, yatırımcı ve ilgili devlet arasında, devletin egemenliğine hanel getirmeyecek şekilde yapılacak anlaşmaya uygun şekilde dağıtılması; millileştirme ve kamulaştırma gibi faaliyetlerin, kamu yararı ve tazminat esasları gözetilerek gerçekleştirilmesi gibi hususlar düzenlenmiştir.²⁸⁰

Doğal kaynaklar üzerinde sürekli egemenlik, sömürge durumundan kurtulmuş devletler için öngörülmüş olmasına karşın günümüzde dahi bütün devletler için esaslı bir menfaatin ifadesidir. Geleneksel kaynaklar açısından uluslararası hukuk sistemi nispeten denge konumunu bulmuş sayılsa da mevcut durumda siber uzayın aktif kullanımı, ekonomik menfaat elde edilen kaynakları da çeşitlendirmiştir. Başta veri olmak üzere siber uzaya ilişkin ekonomik karşılığı olan bazı hususlar ve devletlerin iktisadi egemenlikleriyle yabancı yatırımların karşılaştığı haller ele alınırken bu ilke de göz ardı edilmemelidir.

D. Devlet Egemenliğinin Unsurları ve Konuları

1. Devletin Hak ve Vazifeleri Teorisi

Modern dönemin başlarında doğal hukuk düşüncesinin bir ürünü olarak devletin asli haklarının varlığına ilişkin teoriler gündeme gelmiştir. BM'nin kuruluşu sonrası süreçteki yerli literatürün ilk temsilcilerinden *Alsan*, teorinin temelini “*fertler nasıl insan ve vatandaş sıfatıyla birtakım hakları haiz bulunuyorlarsa, devletlerin de sırf devlet olmak sıfatıyla hakları vardır*” şeklinde ifade ederek; içinde bulunduğu dönemde tabii ve rasyonel hukuk düşüncesine yakın olan Fransız ekolünce bu fikrin kabul gördüğünü, iradeci yaklaşıma sahip Alman ve İtalyan ekolünün ise muhalif pozisyonda olduğunu aktarmıştır.²⁸¹ *Alsan*'dan yirmi yıl sonra *Meray*, “klasik devletler hukuku yazarları” olarak adlandırdığı ekolün, devletlere ait asli hak ve vazifelerin varlığında mutabık olmakla birlikte hakların tespiti konusunda uzlaşmadığını ifade etmiştir.²⁸² Bahsi geçen

²⁸⁰ UN/General Assembly, Permanent Sovereignty over Natural Resources, A/RES/1803(XVII), 14.12.1962, ss.15-16.

²⁸¹ Zeki Mesud Alsan, **Devletler Hukuku Dersleri**, Ankara: T.C. Millî Eğitim Bakanlığı Siyasal Bilgiler Okulu Yayınları, 1947, s.172.

²⁸² Meray, s.313.

iki yerli yazar da söz konusu hakları “egemenlik veya bağımsızlık hakkı”, “varlığını koruma ve gelişme hakkı”, “eşitlik hakkı”, “ticaret hakkı” ve “karşılıklı saygı hakkı” şeklinde saymışlardır.²⁸³ Günümüz uluslararası hukuk eserlerinde ise genel olarak bu teoriye yer verilmediği görülmektedir. Zira uluslararası hukukta süljelerin hak ve vazifelerinin normatif yaklaşımla dinamik olarak tespiti/değişimi kabul görmüştür.

Amerika Kıtası’ndaki 16 devlet tarafından 1933’te akdedilen “Devletlerin Hak ve Vazifelerine İlişkin Montevideo Sözleşmesi”, devletler için “siyasî varlığını koruma ve sürdürme”, “toprak bütünlüğü”, “bağımsızlık”, “meşru müdafaa”, “eşitlik” gibi hakların yanı sıra; “diğer devletlerin haklarına saygı ve riayet”, “kuvvet kullanımı ile elde edilen toprak kazanımlarının ve diğer menfaatlerin tanınmaması”, “milletlerarası uyuşmazlıkların barışçıl yollarla çözümü” gibi vazifeler öngörmüştür.²⁸⁴ Sözleşme, 1948’de Amerikan Devletler Örgütü’nün kurulmasına da zemin hazırlamıştır. Ne var ki bu gelişmelerin ancak bölgesel nitelikte olduğu kabul edilebilecektir.

BM’nin kuruluşundan sonra Genel Kurul kararıyla faaliyete geçen Uluslararası Hukuk Komisyonu’nun (*International Law Commission*) ele aldığı öncelikli konulardan biri devletlerin hak ve vazifelerinin tespiti olmuştur.²⁸⁵ Bu bağlamda oluşturulan Devletlerin Hak ve Vazifeleri Hakkında Taslak Bildirge (*Draft Declaration on Rights and Duties of States*)²⁸⁶, Genel Kurul tarafından üye devletlere iletilerek kanaat ve tavsiyeleri istenmiş fakat çok az sayıda üye devletten geri dönüş alındığı için yine bir Genel Kurul kararıyla üyelerin çoğunluğu bildirimde bulunana kadar metin hakkındaki müzakereler ertelenmiştir.²⁸⁷ Gelgelelim taslakta düzenlenen hak ve vazifelerin, genel uluslararası hukuk açısından çok dar kapsamda kaldığı ve yeterli katılımdan uzak olduğu açıktır. Diğer yandan *Kelsen*’in de metindeki birçok maddeyi gereksiz ve yetersiz olduğu yönünde eleştirdiği görülmektedir.²⁸⁸

²⁸³ Ibid.; Alsan, s.173;

²⁸⁴ Mahmut R. Belik, “Devletlerin Hak ve Vazifeleri Üzerinde Beyanname Projesi”, **İstanbul Hukuk Mecmuası**, Cilt.18, Sayı.1-2, (1952), s.60.

²⁸⁵ Ibid.

²⁸⁶ UN/General Assembly, Draft Declaration on Rights and Duties of States, **A/RES/596(VI)**, 05.02.1952.

²⁸⁷ A/RES/596(VI), s.83-84.

²⁸⁸ Hans Kelsen, “The Draft Declaration on Rights and Duties of States: Critical Remarks”, **The American Journal of International Law**, Vol.44, No.2, (1950), s.259-276.

Sonuç olarak devletlerin hak ve vazifelerine ilişkin yaklaşımın, küresel mutabakata dayalı uluslararası hukuk normu oluşturma projesini başarıya ulaştıramadığı görülmektedir. Modern dönemde uluslararası topluluğun, devletler için doğal hukuk tandanslı hak ve vazife teorisini kemale erdirmek yerine, pozitif hukukta devletlere tanınan hak ve vazifelerin işletilmesini tercih ettiği söylenebilecektir. Bu tercihin günümüze başlıca yansıması, “hak ve vazife” yerine “yetki ve yükümlülük/sorumluluk” konseptinin kabulü olmuştur.

2. Egemenlik ve Yetki İlişkisi

Hukuk disiplini içerisinde ele alındığında “yetki”, bir hukuk düzenindeki sùjelerin sahip olduđu, iradi şekilde hukuki durum kurabilme iktidarı olarak tanımlanabilir.²⁸⁹ Hukuki işlemler meşruiyetini, failinin sùjesi olduđu hukuk sisteminden alır. Uluslararası hukukun asli sùjesi olan devletlerin yetkileri de dolayısıyla uluslararası hukuk tarafından belirlenir. Bu belirleme, uluslararası hukukun iradi yapısı gereği yine bizzat devletlerin eseridir. Böylece uluslararası hukukta devletin yetkisi, devlet egemenliğinden kaynaklı meşruiyete sahip bir iktidarı ifade etmektedir.²⁹⁰

Brownlie, egemenlik (*sovereignty*) ve yetki (*jurisdiction*) kavramlarının, devletlerin hakları, vazifeleri, güçleri, özgürlükleri ve dokunulmazlıkları gibi çok çeşitli hususlar için serbestçe kullanıldığına dikkat çekmiş ve ortaya çıkan karışıklığın üzerine gitmiştir.²⁹¹ Yazara göre egemenlik, en kısa ifadeyle, devletin hukuk kişiliğinin ve devlet olma durumunun hukuki kısaltmasıdır; yetki ise meselenin hak yahut iddialar, serbestiler ve kabiliyetler gibi belirli yönlerini ifade etmektedir.²⁹² Ayrıca bir devletin kendi ülkesinin bir bölümünde başka bir ülkeye münhasır yetkiler tanınmasının mümkün olduğunu örnek vererek; böyle bir ihtimalde şayet yetki rıza dahilinde verilmişse, yetki

²⁸⁹ Pazarcı, s.152.

²⁹⁰ İngilizce literatürde bu iktidar “*jurisdiction*” kavramıyla karşılanmaktadır. Köken itibarıyla “hukuk” anlamındaki “*juris*” ve “söylemek” anlamındaki “*diction (dicere)*” ifadelerinin birleşiminden oluşmasından anlaşılacağı üzere kastedilen iktidar, temelde hukuk vazetme ve uygulama iktidarıdır; Jurisdiction, Merriam Webster Dictionary, Word History, <https://www.merriam-webster.com/dictionary/jurisdiction#word-history> (31.12.2024).

²⁹¹ Brownlie, s.106.

²⁹² Ibid.

veren devletin o bölge üzerinde egemenliğine halel gelmeyeceğini belirtip iki kavram arasındaki farkı açıklamıştır.²⁹³

Shaw, hukuki ilişkileri ve yükümlülükleri kurma, değiştirme veya sonlandırmayı mümkün kılan bir otorite kullanımı şeklinde ele aldığı yetkiyi, devlet egemenliğinin esaslı bir özelliği olarak kabul etmiştir. Yazara göre yetkinin kullanımı yasama, yürütme ve yargı faaliyetleriyle gerçekleşir.²⁹⁴

Staker, İngilizce monografilerde geleneksel olarak yetki için ayrı bir başlık açıldığını; Kıta Avrupası yazarlarının ise konuyu egemenliğe ve bilhassa ülkesel egemenliğe dair başlıklar altında işlediklerini fakat zamanla ayrı başlıkta ele almanın yaygınlaşmaya başladığını ve hatta gidişatın devletlerin -sınır aşan durumlar da dahil olmak üzere- yetki taleplerinin büyük artış göstereceği bir döneme doğru ilerlediğini belirtmiştir.²⁹⁵ Bu tespitlerin egemenlik, uluslararası hukuk ve yetki arasındaki bağıllık ilişkisinin önemli bir yansıması olarak yorumlanması mümkündür.

Yukarıda aktarılan görüşler ve değerlendirmeler sonucunda, uluslararası hukukta devletin yetkisinin; özünde devlet egemenliği kaynaklı, pozitif hukuk tekniği açısından ise meşruiyetini uluslararası hukuk normlarından alan bir iktidar olduğu söylenebilecektir. Devlet yetkisini diğer tüzel kişilerin veya gerçek kişilerin ulusal hukuklardaki yetkilerinden ayıran temel fark da bu özelliğinden ileri gelmektedir. Sonuç olarak devlet egemenliğinin “unsurları”, yetkiye ilişkin ayrımların ele alınmasıyla hukuk sahasında gözlemlenebilecektir; egemenliğin “konuları” ise devletin üzerinde yetki -ve dolayısıyla iktidar- sahibi olduğu olguları ifade edecektir.

3. Yetkiye İlişkin Ayrımlar

Uluslararası hukuka göre egemen olduğu kabul edilen devletin, egemenlik vasfından kaynaklanan ve yine uluslararası hukuk tarafından tayin edilen yetkilerinden bahsedilmiştir. Gelineen noktada iki temel soru ortaya çıkmaktadır. Bunlardan birincisi, “devletin egemenlikten doğan yetkileri nelerdir ve nasıl kullanılır”; ikincisi de “bu

²⁹³ Ibid.

²⁹⁴ Shaw, s.461.

²⁹⁵ Christopher Staker, “Jurisdiction”, Malcolm D. Evans (Ed.), **International Law** içinde (309-335), Fourth Edition, New York: Oxford University Press, 2014, s.311.

yetkiler, neler veya kimler üzerinde kullanılır” sorularıdır. Bu soruların cevapları aynı zamanda sırasıyla devlet egemenliğinin unsurlarını ve konularını açıklayacaktır. İlgili soruları cevaplamak için literatürde çeşitli tasnif metotları bulunmaktadır. Eldeki çalışmada, siber uzay gibi üzerinde egemenlik iddia edilmesi söz konusu olan yeni bir olgu için bu iddianın imkânının ve şayet mümkünse sonuçlarının ele alınması adına başvuru zemini teşkil edecek bir metot ile yetkiye dair hususların analiz edilmesi amaçlanmıştır.

a. Düzenleme Yetkisi, İcra Yetkisi ve Yargı Yetkisi

Devletin bir siyasal iktidar tipi olarak en temel iki fonksiyonu, kural koymak ve uygulamaktır. Yasama, yürütme ve yargı şeklinde klasikleşmiş olarak yapılagelen güç ayrımı, bu fonksiyonların kullanımını temel almaktadır. Devletin düzenleme yapma yetkisi (*prescriptive jurisdiction*), nerede olurlarsa olsun kişiler ve durumlar hakkında hukuk vazetme iktidarını ifade etmektedir. Mevcut normların, yürütme ve yargı erklerinin kullanımıyla kişiler ve diğer olgular üzerinde uygulanması ise devletin icra yetkisinin (*enforcement jurisdiction*) sonucudur.²⁹⁶ Bunun yanı sıra yargı yetkisini (*adjudicative jurisdiction*) icra yetkisinden ayırarak yargılama ve hüküm icrasını ayrı ayrı değerlendirmek de mümkündür.²⁹⁷ Nitekim yargı marifetiyle norm uygulamanın dışında, devletin ülkesinde kararlar alıp eyleme geçme kapasitesi de icra yetkisi ile ilişkilidir.²⁹⁸

Devletler, sınır tanımaksızın her konuda düzenleme yapabilirler. Bu bakımdan düzenleme yetkisinin genel bir yetki olduğu söylenebilir. Fakat yapılan düzenlemelerin icra edilmesi, uluslararası hukukta devlete tanınan sınırlar içerisinde mümkün olacaktır.²⁹⁹ Diğer taraftan devletin bir “konu” üzerinde yargı yetkisine sahip olması, yargılama sonucunda elde edilen her hükmün (“yer” bakımından icra yetkisinin bulunmadığı bir durum olarak) ülke dışında da icra edilebileceği anlamına da gelmeyecektir. Dolayısıyla yetki analizinde asıl olan yargı ve icra yetkisinin incelenmesidir. Başta mahkemeler ve kolluk kuvvetleri olmak üzere ilgili devlet

²⁹⁶ Donald R. Rothwell ve Diğerleri, **International Law: Cases and Materials with Australian Perspectives**, Third Edition, Cambridge: Cambridge University Press, 2018, s.321.

²⁹⁷ Cedric Ryngaert, **Jurisdiction in International Law**, Second Edition, Oxford: Oxford University Press, 2015, ss.9-10.

²⁹⁸ Michael Akehurst, “Jurisdiction in International Law”, **British Year Book of International Law**, Vol.46, (1972-1973), s.146.

²⁹⁹ Martin Dixon, **Textbook of International Law**, Seventh Edition, Oxford: Oxford University Press, 2013, s.149.

organlarınca kullanılan bu yetkilerin sınırları hem hukuki ve cezai bakımdan hem yer ve kişi bakımından ayrı ayrı değerlendirmeye tabi tutulmalıdır.

b. Hukuki Yetki ve Cezai Yetki

Uluslararası hukuk literatürü, devletin icra yetkisi söz konusu olduğunda genel olarak cezai yargı yetkisine odaklanmaktadır.³⁰⁰ Bazı yazarlar, hukuk yargılamaları konusunda devletlerin daha esnek davranmaları ve yetki kullanan devletlere genel olarak olumsuz tepki göstermemeleri sebebiyle uluslararası hukukta kabul görmüş belli bir sınırlama olmadığı yönünde kanaat bildirmişlerdir.³⁰¹ Diğer taraftan *Brownlie*, hukuk yargılamalarının da nihayetinde cezai yaptırımların da dahil olduğu cebri süreçlerle takviye edildiği için hukuki ve cezai yargı yetkilerinin ileri sürülmesinden kaynaklı sorunlar arasında prensipte pek bir fark olmadığını ileri sürmüştür.³⁰² *Wallace ve Ortega* ise yabancılık unsuru bulunan hukuk yargılamasının -ceza hukuku yaptırımlarıyla desteklense dahi- milletlerarası özel hukuk konusu olup kanunlar ihtilafı hükümlerince çözümlenmesine istinaden konuyu uluslararası kamu hukuku bağlamında değerlendirmenin isabetli olmayacağını belirtmiştir.³⁰³ *Hillier* tarafından da desteklenen bu görüşe göre, uluslararası kamu hukukunda devletin yetkisine dair esas problemler cezai yargı yetkisi üzerinden ortaya çıkmıştır.³⁰⁴

Mevcut durumda, özel hukuk işlemlerinde gerçek kişi ve tüzel kişi taraflar sözleşme serbestisiyle herhangi bir devlet mahkemesi için yetkilendirmede bulunabilmektedir. Cezai konular ise devletlerin doğrudan kamu gücüyle ilgili olduğu için yetkiye dair uluslararası hukuk ilkeleri üzerinden çözümlenmektedir. Bununla birlikte devletlerin ülkelerinde hukuki normlar belirlediği ve bu normlara uymayanlara yönelik cezai yaptırımların yanı sıra norma aykırı mal, hizmet veya işlemler için cebren engelleme, durdurma, toplatma, imha etme gibi çeşitli hukuki icra işlemlerine başvurabildiği de yaygın olarak görülmektedir. Ayrıca Türkiye’de 6100 sayılı Hukuk Muhakemeleri Kanunu’nda bulunan disiplin hapsi ve disiplin para cezası gibi hükümler

³⁰⁰ Valerie Epps, *International Law*, Fifth Edition, Durham: Carolina Academic Press, 2014, s.107.

³⁰¹ Shaw, s.488; Akehurst, s.170; Tim Hillier, *Principles of Public International Law*, Second Edition, London, Sydney: Cavendish Publishing Limited, 1999, s.127; Derek William Bowett, “Jurisdiction: Changing Patterns of Authority over Activities and Resources”, *British Yearbook of International Law*, Vol.53, Iss.1, (1982), s.4.

³⁰² Brownlie, s.300.

³⁰³ Rebecca M.M. Wallace ve Olga Martin-Ortega, *International Law*, Eighth Edition, Sweet & Maxwell, 2016, s.125

³⁰⁴ Hillier, s.127.

de hukuk yargılamasının özünde cezai nitelikteki yaptırımlarla desteklenmesine verilebilecek örneklerdendir.³⁰⁵

c. Ülkesel Yetki ve Kişisel Yetki

Devletin, en meşhur tanımıyla “ülke”, “insan topluluğu” ve “etkin siyasal otorite” olmak üzere üç unsurdan oluştuğu kabul görmüştür. Devletin yetkisinin özü, siyasal otoritenin ülke ve insan üzerinde sahip olduğu iktidardır. Ülke ve insan kavramları yetki bakımından, “yer yönünden (*ratione loci*)” ve “kişi yönünden (*ratione personae*)” yetki ayrımının da ana konusunu teşkil etmektedir. Devlet, temelde ülkesi ve vatandaşları üzerinde yargı ve icra yetkisine sahip olmakla birlikte bu yetkilerin istisnai olarak genişlediği ya da kısıtlandığı durumlarla da karşılaşmaktadır. Aynı zamanda devlet egemenliğine nelerin konu olabileceğini de ifade eden bu yetki sınırları, birtakım ilkeler üzerinden belirlenmektedir.

Devlet ve ülkesi arasında kopması mümkün olmayan bir bağ vardır. Öyle ki ülke, bir devletin varlığının kurucu şartıdır. Bu ilişkinin diğer istikametinden bir sonuç olarak da devletin esas egemenlik ve yetki alanı yine kendi ülkesidir. Egemen devletin, ülkesi üzerinde en üstün buyurma gücüne sahip olduğu kabulü; müdahale etmeme ilkesini ve devletin iç yetki (*domestic jurisdiction*) prensibini doğurmuştur.³⁰⁶ Palmas Adası Tahkimi’nde hakem *Huber*, ülkesel egemenliği; başka herhangi bir devlet hariç tutularak, dünyanın bir kısmında bir devletin “işlevlerini yerine getirme hakkı” olarak görmüştür.³⁰⁷ Dünyanın bir kısmı ifadesinden “belirli bir toprak kütlesi, bu toprağın altı, toprak üzerindeki su alanları, eğer denize kıyısı varsa belirli bir açıklığa kadar karasuları³⁰⁸ ve

³⁰⁵ Osman Çakar, “Hukuk Muhakemeleri Kanundaki Ceza Muhakemesi Hükümleri Özelinde Disiplin Hapsi”, **Türkiye Adalet Akademisi Dergisi**, Yıl.8, Sayı.32, (2017), ss.412-413.

³⁰⁶ Shaw, s.485.

³⁰⁷ UN, Reports of the International Arbitral Awards, Island of Palmas Case (Netherlands, USA), Vol.II, 04.04.1928, s.838, https://legal.un.org/riaa/cases/vol_II/829-871.pdf (31.12.2024).

³⁰⁸ Birleşmiş Milletler Deniz Hukuku Sözleşmesi (BMDHS) m.3 hükmüne göre 12 deniz miline kadar.

ilgili toprak ve deniz alanının üzerindeki hava sahası” anlaşılmaktadır.³⁰⁹ Bu unsurların “kara ülkesi”, “deniz ülkesi” ve “hava ülkesi” olarak da formüle edilmesi mümkündür.³¹⁰

Uluslararası Daimî Adalet Divanı’nın Bozkurt-Lotus Kararı’nda benimsediği, engelleyen bir hüküm yoksa devletin yetki kullanabileceğini öngören yaklaşım³¹¹ zamanla eleştiriye uğramış ve yetkide varlığın değil yokluğun esas olduğu, devlet için yetki tanıyan bir hüküm varsa devletin yetki sahibi olacağı yaklaşımı kabul görmüştür.³¹² Bu hükümler ise temelde belli başlı ilkelere dayanmaktadır.

Devletin, ülkesinde yaşayan insanlar, gerçekleşen eylemler ve bulunan ögeler üzerinde yetki sahibi olması, “ülkesellik ilkesi (*territorial principle*)” olarak adlandırılmaktadır.³¹³ Bu ilke aynı zamanda, aksine hüküm olmadıkça yetkinin ülke dışında kullanılamayacağını da belirtmektedir.³¹⁴ Özellikle suç teşkil eden fiiller söz konusu olduğunda, bir devletin ülkesinde etki doğuran fakat ülke dışında gerçekleşen bir fiil için ilgili devlete yetki tanınması ise “objektif ülkesellik ilkesi” bağlamında mümkün görülmüştür; böyle bir fiilin işlendiği ülkeye hâkim olan devlet de “sübjektif ülkesellik ilkesi” gereği yine yargı yetkisine sahip kabul edilecektir.³¹⁵

³⁰⁹ Wallace ve Ortega, s.103.

³¹⁰ Sevin Toluner, **Milletlerarası Hukuk Dersleri: Devletin Yetkisi**, 4. Bası, İstanbul: Beta Basım Yayım Dağıtım, 1989, s.31. Devletin üzerinde egemenlik kurduğu alan İngilizce literatürde “*territory*” kelimesiyle karşılanmaktadır. *Territory*, “*terra*” kökü itibarıyla toprağı ifade etse de egemenliğe konu olmuş deniz ve hava sahalarını da karşılamaktadır. Uluslararası Sivil Havacılık Sözleşmesi m.2 hükmünde, Türkçe’ye “ülke” olarak çevrilen “*territory*” başlığıyla yapılan tanımda; kavramın, sözleşmenin amacı itibarıyla, egemenliğe konu kara alanları (*land areas*) ve bitişindeki karasuları (*territorial waters*) olarak kabul edildiği belirtilmiştir. Sözleşmede ayrıca her bir devletin ülkesi (*territory*) üstünde (*above*) bulunan hava sahası (*airspace*) üzerinde münhasır egemenliğe sahip olduğu düzenlenmiştir. Türkçe’de kullanılan “ülke”, esasen söz konusu kavramın egemenlik ihtiva eden özü itibarıyla “*territory*” kelimesine göre daha tutarlı sonuçlar ortaya koymaktadır. Tek başına “toprak”, devlet egemenliği açısından bir anlam ifade etmezken; üzerinde egemenlik kurulduğunda “kara ülkesi” haline gelecektir. Aynı durum deniz alanları ve hava sahası için de söz konusudur. Dolayısıyla “ülke” genel anlamıyla devletin üzerinde egemenlik haklarına sahip olduğu bütün mekanların toplamını karşılarken; “kara ülkesi”, “deniz ülkesi” ve “hava ülkesi” ifadeleri de ilgili mekanlar için özelleşmiş nitelikte karşılıklar taşımaktadır. Bu bakımdan Türkçe literatürün, İngilizce’deki “*land*”, “*territorial waters*” ve “*airspace*” kavram setine göre konuya ve amaca daha uygun bir sistem önerdiğini söylemek mümkündür.

³¹¹ The Case of the S.S. “*Lotus*”, **Judgment**, PCIJ, Series A, No. 10, 1927, ss.18-20; İkiisi de ticaret gemisi olan Türk bandıralı “Bozkurt” ile Fransız bandıralı “Lotus” arasında açık denizde yaşanan çatma vakası, Bozkurt gemisinde görevli olan sekiz Türk vatandaşının ölümüyle sonuçlanmıştır. Devamında Türk mahkemelerinin Lotus gemisinin Fransız kaptanını yargılamasına karşı Fransa’nın itirazıyla uyumsuzluk, Uluslararası Daimî Adalet Divanı’na intikal ettirilmiştir. Fransa’nın itirazının temel gerekçesi, açık denizdeki gemiler üzerinde bayrak devletinin münhasıran yetkili olduğu ve Türkiye’nin Fransız gemisindeki Fransız kaptanı yargılama yetkisini dayandırabileceği bir uluslararası hukuk hükmünün bulunmadığı yönündedir. Divan, -diğer gerekçelerle birlikte- uluslararası hukukta devletin yetkisini sınırlandıran açık bir hüküm bulunmadığı sürece devletin yetkili kabul edileceği gerekçesiyle Türkiye’nin yargılama talebini haklı bulmuştur.

³¹² Shaw, s.491.

³¹³ Staker, s.316.

³¹⁴ Toluner, s.2.

³¹⁵ Staker, s.317; Dixon, s.152.

Devletin kiři bakımından yetkisi (*pesonal jurisdiction*), en bařta vatandařlarını kapsamaktadır. Ülkesellik ilkesine dayanarak ülkelerinde bulunan bütün uyruklar için özellikle cezai yetki sahibi olan devletlerin, “vatandaşlık ilkesi (*nationality principle*)”³¹⁶ geređi, ülke dıřında dahi olsalar uyrukları üzerinde yetki sahibi oldukları kabul edilmiřtir. Bu ilke, bir devletin ülkesi dıřında gerekleřen ve vatandařını mađdur eden suç fiilleri için ilgili devlete yetki tanıyan “pasif vatandaşlık ilkesi”³¹⁷ (*passive personality/nationality principle*)³¹⁸ ile karřı istikametten de desteklenmiřtir.

Devletin yetki kullanımında ülkesellik ilkesi, kiři bakımından kapsamı vatandaşlıđın ötesine genişletme imkânı sunarken; kiřiliđe ilişkin ilkelerin de yer bakımından kapsamı ülke dıřına genişletme imkânı sunduđu görölmektedir. Bunun yanı sıra devletlere, sınırları ötesindeki fiiller için uyrukluk fark etmeksizin yargı yetkisi tanıyan ilkeler de bulunmaktadır. Devletler, ülkeleri dıřında gerekleřmesine ve vatandaşlık bađı olmayan kiřiler tarafından işlenmesine rađmen güvenliklerine zarar veren fiiller üzerinde “koruma ilkesi (*protective principle*)” geređi cezai yargı yetkisine sahiptir. Bununla birlikte güvenlik ve hayati menfaat gibi kavramların nispi ve tartıřmaya açık karakterlerinin, bu ilkenin istismar edilmesine kapı açabileceđine yönelik görüřler de bildirilmiřtir.³¹⁹ Ülke ve uyrukluk ařan cezai yetkinin dayanaklarından birinin de “evrensellik ilkesi (*universality principle*)” olduđu kabul edilmiřtir. Bu ilke, uluslararası hukuka aykırılıđı üzerinde mutabakat bulunan ve doğrudan uluslararası topluluđu etkileyen az sayıda suç tipi için öngörölmüřtür. Halihazırda deniz haydutluđu suçu ve savař suçları bu kapsamda deđerlendirilmektedir.³²⁰

Yer ve kiři bakımından yetkiye iliřkin bahsi geen ilkelere, eldeki alıřmanın devamında yeri geldike deđerinilip; detaylar ve tartıřmalı hususlar, konuyla ilgili olduđu ölçüde ayrıca ele alınacaktır.

³¹⁶ Wallace ve Ortega, ss.129-130; Dixon, ss.153-154; Shaw, ss.493-497; Staker, ss.318-321, Hillier, ss.132-133.

³¹⁷ İlkenin ceza hukukunda “mađdura göre řahsilik” řeklinde kullanımı da söz konusudur; Aksar, s.308.

³¹⁸ Wallace ve Ortega, s.135; Dixon, s.159; Shaw, ss.497-499; Staker, ss.326-327; Hillier, ss.133-135.

³¹⁹ Wallace ve Ortega, s.130; Dixon, ss.156-158; Shaw, s.499; Staker, s.321; Hillier, ss.129-130.

³²⁰ Wallace ve Ortega, ss.129-133; Dixon, ss.154-156; Shaw, ss.500-503; Staker, ss.322-323; Hillier, ss.135-137.

d. Ortak ve Mütedahil Yetkiler

Uluslararası hukuk, devletlere milli yetki alanı dışında kalan bazı hususlarda ortak yetki kullanımı imkânı tanımıştır. Bu bakımdan en bilinen örnek açık denizlerdir. Açık denizler seyrüsefer, canlı kaynaklardan yararlanma, boru, kablo vb. altyapı elemanları döşeme gibi konularda -barışçıl amaçlar için kullanmak kaydıyla- bütün devletlerin kullanımına açıktır.³²¹ Benzer durum açık deniz üstündeki hava sahasında seyrüsefer ve uzaydan yararlanma bakımından da geçerlidir.³²²

Ülkesel ve kişisel yetkiye ilişkin kabul görmüş ilkeler, bir fiil ve fail üzerinde birden fazla devletin yargı yetkisi ileri sürebilmesine de olanak tanımaktadır. Böylece “mütedahil yargı yetkisi (*concurrent jurisdiction*)” ortaya çıkmaktadır.³²³ Çifte yargılama (*double jeopardy*) olarak da adlandırılan durum, Roma Hukuku’ndaki “*non bis in idem*” ilkesiyle paralel şekilde ele alınmış ve bir devletin yargıladığı suçu başka bir devletin ayrıca yargılayamayacağı kabul edilmiştir.³²⁴ Tabii ki bu kabul, bir kayırma sonucunda suçun cezasız kalması ya da başka sebeplerle etkin bir yargılamanın gerçekleşmemiş olması gibi sonuçlara da mahal vermemelidir.³²⁵

4. Devletin Yetkisinin İstisnaları ve Egemenliğe Tabi Olmayan Alanlar

a. Egemenlik Alanında İrade Beyanına Dayalı veya Ülkesel Kısıtlamalar

Devletler, uluslararası hukuku belirlerken egemenlik alanlarındaki bazı konularda kendi yetkilerini kısıtlamış veya bazı fiilleri yasaklamışlardır. Bunlar, başka bir devlete kendi ülkesinde geçiş hakkı vermek, askeri üs bulundurmasına izin vermek, kapitülasyon tanımak gibi³²⁶ irade beyanına dayanabileceği gibi genel uluslararası hukuk kuralları ile de ortaya çıkabilir. Örneğin bir devletin kendi ülkesindeki belirli bir gruba yönelik soykırımda bulunması, ülkesi ve vatandaşları üzerinde egemen olmasına rağmen kesinlikle meşru kabul edilemeyecektir. Ayrıca devletler, kadim “kendi mülkünü bir

³²¹ Selami Kuran, **Uluslararası Deniz Hukuku**, 6. Baskı, İstanbul: Beta Basım Yayım Dağıtım, 2020, ss.288-289.

³²² Shaw, 405.

³²³ Dixon, s.151.

³²⁴ Mustafa Özen, “Non Bis in Idem (Aynı Fiilden Dolayı İki Kez Yargılama Olmaz) İlkesi, **Gazi Üniversitesi Hukuk Fakültesi Dergisi**, Cilt.14, Sayı.1, (2010), s.405.

³²⁵ Dixon, ss.151-152; Pazarcı, ss.175-176.

³²⁶ Pazarcı, ss.157-162.

başkasına zarar vermeyecek şekilde kullan (*sic utere tuo ut alienum non laedas*)”³²⁷ ilkesi gereği, egemen oldukları ülkede başka devletlere zarar verecek faaliyetlerde bulunamazlar ve ülkelerinde gerçekleşecek bu tür faaliyetlere de engel olma yükümlülüğü altındadırlar.³²⁸ Bir başka örnek de devletlerin egemen eşitliği ve “eşitin eşite üstünlüğü/emretme yetkisi yoktur (*par in parem non habet imperium*)” ilkeleri üzerine inşa edilen; devletlerin, uluslararası örgütlerin, devlet temsilcilerinin, diplomatik temsilcilerin ve konsolosluk temsilcilerinin dokunulmazlık ve yargı bağışıklıklarıdır.³²⁹ Uluslararası hukukun pozitivist yapıda olduğu kabulü üzerinden hareket edildiğinde, devletleri esas bağlayanın söz konusu ilkeler değil; bu ilkelere binaen yine devletlerce kabul edilen uluslararası hukuk normları olduğunu da bu noktada belirtmek gerekir.³³⁰

b. Terra Nullius, Res Communis ve İnsanlığın Ortak Mirası

İnsan ve mekân ilişkisi, insanın ve siyasi yapıların mekâna hükmetme çabası ile şekillenmiştir. Önce insan için bir mücadele sahası olan mülkiyet, siyasi yapıların da varoluşsal zeminini teşkil etmiştir. Ülke, devlet için mülk olarak görülmüş; “mülkîlik” de bu bağlamda hukuk literatürüne kuvvetli şekilde yerleşmiştir. Kara ülkesi, bütün devletler için varlıklarının esaslı unsurudur. Devlet, kara ülkesi olmadan var olamaz; fakat bir kara parçası, ülke haline gelmeden de varlığını sürdürebilir. Kara için geçerli olan bu durum evleviyetle mekâna dair bütün unsurlar için de geçerlidir.³³¹ Bir devletin ülkesi haline gelmemiş mekânsal unsurlar, niteliklerine göre uluslararası hukukça tayin edilmiş rejimlere sahiptir.

Roma Hukuku’ndaki “*res nullius* (sahipsiz şey)”³³² konseptinin devletler için bir uzantısı olarak *terra nullius*, köken itibarıyla “sahipsiz toprak”³³³ anlamına gelse de hukuken, “üzerinde ülkesel egemenlik kurulması mümkün olduğu halde henüz bir

³²⁷ A Dictionary of Law, “sic utere tuo ut alienum non laedas”, Eighth Edition, Oxford: Oxford University Press, 2015, s.577.

³²⁸ Gerald Fitzmaurice, *The General Principles of International Law: Considered from the Standpoint of the Rule of Law*, Leiden: A.W. Sijthoff, 1958, s.188; Erkiner, Uluslararası Terörizm..., 2021, ss.173-175.

³²⁹ Fitzmaurice, ss.187-188.

³³⁰ *Jus cogens* normların iradiliğine dair yukarıda dipnot.257’de bahsedilen durumu burada tekrar hatırlatma fayda görmekteyim.

³³¹ Dünyadaki kara, deniz ve hava unsurlarının yanı sıra dış uzay, gök cisimleri ve tartışmaya fazlasıyla açık olarak sanal mekânsal boyutlar bu kapsamda değerlendirilebilir.

³³² Francis Stephen Ruddy, “Res Nullius and Occupation in Roman and International Law”, *University of Missouri-Kansas City Law Review*, Vol.36, No.2, (1968), s.274.

³³³ Bkz. dipnot.310.

devletin egemenliğine tabi olmayan” mekanları ifade etmektedir.³³⁴ Sömürge dönemi literatüründe Avrupalı olmayan “gayri medeni” toplumların yaşadığı ülkeleri *terra nullius* kabul etme eğilimi ön plana çıkmıştır.³³⁵ UAD’nin 1975’te Batı Sahra hakkında verdiği danışma görüşüyle de ilan edildiği üzere modern dönemde bu yaklaşımdan dönülmüştür.³³⁶ *Terra nullius* alanlar üzerinde bir devletin egemenliğinden bahsedilemese de buralarda genel uluslararası hukukun emredici hükümlerinin geçerliliğini koruduğu göz ardı edilmemelidir.³³⁷

Terra nullius konseptinden farklı olarak *res communis*, bir devletin egemenliği altında olmadığı gibi üzerinde egemenlik iddia edilmesi de mümkün olmayan alanları ifade etmektedir.³³⁸ Roma Hukuku’nun temel eseri *Institutiones*’te *-res communis* ibaresi geçmeksizin- “hava, akarsular, deniz ve dolayısıyla deniz kıyısının” doğal hukuk gereği herkes için ortak olduğu ve zarar vermemek koşuluyla kimsenin bunlara erişiminin yasaklanamayacağı ifade edilmiştir.³³⁹ *Brownlie* de *res communis* özelinde kavramın Roma Hukuku’nda kesin bir içerik kazanamadığını ve zaman zaman *res publicae* ile karıştırıldığını belirtmiştir.³⁴⁰

Uluslararası hukukta *res communis* olduğu en yerleşik şekilde kabul edilen alan açık denizlerdir.³⁴¹ Açık denizlerin üzerindeki hava sahasının statüsünün de bu yönde olduğu çıkarımını yapmak mümkündür. Bunun yanı sıra 1967 tarihli Ay ve Diğer Gök Cisimleri Dâhil, Uzayın Keşif ve Kullanılmasında Devletlerin Faaliyetlerini Yöneten İlkeler Hakkında Antlaşma (*Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and Other Celestial Bodies*) ile uzayın hukuki rejimi de herhangi bir devletin egemenlik iddiasına ve askeri amaçlı kullanımına mahal vermeyecek şekilde düzenlenmiştir.³⁴² Dolayısıyla uzayın da *res*

³³⁴ Hillier, s.110.

³³⁵ Ibid.

³³⁶ Divan burada, sosyal ve siyasal olarak örgütlenmiş kabile yapıları bulunan toprakların *terra nullius* olarak kabul edilemeyeceğini beyan etmiştir; Western Sahara, **Advisory Opinion**, ICJ Reports, 1975, s.39.

³³⁷ Brownlie, s.168.

³³⁸ Hillier, s.110.

³³⁹ J. B. Moyle (Çev.), “The Institutes of Justinian, Fifth Edition, 1913”, Gutenberg, Book II, Title I, para.1, <https://www.gutenberg.org/files/5983/5983-h/5983-h.htm> (31.12.2024).

³⁴⁰ Brownlie, s.169.

³⁴¹ Fitzmaurice, s.156; Hillier, s.110; Shaw, 364; Cassese, s.90.

³⁴² UNTS, Vol.610, No.8843, 1970, s.208.

communis olduğu kabul edilmektedir.³⁴³ Belirtilmelidir ki *res communis* alanlar bütün devletlerin kullanımına açık olmakla birlikte söz konusu ortak kullanım, menfaatlerin de ortaklığı anlamına gelmemektedir.³⁴⁴ Yukarıda değinildiği üzere devletlerin bu alanlarda mütedahil yetkisi söz konusudur ve alanların kullanımı “önce gelen yararlanır” düsturuna dayanmaktadır.³⁴⁵ Bu yararlanma esnasında da uluslararası hukukun genel hükümleri yürürlüğünü korumaktadır.

Uluslararası hukukta görece yeni gelişmiş bir kavram olarak “insanlığın ortak mirası (*common heritage of mankind*)”, üzerinde devlet egemenliği kurulamayacak alanlar için *res communis* rejimlere göre daha sınırlayıcı hükümler öngören bir yaklaşımı ifade etmektedir. Bir alanın insanlığın ortak mirası olarak kabulü halinde artık devletler için bir serbesti ve yarıştan değil; insanlığın menfaatlerini muhafaza etmek adına özel uluslararası rejimlerle kontrol altında tutulan barışçıl faaliyetlerden bahsedilecektir.³⁴⁶

BM Genel Kurulu, barındırdığı zengin doğal kaynaklar sebebiyle özel önem arz eden derin deniz yatağında (bir başka ifadeyle okyanus tabanında) hukuki rejim arayışları sonucu; 1970 tarihli, 2749 (XXV)³⁴⁷ ve 2750 (XXV)³⁴⁸ sayılı kararları ile bu alanı insanlığın ortak mirası olarak tanımlamıştır. Daha sonra BMDHS XI. Kısım’da bu alan “bölge (*the area*)” olarak kısaca adlandırılmış; m. 136 hükmüyle insanlığın ortak mirası olduğu hususu uluslararası antlaşma hükmü haline getirilmiş; m. 137 hükmüyle de bölge üzerindeki hakların bütün insanlığa ait olduğu ve Uluslararası Deniz Yatağı Otoritesi’nin insanlık adına yetkilendirildiği kabul edilmiştir.

1979 tarihli Devletlerin Ay’da ve Diğer Gök Cisimlerindeki Faaliyetlerini Düzenleyen Anlaşma (*Agreement Governing the Activities of States on the Moon and*

³⁴³ Hillier, s.110, Shaw, s.364.

³⁴⁴ Cassese, s.82.

³⁴⁵ Şule Anlar Güneş, “Maden Kaynaklarının Yönetimi Bağlamında Uluslararası Deniz Yatağı Otoritesinin Rolü”, **Uluslararası İlişkiler**, Cilt.17, Sayı.65, (2020), s.109.

³⁴⁶ Alexandre Kiss, “The Common Heritage of Mankind: Utopia or Reality?”, **International Journal**, Vol.40, No.3, (1985), s.425.

³⁴⁷ UN/General Assembly, Declaration of Principles Governing the Sea-Bed and the Ocean Floor, and the Subsoil Thereof, beyond the Limits of National Jurisdiction, **A/RES/2749(XXV)**, 17.12.1970.

³⁴⁸ UN/General Assembly, Reservation Exclusively for Peaceful Purposes of the Sea-bed and the Ocean Floor, and the Subsoil thereof, Underlying the High Seas Beyond the Limits of Present National Jurisdiction and the Use of Their Resources in the Interests of Mankind, and Convening of a Conference on the Law of the Sea, **A/RES/2750 (XXV)**, 17.12.1970.

Other Celestial Bodies),³⁴⁹ Ay'ın ve Güneş Sistemi'ndeki diğer gök cisimlerinin insanlığın ortak mirası olduğunu öngörse de uzayda önemli bir faaliyet göstermeyen az sayıda devlet tarafından imzalanması dolayısıyla uluslararası hukukta etkisiz kalmıştır.³⁵⁰ Antarktika için de henüz insanlığın ortak mirası olduğu hükmüne varılmamış olsa da gidişatın o istikamette olduğu düşünülmektedir.³⁵¹

c. Vatansızlık

Devlet egemenliğinin dışında kalan unsurlar sadece mekânsal değildir. Kişiler için özel bir durum olan vatansızlık³⁵², herhangi bir devlet vatandaşı olmama ve haliyle bulunulan ülkeden veya işlenen fillerden kaynaklı durumlar haricinde kişisel olarak egemenlik altında bulunmama sonucunu doğurmaktadır. İnsan Hakları Evrensel Beyannamesi'nin 15. maddesinde, “her bir ferdin vatandaşlık hakkına sahip olduğu ve hiç kimsenin keyfi olarak vatandaşlığından veya vatandaşlığını değiştirme hakkından yoksun bırakılamayacağı” ilan edilmiştir.³⁵³ “Vatandaşlık hakkı” uluslararası hukuka yerleşirken vatansız kişilerin durumu da göz ardı edilmemiştir. 1954 tarihli “Vatansız Kişilerin Statüsüne İlişkin Sözleşme (*Convention Relating to the Status of Stateless Persons*)”³⁵⁴ ile söz konusu kişilerin durumu uluslararası hukuk nezdinde düzenlenmiştir.

Vatansızlık, kişinin bir devlet vatandaşı olmasına rağmen ilgili devlet tarafından diplomatik koruma sağlanmaması ya da bunu kişinin istememesi halinde *de facto* olarak da ortaya çıkabilmektedir.³⁵⁵ *De facto* vatansızlık 1954 Sözleşmesi'nin kapsamı dışında bırakılmış ve bu tercihin günümüz gerçeklerine uygun olmadığı da belirtilmiştir.³⁵⁶

³⁴⁹ UNTS, Vol.1363, No.23002, 1992, s.3.

³⁵⁰ Kiss, s.436.

³⁵¹ Dixon, s.176-178.

³⁵² Türkçe'de bu kişilerin hukuki durumu için Almanca “heimatlos” kavramının nakliyle “haymatlos” ya da aynı kavramın çevirisi olarak “vatansızlık” tabiri kullanılırken, İngilizce literatürde aslında “devletsizlik” anlamına gelen “statelessness” kavramı kullanılmaktadır. Devlet ve ülkenin ayrılmaz ilişkisi dikkate alındığında, “vatan” tabirinin aslında devlet ülkesini karşıladığı ve vatandaşı olunan devletin yokluğunu ifade eden devletsizlik ile vatansızlığın birbirini sağlayan durumlar olduğu söylenebilecektir. Dolayısıyla iki tabirin kullanımı da vardıkları ortak sonuç itibarıyla anlamlı ve isabetlidir.

³⁵³ UN/General Assembly, A Universal Declaration of Human Rights, A/RES/217(III), 10.12.1948.

³⁵⁴ UNTS, Vol.360, No.5158, 1960, s.117.

³⁵⁵ United Nations High Commissioner for Refugees (UNCHR), **Vatansız Kişilerin Korunması Hakkında El Kitabı: Vatansız Kişilerin Statüsüne Dair 1954 Sözleşmesi Kapsamında**, Cenevre, 2014, s.5.

³⁵⁶ Yeşim Yıldız, “Terör Örgütü Üyeliği Sebebiyle Vatandaşlıktan Çıkarmanın Uluslararası Hukuk Açısından Değerlendirilmesi”, *Sakarya Üniversitesi Hukuk Fakültesi Dergisi*, Cilt.9, Sayı.2, (2011), s.320.

Vatansız kişiler hakkındaki bir diğer önemli uluslararası sözleşme de 1961 tarihli “Vatansızlığın Azaltılmasına İlişkin Sözleşme (*Convention on the Reduction of Statelessness*)”³⁵⁷ olmuştur. Taraf devletlerin vatansızlığın azaltılması adına uluslararası topluluğun tamamına karşı taahhütte bulunması, sözleşmeden doğan uluslararası yükümlülöklere *erga omnes* nitelik kazandırmıştır.³⁵⁸

Vatansızlığın gerek kişileri vatandaşlığın sağladığı önemli hak ve korumalardan mahrum bırakması gibi kişi hallerine ilişkin; gerek “orada bulunma hakkı olmadığı halde bulunan insanlar yaratması” gibi uluslararası sisteme ilişkin sorunlar doğurduğu ileri sürölmüştür.³⁵⁹ Dolayısıyla 1961 Sözleşmesi’nde kabul edilen yaklaşım ile de paralel olarak, vatansızlığın uluslararası topluluk için istenmeyen bir durum olduğu açıktır. Zira egemen siyasi yapıların oluşturduğu bir hukuk sisteminde, kişilerin fiillerinden ve bulundukları ölkeden bağımsız olarak bir devletin egemenliğine tabi olmaları asli önem taşıyacaktır. Yine de fiili şartlar ve siyasi gerekçelerle vatansızlık durumu milyonlarca insan için varlığını korumaktadır.³⁶⁰

³⁵⁷ UNTS, Vol.989, No.14458, 1983, s.175.

³⁵⁸ Gülin Güngör, “Vatansızlığın Azaltılmasına Dair Birleşmiş Milletler Sözleşmesi’nin Bazı Hükömlerinin 5901 Sayılı Türk Vatandaşlığı Kanunu Üzerindeki Etkisi”, *Ankara Üniversitesi Hukuk Faköltesi Dergisi*, Cilt.63, Sayı.3, (2014), s.480.

³⁵⁹ Matthew J. Gibney, “Statelessness and Citizenship in Ethical and Political Perspective”, Alice Edwards ve Laura van Waas (Ed.), *Nationality and Statelessness under International Law* içinde (44-63), Cambridge: Cambridge University Press, 2014, s.49.

³⁶⁰ UNCHR, 96 ölkeden topladığı verilere göre 2021 sonu itibarıyla 4.3 Milyon kişinin vatansız ya da tabiiyeti belirsiz durumda olduğunu raporlamıştır; International Development Law Organization (IDLO) ve UNCHR, *Addressing Statelessness through the Rule of Law*, 2022, s.5.

İkinci Bölüm

SİBER UZAY GENEL HUKUKU

I. SİBER UZAYIN HUKUK İLE İLİŞKİLENDİRİLMESİ

Siber uzayın boyut ve unsurları üzerinde devlet egemenliğinin mevcudiyetini ve hukuki sonuçlarını sorgulamadan önce, siber uzayın genel itibariyle hukuka konu olmasını ve siber uzaya ilişkin genel hukuk teorisine yönelik tartışmaları ele almak gerekmektedir.

Siber uzay eldeki çalışmada teorik bir uzay olarak tanımlanıp analiz edilmiş olsa da siber uzayın hukuk ve devlet ile ilişkilendirilmesi, internetin yükselişi ve klasik siber uzay teorisinin doğuşu ile gerçekleşmiştir. Web fikrinin 1990’da kabulü ve işlerlik kazanmasını takip eden süreçte, özellikle internetin topraklarında doğduğu ABD akademik yazınında dikkate değer bir canlılık yaşanmıştır.

Siber uzay ve hukuk eşleşmesi, en başından bu yana iki yönlü olarak ayrı ayrı değerlendirmelere tabi tutulmuştur. Bir yandan siber uzaydaki gelişmelerin hukuk disiplini ve yargı işleyişini nasıl etkilediği veya etkileyeceği düşünülürken;³⁶¹ diğer yandan hukukun siber uzayı nasıl düzenleyeceği tartışmaları süregelmiştir. Bu ayrımı “hukukun dijitalleşmesi” ve “dijitalleşmenin hukuku” şeklinde ifade etmek de mümkündür.³⁶² Hukukun dijitalleşmesi de bilgi teknolojilerinin üzerinde durulması gereken önemli bir getirisi olmakla birlikte, eldeki çalışmanın esas unsurunu dijitalleşmenin hukuku teşkil etmektedir. Zira bu husus, devlet egemenliğinin omurgası olan hukuk vazetme ve uygulama iktidarı ile doğrudan ilgilidir. Odak nokta, bilgi teknolojilerinin, hukuku konu edinmesinden ziyade; hukukun, bilgi teknolojilerini konu edinmesidir. Bilgi teknolojilerinin hukuk karşısındaki görünümü ise en kapsayıcı ve belirgin haliyle “siber uzay” olarak ifade edilmiştir. Haliyle siber uzayın ele alınma şekli,

³⁶¹ Erken dönem örneklerinden biri olarak *Katsh*’in, LEXIS ve WESTLAW dijital veri tabanlarından hareketle, dönemindeki gelişmelerin hukuk disiplini ve mesleği üzerinde mevcut ve olası etkilerini değerlendirmesi gösterilebilir; Ethan Katsh, “Law in a Digital World: Computer Networks and Cyberspace”, *Villanova Law Review*, Vol.38, Iss.2, (1993), s.403 vd.

³⁶² Jan Oster, “Code is Code and Law is Law – the Law of Digitalization and the Digitalization of Law”, *International Journal of Law and Information Technology*, Vol.29, Iss.2. (2021), s.102.

üzerinde uygulanacak hukukun varlığına ve niteliğine yönelik tasavvurlar için de belirleyici olmuştur.

Siber uzaya ilişkin hukuk teorisini değerlendirmek için literatürde çeşitli tasnif metotları kullanılmıştır. *Hatipoğlu Aydın*, yazarları siber uzayın düzenlenmesine ilişkin yaklaşımlarına göre “siber liberteryenler”, “siber paternalistler” ve “ağ komüniteryenleri” şeklinde; siber uzay için ayrı bir hukuk ihtiyacına yönelik yaklaşımlarına göre de “olağancı” ve “istisnacı” şeklinde kategorize ederek konuyu açıklamayı tercih etmiştir.³⁶³ Benzer olarak, siber uzayın hukuki düzenlemesinin “özerk”, “devlet yasamasıyla” ya da “uluslararası düzenlemelerle” yapılması yönündeki görüşlere göre inşa edilen tasnif örnekleri de söz konusudur.³⁶⁴ Ayrıca çeşitli ekollerden yazarların üzerinde tartıştığı meseleleri esas alan tasniflerle de sıklıkla karşılaşılmaktadır.

Bu çalışmada siber uzay ve hukuk teorisini incelemek için özgün bir dönemlendirme denemesi yapılmıştır. Şüphesiz ki dönemlendirme metodu bu alanda da halihazırda kullanılan bir metottur. Örnek olarak *Lund*, internet teknolojilerinin gelişim durumunu esas alan bir yaklaşımla dört döneme ve teorilerin niteliğine göre beş nesle ayrılmış bir tasnif yapmıştır:³⁶⁵

Çevirmeli ağ (<i>dial-up</i>)	(1996-1998) – 1. Nesil
Geniş bant (<i>broadband</i>)	(1998-2002) – 2 ve 3. Nesil
Mobil internet ve uygulama yayımı	(2010-...) – 4. Nesil
Nesnelerin interneti (<i>internet of things</i>)	(2020-...) – 5. Nesil

Bir diğer dönemlendirme örneği *Svantesson*’a aittir. Yazarın, siber uzayın ilgili dönemlerdeki düzenlenme durumunu esas alarak esprili isimlendirmelerle yaptığı tasnif aşağıdaki gibidir:³⁶⁶

Başlangıçta Hiçbir Şey Yoktu (<i>In the Beginning There Was Nothing</i>) (...-1991)
Vahşi Vahşi Ağ (<i>Wild Wild Web</i>) (1991-1999)

³⁶³ Hatipoğlu Aydın, s.55 – s.131.

³⁶⁴ Bernard Oluwafemi Jemilohun, “Regulating Cyberspace: An Examination of Three Theories”, **International Journal of Business and Management Invention**, Vol.8, Iss.5, (2019), s.20 vd.

³⁶⁵ Luana Lund, “Cyber-regulatory Theories: Between Retrospection and Ideologies”, UNIO EU Law Journal, The Official Blog, Essays, 03.06.2019, <https://officialblogofunio.com/2019/06/03/cyber-regulatory-theories-between-retrospection-and-ideologies/> (31.12.2024).

³⁶⁶ Dan Jerker B. Svantesson, **Solving the Internet Jurisdiction Puzzle**, Oxford, New York: Oxford University Press, 2017.

Aşırı Düzenlemenin İlk Fazı	(2000-2009)
Bir Nebze Yetersiz Düzenleme	(2010-2014)
Hiper Düzenleme Çağı	(2015-?)

Eldeki çalışmada ise literatürdeki başlıca eserler kronolojik bir yaklaşımla ele alınıp, teorinin gelişimi alışlageldik bir isimlendirmeye “erken”, “klasik” ve “modern” dönemlere bölünmüştür. Bu dönemlerin altında ise ilgili dönemin öne çıkan tartışma başlıkları incelenmiştir. Dolayısıyla izlenen metodun mesele bazlı tasnif ile dönem bazlı tasnifin bir karması olarak değerlendirilmesi mümkündür. Görüşlerine göre yazarları kategorize etmektense yazarların görüşleriyle şekillenen genel teorinin gidişatını siber uzayın kısa tarihi içerisinde incelemenin, eldeki çalışmanın sistematığıne daha uygun düşeceği kanaatindeyim. Her bir dönemin kendi karakteristik özellikleri olmakla birlikte, düşünce esasına göre tespit edilen dönemleri keskin sınırlarla ayırmak mümkün değildir. Tıpkı yazarların görüşlerinin ait oldukları ekole mutlak şekilde bağlı olmaması gibi, dönemler içinde de eski dönemden kalma tartışmalara yahut sonraki dönem konularında öncü nitelikte istisnai yaklaşımlara rastlanabilmektedir.

A. Erken Dönem

Öncelikle belirtmelidir ki; siber uzayın kavramsal olarak literatürde hakimiyet kazanmasından önceki dönemlerde dahi bugünkü anlamıyla siber uzaya ilişkin olduğunu söylemeye imkân veren hukuki düzenlemeler mevcuttur. Nitekim yaşanan bilgisayar korsanlığı vakalarına çözüm bulmak amacıyla 1984 yılında ABD’de kabul edilen ve daha sonradan 1986 tarihli “Bilgisayar Dolandırıcılığı ve Kötüye Kullanımı Yasası (*Computer Fraud and Abuse Act*)” ile tekâmül ettirilen “Cihazlara Yetkisiz Erişim, Bilgisayar Dolandırıcılığı ve Kötüye Kullanımı Yasası (*Counterfeit Access Device and Computer Fraud and Abuse Act*)”, söz konusu erken dönem düzenlemelerinin bilişim suçları kategorisindeki ilk örneği olarak kabul edilmektedir.³⁶⁷ Benzer şekilde 1986 tarihli “Elektronik İletişimin Gizliliği Yasası (*Electronic Communications Privacy Act*)” da henüz Web’in ortaya çıkmadığı ve NSFNET’in yeni kurulduğu dönemde görülen öncü

³⁶⁷ Dodd S. Griffith, “The Computer Fraud and Abuse Act of 1986: A Measured Response to a Growing Problem”, *Vanderbilt Law Review*, Vol.43, Iss.2, (1990), s.466.

bir normdur.³⁶⁸ Neuromancer'ın 1984'te basılmış olmasından da çıkarılacağı üzere; bu normlar ihdas edilirken, ilgili düzenlemelerin siber uzay kavramıyla ilişkilendirilmesi henüz söz konusu değildir. Öğretide bu ilişkilendirmeye, klasik teorinin hâkim olduğu 1990 sonrası eserlerde başvurulmaya başlanmıştır.³⁶⁹

Erken dönem literatüründe siber uzaya ilişkin sorunlar, elektronik iletişim ve “sınır aşan veri akışı (*transborder data flow*)” kavramları üzerinden ele alınmıştır. Henüz 1986'da *Glasner*, uluslararası iletişimde hakimiyeti olan çok uluslu şirketlerin sınır aşan veri akışını giderek yükselen bir hızla kullanmasının devlet egemenliğine karşı bir tehdit olarak görülmesi sebebiyle, ABD'nin bu veri akışına yönelik kısıtlayıcı düzenleme girişimlerinde bulunduğunu ifade etmiştir.³⁷⁰ *Miller*'a göre devletler siyasi, sosyal ve kültürel menfaatlerini korumak için sınır aşan veri akışını serbest bırakmaktan kaçınmakta ve serbest akışın getireceği menfaatlerden bilgisel egemenliğin tesisi maksadıyla feragat etmektedir.³⁷¹ *Kirby* ise sınır aşan veri akışının “bilişim” şeklinde de ifade edildiğini vurgulamış ve bu küresel fenomenin klasik anlamdaki ülkesel yargı yetkisiyle alay ederek egemenliğe meydan okuduğunu ileri sürmüştür.³⁷²

EFF kurulurken *Kapor* ve *Barlow*, siber uzayın; teknik, hukuki, sosyal ve kültürel anlamda bütün zorlukların üstesinden gelmeye çalışan bir grup insanın cephe hattı olduğunu iddia etmişlerdir.³⁷³ Altı yıl sonrasında Siber Uzay Bağımsızlık Bildirgesi'ni de yazacak olan *Barlow*'un görüşleri bu zemin üzerinde şekillenmiş görünmektedir. *Branscomb* da EFF kurucularının tanımına atfen “elektronik cephe” olarak tanımladığı siber uzay için geçerli olacak hukuku sorgulayan çalışmasında, o dönemde Web'in

³⁶⁸ I. Trotter Hardy, “The Proper Legal Regime for 'Cyberspace'”, *University of Pittsburgh Law Review*, Vol.55, Iss.4 (1994), s.1046.

³⁶⁹ Yine de 1987'de Aronson'un zaman, uzay, coğrafya ve siyasi organizasyonu kapsayan elektronik çevreyi siber uzay olarak adlandırıp hukuk ile ilişkilendirmesi gibi istisnai örnekler görülebilmektedir; Jay D. Aronson, “Telecommunications Negotiations in GATT”, *Transnational Data and Communications Report*, Vol.10, No.2, (1987), ss.11-13.

³⁷⁰ Sol Glasner, “Multinational Corporations and National Sovereignty”, Anne W. Branscomb (Ed.), *Toward a Law of Global Communications Networks* içinde (335-342), New York, London: Longman, 1986, s.339.

³⁷¹ Anthony Paul Miller, “Teleinformatics, Transborder Data Flows and the Emerging Struggle for Information: An Introduction to the Arrival of the New Information Age”, *Columbia Journal of Law and Social Problems*, Vol.20, No.1, (1986), s.107 vd.

³⁷² Michael Kirby, “Legal Aspects of Transborder Data Flow”, *Computer/Law Journal*, Vol.11. Iss.2, (1991), s.233.

³⁷³ Mitchell Kapor ve John Perry Barlow, “Across the Electronic Frontier”, 10.07.1990, <https://www.eff.org/tr/pages/across-electronic-frontier> (31.12.2024).

öncüsü sayılabilecek elektronik bülten panolarından³⁷⁴ (*bulletin board system* (BBS))³⁷⁵ hareketle; bunların bir kısmının tıpkı bir sokak köşesi gibi hem özel hem kamusal nitelikteki ilişkilere açık hibrit alanlar olduğu, önemli bir kısmının ise özel amaçla ve belirli kullanıcılar tarafından erişilen siteler olduğu yönünde ayırıcı bir tespit yaparak birtakım sorular ortaya koymuştur.³⁷⁶ Yazara göre topluluklar genellikle kendi etik değerlerini temsil eden ve usulüne uygun olarak çıkarılan yasalarla yönetilir. Fakat sözgelimi bir BBS birden fazla ülkeden ya da farklı vatandaşlıklara sahip kişiler tarafından erişilebilir olduğunda farklı hukuk sistemlerinin kapsama alanına girecektir. Bu durumda yazarın temel sorusu, ilgili kuralların yer itibarıyla (*locus*) coğrafi esaslı mı yoksa elektronik esaslı mı değerlendirileceği yönündedir. Şayet bu soruya cevap olarak elektronik ortam esas alınacaksa, bu alandaki düzenlemelerin nasıl ve kimler tarafından tespit edileceği ile uyumsuzlukların çözümünden hangi kurumların sorumlu olacağı gibi sorular doğacaktır. *Branscomb* sorduğu soruları bu çalışmada cevapsız bıraksa da siber uzayın genel hukukunun kullanıcıların çabalarıyla gelişeceği öngörüsünde bulunmuştur.³⁷⁷ Bir başka erken dönem yazarı olan *Burk*, konuyu benzer şekilde patent hakları üzerinden ele aldığı çalışmada siber uzay için yaptığı “küresel bilgi otobanları” yakıştırması ile *Gibson*’ın kurgusunun gerçeğe dönüştüğünü savunmuş ve siyasi sınırların ortadan kalktığı yerde siyasi kaosun ortaya çıkabileceğini; bilginin sınırlarının olmadığı yerde de mahremiyet ve hatta kimlik kaybının gerçekleşebileceğini öngörmüştür.³⁷⁸ *Branscomb* da benzer şekilde küresel ağları dünya çapında bilgi transferinin gerçekleştiği elektronik otobanlara benzetecektir. Yazar, bu sınır aşan çevredeki işleyiş ve unsurlara hâkim ulusal hukuk düzenlerinin yeknesak olmayışının, özgün nitelikteki birçok hususun henüz düzenlenmemiş olmasının ve özgürlük talep ederek eylemlerini bu yönde icra eden kullanıcıların ulus devletler için egemenlik kaygılarına yol açtığını ifade etmiştir.³⁷⁹

³⁷⁴ Türkçeye BBS kısaltmasıyla uyumlu olması bakımından “bilgisayarlı bilgi sistemi/servisi” şeklinde de çevrilmektedir.

³⁷⁵ Açıklayıcı bilgi için bkz. “Bulletin-board system”, Britannica, <https://www.britannica.com/technology/bulletin-board-system> (31.12.2024).

³⁷⁶ Anne Wells Branscomb, “Common Law for the Electronic Frontier”, *Scientific American*, Vol.265, No.3, (1991), s.158.

³⁷⁷ Ibid.

³⁷⁸ Dan L. Burk, “Patents in Cyberspace: Territoriality and Infringement on Global Computer Networks”, *Tulane Law Review*, Vol.68, No.1, (1993), ss.3-4.

³⁷⁹ Anne Wells Branscomb, “Jurisdictional Quandaries for Global Networks”, Linda M. Harasim (Ed.), *Global Networks: Computers and International Communication* içinde (83-103), Cambridge: The MIT Press, 1993, ss.102-103.

B. Klasik Dönem

Elektronik iletişim ve sınır aşan veri akışı gibi kavramlar, erken dönem sonunda Web'in doğuşuyla birlikte toplu olarak siber uzay kavramında mündemiç hale gelmiştir. Klasik dönemin karakteristik özelliği, siber uzayın sanal bir mekân olarak kabul edilmesi ve bu kabule ilişkin şöyle bir tartışma zincirinin ortaya çıkmasıdır:

- 1 – Siber uzayın fiziksel uzaydan ayrı bir mekân olarak kabulü mümkün müdür?
- 2 – Şayet böyle bir mekânın varlığı kabul edilirse; burada geçerli bir hukuk ihdası mümkün müdür?
- 3 – Şayet hukuk ihdası mümkünse; böyle bir faaliyet gerçekten gerekli midir?
- 4 – Şayet hukuk ihdası mümkün ve gerekliyse bu faaliyet nasıl ve ne yönde gerçekleşmelidir?

Rusch'a göre; 1. soruya verilen olumlu bir cevap, fiziki uzayda geçerli hukuk normlarının siber uzayı düzenleyemeyeceği ve siber uzay için ayrı bir hukuka ihtiyaç duyulduğu kabulünü zımni olarak içinde barındırır.³⁸⁰ Söylenebilir ki klasik dönemin öne çıkan yönü, bu önermeyi kabul eden ve reddeden yazarlar arasındaki teorik tartışmadır.

1. İlk Analoji Tartışmaları

Yeni ortaya çıkan herhangi bir olgunun hukuka konu edilmesinde, kadim bir metot olan kıyas ve analojiye başvurulması kaçınılmazdır. Analoji tartışmaları klasik dönemle sınırlı kalmadan günümüzde dahi devam etmektedir. Web sonrası dönemde, fiziki uzayda cari olan hukuk normlarının analoji yoluyla siber uzaydaki olgular üzerinde geçerli kılınması fikrine yönelik karşıt sesler yükselmeye başlamıştır.³⁸¹ *Hardy*, siber uzaya dair ayrı bir hukuk ihtiyacının varlığına ilişkin tartışmaları etraflıca ve yüksek bir perspektifle ele alarak klasik dönemin öncü çalışmalarından birine imza atmıştır. Yazar, siber uzayın gerçekten yeni ve farklı bir alan olup olmadığı sorusuna verilecek cevabın büyük ölçüde öznel olacağını ifade edip; meselelere soyut ve yüksek irtifadan yaklaşıldığında, genel hukuk kurallarının dünyadaki her olgu için bir şekilde uygun

³⁸⁰ Jonathan J. Rusch, "Cyberspace and the 'Devil's Hatband'", *Seattle University Law Review*, Vol.24, Iss.2, (2000), s.591.

³⁸¹ *Hardy*, s.994.

düşebileceği hatta tikel konuların bir jüriye teslim edilip jürinin adalet anlayışına göre dahi çözümlenebileceği söylenebilecekken; detaycı ve derinlikli yaklaşıldığında ise her hukuki sorunun -sadece tarafların isimlerinde dahi olsa- farklılık arz edeceği ve dolayısıyla her meselenin yeni ve düzenlenmeye muhtaç olduğu kabulünün doğacağını ifade etmiştir.³⁸² Hukuka konu olan her sahada olduğu gibi bilişim ve dolayısıyla bilişimin tecessüm ettiği siber uzay için de bu yaklaşım yelpazesi içinde en isabetli pozisyonun tespiti temel bir problemidir.

Hardy, siber uzay kaynaklı bazı problemlerin asla yeni olmadığını ve sadece bağlamın farklı olduğunu; bazılarının ise “gerçek uzay (*real space*)” sorunlarına göre yeni özellikler taşıdığını ve bu konulardaki hukuki hükümlerin tartışmaya açık olduğunu savunmuştur.³⁸³ Bir sahada geçerli normlar, yukarıdan aşağıya doğru hukuk vazedilmesiyle oluşabileceği gibi; teamüller ve doktrin yoluyla aşağıdan yukarıya doğru da inşa edilebilmektedir. Yazara göre, teknolojik gelişmelerin hızı ve oluşan durumların değişkenliği göz önüne alındığında en esnek yol olan adem-i merkezîyetçiliğin daha uygun olduğu söylenebilecektir. Siber uzaya müdahale edilmediği takdirde insanlar doğal bir süreç olarak önce kendi kendine yetme yoluna gidecek; bu tavır ihtiyaçları karşılamadığında sözleşme yoluna başvuracak ve topluluğun anlaşmalı hareketleriyle aşağıdan yukarıya doğru bir norm üretimi sağlanabilecektir. Fakat üçüncü kişilerin zarar gördüğü durumlarda (ayrıca kamu düzenini ilgilendiren konularda) ise yukarıdan aşağıya yasa üretimine ve yargısal çözüm yollarına ihtiyaç doğacaktır.³⁸⁴

Eldeki çalışmanın ilk bölümünde *Dyson*, *Gilder*, *Keyworth* ve *Toffler*’ın siber uzaya ilişkin tanımlarına değinilmiştir. Yazarlar aynı eserde öncelikle siber uzayın “bilgi otobanı” şeklinde ifade edilmesine karşı çıkmışlardır.³⁸⁵ Bu karşı çıkışın temelinde, yazarların esas hareket noktası olan, insanlığın tarım toplumu ve devamındaki sanayi toplumu dönemlerinin ardından artık üçüncü dalga olarak bilgi toplumuna geçmekte olduğu ve bu dönemin ikinci dalga argümanlarla ele alınmasının yanlışlığı düşüncesi

³⁸² Ibid., 996.

³⁸³ Söz gelimi bir hakaretin ya da tehdidin e-posta yoluyla iletilmesinin, telefon ya da mektupla iletilmesinden hukuk nezdinde bir farkı yoktur. Fakat *Hardy*’nin kendi dönemi itibarıyla BBS yöneticileri ile örneklediği ve günümüzde “yer sağlayıcı (*hosting provider*)” olarak adlandırılan kişi ve kurumların durumu, fiziki uzaydaki kitapçı, kütüphane ve gazete/dergi gibi örneklere göre kritik farklılıklar arz etmesi yönüyle “yeni” niteliklere sahiptirler.

³⁸⁴ *Hardy*, s.1054.

³⁸⁵ *Dyson ve Diğerleri*, s.297.

yatmaktadır. Yazarlara göre üçüncü dönemde hükümetler, çağın getirisi olarak küçülmeli ancak temel ve kurucu fonksiyonlarını en güçlü şekilde yerine getirmelidir. Diğer taraftan bu dönemin başrolünde bulunan ve ayrı bir mekân olan siber uzay için ise ikinci dalga hukuki kabulleri terk ederek yeni nesil ve özgürlükçü yaklaşımlara geçilmesi gerekmektedir.³⁸⁶ “Otoban” ifadesinin kullanımı dahi eski dönemin sınırlarıyla çerçevelenecek bir analogi olacağı için siber uzayın hakikatini yansıtmaktan uzak kalacaktır. Aynı dönemde *Barlow* da siber uzayın düzenlenmesi girişimlerine karşı çıkarak, ABD topraklarında birbirinden çok farklı grupların otorite yokluğu/boşluğu altında yaşadığı girişimci, rekabetçi ve devingen özellikleriyle maruf “Vahşi Batı” olarak adlandırılan dönemi olumlu anlamda örnek gösterip; siber uzayın, müesses nizamın desteklediği çıkar gruplarının menfaatlerine uygun şekilde dizayn edilmesinin kabul edilemez olduğunu savunmaktaydı.³⁸⁷

2. İlkesel Tartışmalar

1994’ün aralık ayında Yale’de gerçekleşen bir sempozyum, gelişen medya teknolojisiyle ortaya çıkan özgürlükçü yaklaşımların ABD Anayasası’nın ifade özgürlüğünü düzenleyen meşhur 1. Değişiklik (*First Amendment*) hükümlerine atfen nasıl ele alınacağını konu edinmişken, siber uzayın hukuk teorisi için öncü yaklaşımların beyan edilmesine de vesile olmuştur. Bunun arka planında, ağda faaliyet gösteren toplulukların özgürlükçü ve devlet egemenliğinden -en azından sanal ortam içinde- istisna tutulmaya yönelik taleplerinin olduğunu görmek mümkündür. Söz konusu programdaki katılımcıların belli başlı görüşlerine değinmek, genel teorinin ana tartışma noktalarının görülmesi açısından faydalı olacaktır.

Konuyla ilgili çalışmaları erken döneme dayanan *Branscomb*, bu kez siber uzaydan genel anlamıyla bahsetmek yerine; “ağdaş (*netizen*)” olarak tabir ettiği kişilerden müteşekkil siber-toplulukların oluşturduğu “siber uzaylar” olduğunu ve bunların tamamının bir “ağ dünyası (*networld*)” meydana getirdiğini söylemeyi tercih etmiştir.³⁸⁸

³⁸⁶ Ibid., s.303.

³⁸⁷ John Perry Barlow, “Jack In, Young Pioneer!”, 11.08.1994, <https://www.eff.org/tr/pages/jack-young-pioneer> (31.12.2024).

³⁸⁸ Anne Wells Branscomb, “Anonymity, Autonomy, and Accountability: Challenges to the First Amendment in Cyberspaces”, *The Yale Law Journal*, Vol.104, No.7, (1995), s.1640.

Yazara göre, liberal talepler üç faktörlü bir denge mekanizması gözetilerek değerlendirilmelidir. Bu faktörleri de “anonimlik”, “özerklik” ve “hesap verilebilirlik” şeklinde tespit etmiştir. Bir tarafa ağırlık verildiğinde diğer değerlerden taviz verilmesi gerekecek ve bu taviz dengesinin ideal formunun tespit edilmesi önem arz edecektir.³⁸⁹ Siber uzayların, erişim için belli seviyede maddi imkana ihtiyaç duyulması göz önüne alındığında erişime yönelik eşitlikçiliği sorgulanabilir olsa da ve kötü niyetli kişilerin suiistimaline açık noktaları bulunsa da toplulukların bu sorunları aşmaya yönelik etkili çalışmaları olduğunu ifade eden yazar; siber uzayların hukukunu inşa etme yolunda kesin hükümlerde bulunmanın doğru olmadığını ve özgün bir “net-etik (*netiquette*)” inşa etmeleri yönünde siber-topluluklara fırsat tanınması gerektiğini savunmuştur.³⁹⁰

Sunstein, siber uzaya anayasal temelden ve ifade özgürlüğü perspektifinden yaklaşarak siber uzay için genel hukuk teorisinin, -çoğulculuğun ve siyasi eşitliğin sağlanması adına devlet eliyle düzenlemeler yapılması gerekliliğini savunan- Madisoncu esaslara göre inşasının imkanını sorgulamıştır.³⁹¹ Bu konuda Madisoncu yaklaşımın izlerini taşıdığını düşündüğü ABD Yüksek Mahkemesi’nin “*Turner Broadcasting System, Inc. v. FCC*”³⁹² kararını örnek gösteren yazar; bu örneğin, gelişen teknolojilere binaen 1. Değişiklik hükümlerine uygun düzenlemeler getirmesi için devlete bir alan açtığını ileri sürmüştür.³⁹³

Gerek konu hakkında ürettiği eser sayısı gerek bu eserlerin akademik sahadaki etkisi itibariyle siber uzay ve hukuk ilişkisi adına en önde gelen yazar olduğu söylenebilecek *Lessig* burada konuya ilk girişini yaparak *Sunstein*’in görüşüne temkinle yaklaşmıştır.³⁹⁴ Yazar öncelikle insanların siber uzayda -gerçek uzayda mümkün olmayan

³⁸⁹ Ibid., s.1641.

³⁹⁰ Ibid., ss.1677-1679.

³⁹¹ Sunstein, s.1804.

³⁹² Kablolu TV yayıncılığının karasal yayına göre sahip olduğu üstünlükler, ABD Kongresi’ni -karasal kanalların belirli oranlarda kablolu TV operatörlerince taşınması zorunluluğunu da içeren- rekabeti dengeleyici önlemler almaya yöneltmiştir. Arka plandaki niyetin, karasal yayıncıların maddi menfaatlerinin korunması mı; serbest karasal yayıncıların hayatta kalamaması sonucunda, yönetimi operatörlerin elinde olan kablolu TV aboneliğine halkın mecbur kalması ihtimalinin önüne geçilmesi mi; dezavantajlı duruma düşen karasal yayınlara erişimin Madisoncu bağlamında çeşitliğin sağlanması adına desteklenmesi mi olduğu hususu tartışmalıdır. Turner Yayıncılık Şirketi’nin kanuna karşı -yayıncıların içeriğine müdahale edilerek ifade özgürlüğünün ihlal edildiği iddiasıyla- yaptığı yargı başvurusuyla alınan 1994 ve 1997 kararları sonucunda kanun hükümlerinin anayasaya aykırılık içermediğine hükmedilmiştir; 512 U.S. 622 (1994) – 520 U.S. 180 (1997).

³⁹³ Sunstein, ss.1779-1780.

³⁹⁴ Lawrence Lessig, “The Path of Cyberlaw”, *The Yale Law Journal*, Vol.104, No.7, (1995), s.1754.

yollarla- toplandıklarını, konuştuklarını, “yaşadıklarını” ve kendilerini inşa edip tanımladıklarını ifade ederek aslında siber uzayın gerçek uzaydan ayrı bir mekân olduğu kabulüne varmıştır.³⁹⁵ Siber uzayın sonuçlarının hangilerinin “gerçekten yeni” olduğu sorusuna da eğilen *Lessig*, önemli ve gerçekten yeni olan şeyin, pazar yerleri gibi sıradan uzayda da bulunan yerlerin dijital karşılığından ibaret olgular değil; siber uzayın doğurduğu topluluklar ve bu toplulukların inşa ettiği yeni ilişki biçimleri olduğunu belirtmiştir.³⁹⁶ Bu yenilikler bakımından da insanlığın mevcut konumunu, telefonun mucidi Graham Bell’in söz gelimi modern anlamda “uzak mesafe ilişkisi” kavramını - vizyoner kişiliğine rağmen- anlamasının imkansızlığına benzetmiştir.³⁹⁷ Yazara göre kimlik gizleme ya da mesaj şifreleme gibi fiiller dijitalliğin hiç olmadığı zamanlarda da mümkündür fakat bunların mutlaklaşması ya da kolaylaşarak yaygınlaşması, devletlerin yeni hukuki tedbirlerle müdahale isteklerini haklı çıkarabilecektir.³⁹⁸ *Lessig* nihayetinde, siber uzayın düzenlenmesi yönünde daima devam edeceğini düşündüğü özgürlükçü ve düzenlemeci yaklaşım arasındaki çatışmada pozisyon seçmekten kaçınıp zamanlamaya dikkat çekmiş ve ancak siber uzayın insan hayatına tam olarak kök salmasıyla normların isabetli şekilde tespit edilebileceğini savunmuştur.³⁹⁹ Bu süreçte tabii ki bazı somut olayların yargı önünde çözümü gerekecektir ve mahkemeler bundan kaçınamayacaktır. Alt mahkemelerin bu kararları, hukuk inşası sürecinde önemli rol oynayacaktır. Fakat mahkemeler siber uzay ve insanlık ilişkisi yeterli olgunluğa ulaşınca dek bağlamın tartışmalı doğasını göz ardı ederek kesin hükümler vermekten kaçınmalı, çekişmenin kendi kendini çözmesinin yollarını aramalıdır. Nitekim istikrarlı doktrinler ancak uzun süren ve tekrar eden deneysel süreçler sonunda kurulabilir. Böylece siber uzayın ve barındırdığı toplulukların üretkenliğinin önüne geçilmemesi de sağlanacaktır.⁴⁰⁰

Yukarıdaki yazarların görüşlerinden anlaşılacağı üzere bu noktaya kadar siber uzayın ayrı bir mekân olduğu ve -özgürlükçü kullanıcıların çeşitli itirazları söz konusu olsa da- bu mekânda geçerli olacak hukuki düzenlemelere ihtiyaç duyulacağı genel olarak kabul edilmiştir. *Hatipoğlu Aydın* da “siber paternalistler” ve “siber liberteryenler”

³⁹⁵ Ibid., s.1746.

³⁹⁶ Ibid., s.1745.

³⁹⁷ Ibid., s.1747.

³⁹⁸ Ibid., s.1751.

³⁹⁹ Ibid., s.1752.

⁴⁰⁰ Ibid., ss.1753-1755.

şeklinde tanımladığı düzenlemeci ve özgürlükçü tarafların, siber uzayı ayrı bir mekân olarak görmekte mutabık olduklarına dikkat çekmiştir.⁴⁰¹

3. “At Hukuku”

Devletlere ve onların egemenliklerine siber uzayda yer olmadığını iddia eden Barlow’un meşhur bildirgesiyle⁴⁰² başlayan 1996 yılı, karşıt görüşlerdeki yazarların günümüz eserlerinde dahi sıkça anılan çalışmalarına sahne olması bakımından klasik dönem teorisi için önemli bir dönemeçtir. Bu noktada en dikkat çekici görüşlerden birinin *Easterbrook*’a ait olduğu söylenebilir. *Easterbrook*, nasıl ki atlara dair insan hayatında çok çeşitli hukuki durumlar bulunmasına rağmen⁴⁰³ “at hukuku” kavramından bahsedilmiyor ve bu konudaki meseleler ilgili genel hukuk dallarının hükümlerince çözülüyorsa; benzer şekilde siber uzay için de özel bir hukuk öngörülmesinin yersiz olacağını iddia etmiştir.⁴⁰⁴ Fikri mülkiyet ve telif hakları üzerinden hareket eden yazar, esas ihtiyacın siber uzay için bir fikri mülkiyet hukuku inşa etmek değil; mevcut fikri mülkiyet hükümlerinin daha çok geliştirilmesi olduğunu ve siber uzayda ortaya çıkacak hukuki meseleleri de bu hükümlerle çözmeye devam etmenin isabetli olacağını savunmuştur. Zira sürekli ve çok hızlı değişen bir olguya dair hukuk inşasında ısrar etmek beyhude olacaktır.⁴⁰⁵ Yazar, siber uzayın varlığını olgusal olarak pek tabii tanımış görünmektedir; fakat ayrı bir mekân oluşuna dair kanaat belirtmemiştir. Ayrıca siber uzaya özgü bir hukuk rejiminin gerekliliğini reddetmekle birlikte siber uzayın gelişimini serbest bırakmak ve kullanıcıların çözümlerini kendi kendilerine bulmalarını teşvik etmek yönünde bir pozisyon almıştır. Yargıç *Easterbrook*’un bu düşüncelerini ileri sürdüğü konferansta dinleyiciler arasında bulunan *Lessig* ise yazarın düşüncelerine yönelik -üç yıl sonra da olsa- kapsamlı ve doğrudan bir cevap metni yazacaktır. *Lessig* aslında at hukukunu savunmamaktadır ve *Easterbrook*’un kaygılarına da hak vermektedir. Ancak siber uzay hukukunun müstakilen ele alınmasının, sadece siber uzaya ilişkin özel

⁴⁰¹ Hatipoğlu Aydın, s.41.

⁴⁰² John Perry Barlow, **A Declaration of the Independence of Cyberspace**, Electronic Frontier Foundation, <https://www EFF.org/tr/cyberspace-independence> (31.12.2024).

⁴⁰³ Yazar, bu durumları; “atların satışı, insanları tekmelemesi, lisanslanması, yarıştırılması ya da veterinerlerin atlara bakım vermesi veya at gösterilerinde ödüller verilmesi” şeklinde örneklemiştir; Frank Hoover Easterbrook, “Cyberspace and the Law of the Horse”, *The University of Chicago Legal Forum*, 1996, s.207.

⁴⁰⁴ *Ibid.*, ss.207-208.

⁴⁰⁵ *Ibid.*, s.210.

kaygıların değil; hatta daha çok genel hukuka ilişkin kaygıların bir sonucu olduğunu ifade etmiştir.⁴⁰⁶ Yazarın özellikle üstünde durduğu nokta, siber uzayın kendisini inşa eden kodlar sebebiyle gerçek uzaydan çok farklı bir “tasarıma” ve dolayısıyla farklı dinamiklere sahip olmasıdır. Kimlik gizleyerek kanundan kaçınma, fiillerin takip edilmesi, mahremiyetin ihlal edilmesi gibi çeşitli hususların gerçek uzaydaki biçimleriyle siber uzaydaki biçimleri arasında çok temel farklılıklar vardır. Dolayısıyla gerçek uzayda uygulanan genel hukuk normlarının siber uzayın mimarisiyle uyumsuzluğu, bazı sorunları beraberinde getirecektir.⁴⁰⁷ Ortada bir zorluk olduğu açık olsa da siber uzayın hükümetler tarafından düzenlenemeyeceğini düşünmek de yanlıştır. Zira siber uzayı inşa eden kod ve dolayısıyla siber uzayın tasarımı değiştirilemez değildir. Hükümetlerin de bunun değişmesini hukuk yoluyla sağlaması imkânsız değildir.⁴⁰⁸

Öğretideki siber uzay tanımları değerlendirilirken de değinildiği üzere siber uzayın ayrı bir mekân olarak kabul edilmesine karşı çıkan yazarlardan olan *Shapiro* da at hukuku tartışmasına katılmıştır. Yazar öncelikle bir vasiyetnamenin dijital olarak yazılması yahut bir bankanın internet üzerinden soyulması gibi durumlar için ayrı bir disipline ihtiyaç olmadığından ve gerçek uzayda geçerli hukuk kurallarının yeterli olduğundan bahisle, eleştirisini at hukukuna benzer bir konsept olarak “alfabe hukuku” metaforuyla temellendirmiştir.⁴⁰⁹ *Easterbrook*’un at hukuku eleştirisini de dolayısıyla haklı bulan *Shapiro*, *Lessig*’i de koda ve mimariye işaret etmesi bakımından desteklemiştir. Nitekim insanların gerçek uzaydaki bir konuya dair davranışlarının düzenlenmesi istendiğinde, yasaklama veya serbest bırakma gibi hukuk normlarının yanında, hayatın pratiklerine ve gerçek uzayın tasarımına yönelik düzenlemeler de büyük önem arz edecektir. Siber uzay ile ilişkili eylemler için de kodun böyle bir önemi söz konusudur.⁴¹⁰ Bu görüşler, modern dönemin önemli başlıklarından olacak “kodun hukuka konu edilmesi” meselesinin de ayak sesleri niteliğindedir.

⁴⁰⁶ Lawrence Lessig, “The Law of the Horse: What Cyberlaw Might Teach”, **Harvard Law Review**, Vol.113, No.2, (1999), s.503.

⁴⁰⁷ Ibid., ss.503-505.

⁴⁰⁸ Ibid., s.505.

⁴⁰⁹ Yazara göre siber uzay, tıpkı telefon ve televizyon gibi hatta en kadimi olan alfabe gibi iletişim kanallarından sadece bir tanesidir. Yazı da bir teknolojidir fakat insanlar, iletişimlerine aracı kıldıkları bu teknoloji için ayrı bir hukuk arayışına girmemişlerdir; *Shapiro*, ss.712-713.

⁴¹⁰ Ibid., ss.717-719.

Sommer, siber uzay için ayrı bir hukuk düşüncesine en keskin şekilde karşı çıkan yazarlardandır. Yazara göre siber uzayın hukuka ilişkin özel konumunu internetin yönetimi ile sınırlandırmak gereklidir. Siber uzayla doğan sosyal sonuçlar açısından ise hukuk, teknolojiye göre belirlenmeyecektir.⁴¹¹ *Sommer*, teknolojinin hukuk karşısında gerçekten “yeni” olan bir durum doğurmasının çok istisnai olduğunu; siber uzayla ilişkilendirilen hukuki durumların hemen hepsinin mevcut hukuk disiplininin cevaplandığını iddia etmiştir.⁴¹² Özellikle yakın tarihte teknik ve teknolojik gelişmeler sıklıkla sosyal ilişkileri etkilemiş ve hukukun çözüm getirmesi gereken olgular gözlemlenmiştir. Fakat bu çözümler genel hukuk kurallarıyla gerçekleşmiş ya da alana özgü hukuk yapılsa dahi teknolojinin kendisinden bağımsız olarak, sosyal ve fiziksel sonuçlar üzerinde inşa edilmiştir. *Sommer*, düşüncesini pamuk çırçırının icadına, petrol ile gazın çıkarılmasına ve mülkiyetine dair hususların düzenlenmesi gibi örnekler üzerinden açıklamıştır. At hukuku eleştirisine benzer şekilde vermiş olduğu, aşağıdaki alıntılarda görülen örnekler de ilgi çekicidir:

*“Görgü tanıklığı için insan gözünün ışığa ihtiyaç duyması onu “optik hukuku” konusu yapmaz; insan vücudunun zayıflığı ve acıya karşı hassasiyeti sebebiyle cismani zarara ilişkin hukuka “lezyonlar hukuku” adı verilmez. Teknoloji doğal bir olgu değildir. Doğa ya da mantık bilimleri tarafından kısıtlanmış da olsa toplumsal bir çabadır.”*⁴¹³

*“Birçok açıdan, siber uzay diğer sosyal pratiklerden ya da sosyal pratik setlerinden daha benzersiz değildir. “Hukuk ve siber uzay”, hukukun başka herhangi bir sosyal pratikle yan yana anılmasına benzer. Egemenlik tartışması bu noktayı çok iyi gösteriyor. “Siber uzay ve egemenlik” yapısal olarak “bankacılık ve egemenlik”ten, “küreselleşme ve egemenlik”ten, “alışveriş merkezleri ve egemenlik”ten veya benzerlerinden farklı değildir. Hepsi aynı siyasi teoriden ve aynı hukuk kaynaklarından beslenmektedir. Hiçbiri kendilerini diğerlerinden olağanüstü derecede farklı kılan yapısal özelliklere sahip değildir.”*⁴¹⁴

⁴¹¹ Joseph H. Sommer, “Against Cyberlaw”, *Berkeley Technology Law Journal*, Vol.15, No.3, (2000), s.1227

⁴¹² Ibid., s.1228.

⁴¹³ Ibid., s.1153.

⁴¹⁴ Ibid., ss.1230-1231.

Yine de *Sommer*, siber uzay hukukunu anlamsız bulmakla birlikte, bütün olgular gibi siber uzayın da hukuk ile ilişkilendirmesinin hukuk disiplinine dair birçok konunun aydınlatılmasına fayda sağlayacağını ifade etmiştir.⁴¹⁵

4. Siber Uzayın Özerklik Talebi Olarak “Siber Hukuk”

Modern devlet egemenliğinin en önemli sonuçlarından birinin ülkesel yetki olduğundan yukarıda bahsedilmiştir. Klasik dönemde en çok ses getiren görüşlerden biri, EFF takipçileri olan *Johnson ve Post* tarafından serdedilmiştir. Yazarlar siber uzayın, sınır aşan özelliklerine binaen, genel geçer egemenlik ve ülkesel yetki doktrininin istisnası haline geldiğini savunmuşlardır.⁴¹⁶ Siber uzayı ayrı bir mekân olarak ele alan yazarlara göre, siber uzayın ülkesel esaslarla belirlenmiş sınırları yoktur; zira siber uzayda bir ileti gönderiminin hızı ve maliyeti, fiziksel konumdan neredeyse tamamen bağımsızdır.⁴¹⁷ Bu bakımdan siber uzayda dolaşan bilginin hükümetlerce kontrol edilerek ülkesel egemenliğe tabi kılınması mümkün değildir.⁴¹⁸ Benzer şekilde, uyrukluğunda olduğu devletin hukukuna tabi olmayı ve tam bir serbestlikle uyrukluk değiştirmenin veya ülkeler arası dolaşmanın imkansızlığını gerektiren “vatandaşlık” konsepti de siber uzayda anlamını yitirmiştir.⁴¹⁹ Yazarlar, normlardan azade bir siber uzay iddiasında da değildir. İşaret ettikleri temel nokta; kendi özgün dinamiklerine sahip olan sanal bir mekânın, fiziksel uzaya göre kurgulanmış normlara tabi tutulmaması gerektiği düşüncesidir. Düzenlemeci yazarlardan ayrıldıkları husus ise; doğan ihtiyacı karşılayacak olanın yine siber uzayın kendisi olduğu iddialarıdır. İddialarına göre “siber hukuk (*cyberlaw*)”, devletlerin hukuk yapma mekanizmalarının dışında; bir nevi siber uzayın kendi yasama ve yürütme sistemi üzerinde kurulacaktır. Zira eğer ayrı bir mekân mevcut ise onun ayrı bir hukukunun olmasını düşünmek de doğal olacaktır.⁴²⁰

Johnson ve Post’un görüşleri literatürde oldukça ses getirmiş, çok sayıda eleştiri yazısına da maruz kalmıştır. Bunların arasından başat örnek, iki yıl sonrasında kaleme

⁴¹⁵ Ibid., s.1231.

⁴¹⁶ David R. Johnson ve David Post, “Law and Borders: The Rise of Law in Cyberspace”, *Stanford Law Review*, Vol.48, No.5, (1996), s.1367.

⁴¹⁷ Ibid., s.1370.

⁴¹⁸ Ibid., s.1372.

⁴¹⁹ Ibid., s.1402.

⁴²⁰ Shapiro, s.708.

aldığı kapsamlı çalışmasıyla *Goldsmith* olacaktır. *Goldsmith, Johnson ve Post*’u “düzenleme şüphecileri” olarak adlandırdığı grubun önde gelenleri ilan ederek özellikle hedefe aldığı makalesinde,⁴²¹ öncelikle şüphecilerin iddialarını toparlamış ve ardından siber uzayın ulusal ve uluslararası düzenlemelere tabi tutulmasının neden mümkün ve meşru olduğunu izah etmeye girişmiştir. Yazar, siber uzayın özgün ve sınır aşan ilişki biçimleri üzerinde yargı yetkisi kurmanın güçlüğüne kabul etmiş fakat ticari tahkim sistemini örnek göstererek uygun hukuk rejiminin tespitinin imkânsız olmadığını savunmuştur.⁴²² Tahkimde esas olan “ taraflar arasındaki tahkim sözleşmeleri”, “ulusal tahkim kanunları” ve “uluslararası uygulama antlaşmaları”⁴²³ şeklindeki üç katmanlı ilişki; çok uyruklu, sınır aşan ve kendine has kuralları bulunan ticari ilişkilerin çözümü için muteber bir mekanizma oluşturmuştur ve benzer özellikler taşıyan siber uzay için de esas alınabilecek niteliktedir.⁴²⁴ Bu şekilde örneklendiği üzere, gerçek uzayda da ulus-üstü ve sınır aşan işlemler gerçekleşmektedir. Yazara göre siber uzaydaki işlemler de bunlardan farklı değildir. Siber uzayın devletlerce düzenlenmesi belki bir miktar zorlayıcı olacaktır fakat gerçek uzaydaki benzer nitelikli işlemlerin düzenlenmesinden daha zor da olmayacaktır.⁴²⁵

Lessig de Johnson ve Post’un görüşlerini eleştirenler arasındadır. *Lessig*’e göre siber uzayın ayrı bir yer olduğu, özgün dinamikleri olduğu ve yeni bir hukuk doğuracağı doğrudur fakat siber uzay ve gerçek uzay, dahillerinde işlenen fiillerin sonuçları ve failleri itibariyle birbirinden mutlak bağımsız değildir.⁴²⁶ Ayrıca her ne kadar siber uzayın yapısı gereği devletlerin düzenlemeleri az ya da çok etkisiz kalıyor olsa da bir düzenlemenin “yeterince” etkili sayılması için “mutlak” olarak etkili olmasını aramak doğru olmayacaktır.⁴²⁷ Siber uzayın mimarisini oluşturan kodun düzenleyici ve bağlayıcı yönüne burada tekrar değinen *Lessig* özetle; bir “siber uzay hukukunun” mümkün

⁴²¹ Jack L. Goldsmith, “Against Cyberanarchy”, *The University of Chicago Law Review*, Vol.65, No.4, (1998), s.1199.

⁴²² Ibid., s.1246.

⁴²³ En önemli örnek olarak 1958 tarihli “Yabancı Hakem Kararlarının Tanınması ve İcrası Hakkındaki New York Sözleşmesi” verilmiştir

⁴²⁴ Goldsmith, ss.1246-1247.

⁴²⁵ Ibid., s.1250.

⁴²⁶ Lawrence Lessig, “The Zones of Cyberspace”, *Stanford Law Review*, Vol.48, No.5, (1996), s.1404.

⁴²⁷ Ibid., s.1405.

olduğunu, bunun da başta kodu düzenleyecek gerçek uzay normlarıyla en verimli şekilde yapılabileceğini ifade etmiştir.⁴²⁸

Johnson ve *Post*'un görüşlerine yönelik bir cevap da *Wu*'dan gelmiştir. *Wu* “siber uzay egemenliği” kavramını ele alarak, kavramın “siber uzayın, ulus-üstü ve sınır aşan yapısı gereği ‘ülkesel’ nitelikteki devletlerin egemenliğinden vareste olduğu ve devletlerin, siber uzayın kendi kurallarına saygı göstermesi gerektiği” kabulünü içinde taşıdığını ifade etmiştir.⁴²⁹ Bu görüşün ancak internetin devlet tarafından düzenlenmesinin imkansızlığı ya da anlamsızlığı durumunda makbul olabileceğini savunan yazar, iki soru yöneltmiştir: “ulus devletlerin interneti düzenlemesi mümkün müdür”; “eğer mümkünse ulus devletler interneti düzenleyecek midir”.⁴³⁰ *Wu*'nun görüşleri de *Lessig* ile paralel niteliktedir. Yazar, sözgelimi yasaklanan bir şeyin tamamen imkânsız hale getirilemese dahi zorlaştırılmasının da hukuken bir kazanım olacağını; devletlerin, siber uzayın fiziksel ve mantıksal boyutlarını oluşturan unsurlara bu minvalde müdahale edebileceğini; bu müdahaleye açıklık durumunun da siber uzayı -hem içerik açısından hem dahilinde işlenen fiiller açısından- devletlerce düzenlenebilir kıldığını ileri sürmüştür.⁴³¹ Devletler, internet sistemine katılmak suretiyle, teknik şartlar ve protokoller dahil olmak üzere bir dizi kuralı kabul etmektedirler; fakat egemen devletin interneti ancak kendi çıkarlarına hizmet ettiği sürece özgür bırakacağını ve her devletin bu mutabakatı farklı bir seviyede kabul edeceğini söylemek de yanlış olmayacaktır.⁴³² *Wu*'ya göre sonuç olarak internet düzenlenebilir ve gerek devletler gerek şirketler gerek kişiler bu düzenlemeleri halihazırda gerçekleştirmektedirler.⁴³³

Buraya kadar bahsi geçen metinlerde siber uzayın genel olarak internetle özdeşleştirilmesi, klasik dönemin mekânsal bakışının bir yansımasıdır. Arka planındaki kabule göre; siber uzay bir mekân ise bu mekânı “ağlar ağı” olan internet oluşturmaktadır ve mekâna giriş, internete bağlanmak suretiyle gerçekleşmektedir.

⁴²⁸ Ibid., s.1408.

⁴²⁹ Timothy S. Wu, “Cyberspace Sovereignty? – The Internet and the International System”, **Harvard Journal of Law and Technology**, Vol.10, No.3, (1997), s.648.

⁴³⁰ Ibid., s.649.

⁴³¹ Ibid., ss.649-655.

⁴³² Ibid., s.558 vd.

⁴³³ Ibid., s.665.

Ağdaş ve siber hukuk gibi kavramların siyasal bir topluma atıfta bulunduğu düşünülebilir. Bu bağlamda, siber uzayın bir mekân ve siber uzayda eylemde bulunan insanların bir toplum olarak kabulüne binaen bu mekân ve toplum üzerinde geçerli özerk bir hukuk sisteminden söz edilmesi de eleştiriye uğramıştır. *Stein*, siber uzaydaki topluluğun hukuk inşa edecek ve bu yönüyle özerklik iddia edebilecek bir toplum olmadığını ifade etmiştir. Dinin ya da bir inancın mensupları yahut birden fazla ülkede yaşayan aynı etnik kökene sahip gruplar gibi örneklerde görüleceği üzere; gerçek uzayda da coğrafi sınırlardan bağımsız şekilde var olan topluluklar mevcuttur. Siber uzaydaki insanlar ise bunlardan farklı olarak ortak otorite, inanç, ideoloji, etnisite, tarih vs. hususları paylaşmamaktadır. Tamamen siber uzayın sağladığı çok geniş yelpazedeki imkanlardan faydalanmak için tesadüfen bir araya gelen ve birbirleriyle büyük ölçüde alakasız olan bir kalabalık görüntüsündedir. *Stein* bu durumu, ilgili topluluğun, İslam Ümmeti’ni değil, telefon kullanıcılarının alemini çağrıştırdığı tespitiyle betimlemiştir.⁴³⁴ Bu yaklaşım bir taraftan da aynı dönemde dile getirilen “siber ulus (*cybernation*)”⁴³⁵ düşüncesine karşı cevap niteliğindedir.

Shapiro, siber uzay kavramına ilişkin muhalif düşüncelerini serdederken tabii olarak *Johnson ve Post*’a yönelik eleştirilere de dahil olmuştur. Şayet siber uzay, gerçek dünyadan ayrı bir yer olarak tanımlanacaksa siber uzay hukuku da bir anlamda ayrı bir yerin hukuku (*law of another place*) olarak kabul edilecektir. Bu durum da New York Eyaleti veya Birleşik Krallık gibi “yer”lerin kendi hukuklarına sahip olmasına benzeyecektir.⁴³⁶ *Shapiro*, yazı ya da telefon kullanımı gibi iletişim metotlarına atıf yaparak; bilgisayar ağları üzerinden gerçekleşen iletişimin bunlardan farklı ele alınıp sanki gerçek dünyadan ayrı bir yerde yaşanıyormuş gibi kabul edilmesi şeklinde yorumladığı yaklaşımın, en kötü haliyle “siber romantizm” olduğunu iddia etmiştir.⁴³⁷ Yazara göre siber uzay özerk ve egemen bir alan değildir; New York’ta olan hukuk gibi bir siber uzay hukuku söz konusu olamayacaktır.⁴³⁸

⁴³⁴ Allan R. Stein, “The Unexceptional Problem of Jurisdiction in Cyberspace”, *The International Lawyer*, Vol.32, No.4, (1998), s.1173.

⁴³⁵ Rusch, s.592.

⁴³⁶ Shapiro, s.708.

⁴³⁷ Ibid., s.709.

⁴³⁸ Ibid. s.717.

5. Lex Mercatoria ve Siber Uzay

Reidenberg, yukarıda ilgili yazarların öne sürdüğü “kodun normatif gücü” ve “siber hukuk” gibi yaklaşımları bir potada eritmiştir. Yazar, siber uzayda geçerli olacak hukukun yegâne kaynağının devlet düzenlemeleri olmadığını; teknolojik yeterliliklerin, sistem tasarımının, yerleşik standartların ve hatta kullanıcı tercihlerinin dahi siber uzayın unsurları üzerinde kurallar ihdas edebileceğini savunmuştur.⁴³⁹ Bu kural setinin de tarihte “tüccarların sınır aşan faaliyetlerinde normatif yeknesaklığı sağlamak adına kendi aralarında muteber ve devletlerin hukuklarından özerk kıldıkları bir hukuk rejimi” olarak ifade edilebilecek “*Lex Mercatoria*” örneğine atfen “*Lex Informatica*” adıyla kabul görebileceğini ileri sürmüştür.⁴⁴⁰ *Lex Informatica*, devletlerin hukukunu dışarıda bırakmamaktadır. Hukuk ve *Lex Informatica* arasında karşılıklı etkileşime dayalı bir ilişki söz konusu olacaktır. İki düzen de kudret ve kabiliyetleri oranında bir diğerini şekillendirecektir.⁴⁴¹ *Reidenberg*’in teorisi de siber uzayın sanal bir dünya olduğu kabulü üzerine inşa edilmiştir. Bir çeşit siber uzay teamül hukuku olarak da ifade edilebilecek yaklaşım, sistem mimarisinin zorunlu kıldığı kurallar dikkate alındığında tabiat kanunlarıyla da özdeşleştirilebilecektir. Burada kritik nokta şudur ki; siber uzayı inşa eden fail tek bir kişi değildir. Siber uzayın mimarisi, kanun mesabesinde olsa dahi inşası itibarıyla kolektif bir ürün olduğu için, tanrısal vasıflar taşıyan bir mimardan bahsedilemeyecektir. Dolayısıyla siber uzayın “tabiat kanunlarının” yine hukukun etki alanında şekilleneceğini söylemek makul olacaktır. Nitekim *Reidenberg*’in teorisiyle aynı yılda yayımlanan eserinde *Perritt*, siber uzayda var olmak isteyen sibernetların (*cybernaut*) uymak zorunda olduğu siber uzayın kendi kendini yönettim (*self-governance*) kurallarını, *Reidenberg* ile benzer şekilde *Lex Mercatoria* ile özdeşleştirip, bu tür bir rejimin varlığının ancak uluslararası ilişkilerin ve dolayısıyla hukukun gelişimine fayda sağlayacağını belirtmiştir.⁴⁴² Döneminde revaçta olan, internetin gelişiminin devlet egemenliğini tehdit ettiği düşüncesine meydan okuyan *Perritt*; teknolojik gelişmelerin uluslararası hukuku ve ilişkileri, ekonomide karşılıklı bağımlılığı ve küresel sorunlara

⁴³⁹ Joel R. Reidenberg, “Lex Informatica: The Formulation of Information Policy Rules through Technology”, *Texas Law Review*, Vol.76, No.3, (1998), ss.554-555.

⁴⁴⁰ Ibid., ss.553-554. Bu yaklaşım, *Goldsmith*’in örnekleriyle de paralellik taşımaktadır.

⁴⁴¹ Ibid., s.585.

⁴⁴² Henry H. Perritt Jr., “The Internet as a Threat to Sovereignty? Thoughts on the Internet’s Role in Strengthening National and Global Governance”, *Indiana Journal of Global Legal Studies*, Vol.5, Iss.2, (1998), s.427 vd.

çözüm arayacak sivil toplumu geliştireceği görüşünü de savunmuştur.⁴⁴³ İnternetin devlet egemenliği altında yönetimine dair zorlukların da farkındadır fakat bu durumun egemenliğe hâlel getirmeyeceği; aksine üzerinde devlet politikalarının işletilerek geliştirilmesi adına bir fırsat teşkil ettiği düşüncesindedir.⁴⁴⁴ Yazar ayrıca aynı dönemdeki bir başka çalışmasında, internetin gerek ulusal hukuklar gerek uluslararası hukuk için sağladığı yerel ve küresel etkileşim imkanlarıyla hukuka ve yönetime yabancılaşmanın önüne geçileceği, nihayetinde ise genel anlamda hukukun internet sayesinde gelişip güç kazanacağı öngörüsünde bulunmuştur.⁴⁴⁵

C. Modern Dönem

Klasik dönemde bir yandan siber uzayın ayrı bir mekân ve devletlerin egemenliğinden bağımsız bir alan olduğuna yönelik görüşler ileri sürülürken; diğer yandan bilgisayar ve internetin yaygınlaşmasıyla yargı uygulamasındaki tablo netleştikçe, siber uzayda devletlerin hukuk icrasının mümkün olduğuna ve bu hukukun niteliğine yönelik çalışmalar kuvvet kazanmıştır. Siber uzayın kendi hukuk sistemine sahip olacağına yönelik düşüncenin özellikle hukukçu yazarlarca ağır şekilde eleştirilmesi, siber uzaya ilişkin hususların genel hukuk teorisi içerisinde değerlendirilerek, günümüzde varlığı genel kabul gören “bilişim hukuku” disiplininin oluşmasına giden yolu açmıştır. Birinci Bölüm’de anlatılan, siber uzayın tanımlanmasında kabul edilen yaklaşımların değişimine paralel şekilde, siber uzayın mekansallığı, uzay olmaklığı ve hukuka konu edilme biçimi gibi başlıklardaki düşünceler de değişime uğramıştır. Modern dönemin öne çıkan özelliği; insanın siber uzay ile etkileşiminin dramatik bir hızla artıp yaygınlaşması sonucunda temel ilkelerin belirginleşmesi ve daha somut hukuki meselelerin ele alınmasıdır.

1. Kodun Gücü

Modern dönemin ayak sesleri, siber uzayın düzenlenmesinde kodu ve mimariyi işaret eden eserlerle duyulmuştur. Köken itibarıyla anayasa hukukçusu olan ve kendini

⁴⁴³ Ibid., s.424.

⁴⁴⁴ Ibid., s.432.

⁴⁴⁵ Henry H. Perritt Jr, “The Internet is Changing International Law”, *Chicago-Kent Law Review*, Vol.73, Iss.4, (1998), ss.1049-1054.

de anayasacı (*constitutionalist*) olarak tanımlayan Lessig'in "Kod ve Siber Uzayın Diğer Yasaları" başlıklı eseri; siber uzayın klasik telakkisinin pratikte karşılığının kalmadığını ilan etmesi ve siber uzaydaki fiiller üzerinde düzenleyici etkisi olan unsurları ele almasıyla modern dönem düzenlemeciliğinin öncülerinden kabul edilebilir. Yazarın üzerinde durduğu esas nokta, siber uzayın verili bir tabiatının olmamasıdır. Siber uzay, donanımların ve bunlar üzerinde işleyen yazılımların tasarım ve kapasiteleriyle şekillenmektedir. Sonuç itibarıyla bunlar da tabiat kanunlarına tabi olsalar dahi doğal olarak var olmamışlar ve insan tarafından sonradan üretilmişlerdir. Kodu yazanlar nasıl bir mimari kurgularsa siber uzay da o yönde şekil alacaktır. Lessig bu tespiti şöyle ifade etmiştir.⁴⁴⁶

"Gerçek uzayda hukukların anayasalar, tüzükler ve diğer hukuki metinler aracılığıyla nasıl düzenleme yaptığını biliyoruz. Siber uzayda da kodun nasıl düzenlediğini anlamalıyız; siber uzayı siber uzay yapan yazılım ve donanımın, siber uzayı olduğu gibi nasıl düzenlediğini. William Mitchell'in ifadesiyle bu kod siber uzayın "yasası"dır. Kod, yasadır.

Bu kod, liberal ya da liberteryen idealler için en büyük tehdidi ve aynı zamanda en büyük vaadi oluşturmaktadır. Temel olduğuna inandığımız değerleri korumak için siber uzayı inşa edebilir, tasarlayabilir veya kodlayabiliriz; ya da bu değerlerin yok olmasına izin verecek şekilde siber uzayı inşa edebilir, tasarlayabilir veya kodlayabiliriz. Bunun ortası yoktur. Bir tür inşa içermeyen hiçbir seçenek yoktur. Kod, keşfedilmemiştir; o yalnızca üretilir ve yalnızca bizim tarafımızdan üretilir. Mark Stefik'in de belirttiği gibi; "[Siber uzayın] farklı versiyonları, farklı türden hayalleri destekler. Akılcıca olsun ya da olmasın; biz seçeriz".

Lessig, kodun fonksiyonunu izah etmek adına Chicago ve Harvard üniversitelerinde bulunan ağ yapıları arasındaki farklılıkları örnek göstermiştir. Chicago ağına (Lessig, internetin klasik dönemindeki haline atıfla Net95 olarak isimlendirmiştir) herhangi bir kişinin herhangi bir cihazla bağlanabilmesi ve anonim olarak eylemde bulunabilmesi mümkünken; Harvard ağına erişmek için üniversite mensubu olmak ve bağlanacak cihazı kaydettirmek gereklidir. Ayrıca Harvard ağında anonim olarak bulunmak mümkün değildir; erişim ve etkileşimler de kayıt altındadır.⁴⁴⁷ İki ağ arasındaki farklılıklar tasarımlarından kaynaklanmaktadır. Tasarımı oluşturan ise koddur. Siber

⁴⁴⁶ Lawrence Lessig, *Code and other Laws of Cyberspace*, New York: Basic Books, 1999, s.6.

⁴⁴⁷ Ibid., ss.26-27.

uzayda kodun nasıl yazılacağını ve tasarımın nasıl yapılacağını düzenlemek mümkündür. *Lessig*, bir canlının davranış ve kararlarını etkileyen dört dış unsurun varlığından bahsetmiştir. Bunlar; hukuk, sosyal normlar, piyasa ve mimaridir.⁴⁴⁸ Aynı unsurlar siber uzayda da benzer kuvvete sahiptir. Kod ise “mimarinin analogudur”.⁴⁴⁹ Yazılım ve donanımların sağladığı imkân ve kısıtların, siber uzaydaki davranışlar üzerinde düzenleyici etkisi bulunmaktadır.⁴⁵⁰

Koda dikkat çeken teoriler siber uzayın düzenlenmesinde önemli bir ayrımı tespit etmiştir. Hukukun konusu sadece siber uzaydaki fiiller ve failler değildir. Siber uzayın yapısal özellikleri insan eliyle belirlenmektedir ve dolayısıyla bu özelliklerin belirlenmesi de hukuk kurallarına tabi tutulabilecektir. Gerek doğrudan fiiller ve failler üzerinde gerek mimari üzerinde yapılacak hukuk; isabetinden, etkisinden ya da verimliliğinden bağımsız olarak mümkün bir hukuktur. Yazılımın ve donanımın yapısı hukukun öngördüğü şekilde tasarlandığı takdirde, siber uzayda faaliyet gösteren kişilerin eylemleri de buna göre şekillenmek durumunda olacaktır. Böylece kurallara uyum, polis ve mahkeme gibi devlet unsurları tarafından ihlal sonrası (*ex-post*) sağlanmasındansa; son kullanıcının ihlalini oldukça zorlaştırarak önceden (*ex-ante*) sağlanacaktır.⁴⁵¹

Siber uzayın mimarisine yönelmek, nasıl tasarlanması gerektiği sorusunu doğuracaktır. *Rusch*, alanında şöhret sahibi olmuş eserinde, siber uzayda çitlerin hangi ilkeye göre çekileceğini sorgulamıştır.⁴⁵² Sorgulamasını da iki farklı hukuk yaklaşımının kıyası üzerinden analogiyle yapmıştır. İspanyol hukuk geleneğinde çiftçilerin sığırları dışarıda tutmak için arazilerini çitle çevirmeleri gerektiği; İngiliz örf ve âdet hukukunda ise hayvan sahiplerinin hayvanlarını çitle çevirerek kontrol etme yükümlüğü olduğu kabul

⁴⁴⁸ Ibid., s.88.

⁴⁴⁹ Fiziksel dünya ile kıyasla yazılımcının siber uzayda mimar, inşaatçı, müteahhit ve aynı zamanda iç mimar olduğunu düşünen *Katsh* ve bilgisayarlarla inşa edilmiş mikro dünyaları yöneten kuralların, insanın fiziksel arayüzler vasıtasıyla etkileşime geçtiği programların kaynak metinlerinde tanımlandığı gerekçesiyle kodun yasa olduğu fikrini savunan, kendisi de gerçek manada bir mimar olan *Mitchell* bu düşüncenin öncülerindendir; M. Ethan Katsh, “Software Worlds and the First Amendment: Virtual Doorkeepers in Cyberspace”, **University of Chicago Legal Forum**, Vol.1996, Iss.1, (1996), s.340; Willam J. Mitchell, **City of Bits: Space, Place, and the Infobahn**, MIT Press, 1995, s.111.

⁴⁵⁰ Lessig, 1999, *Code and...*, s.89.

⁴⁵¹ Primavera De Filippi ve Samer Hassan, “Blockchain Technology as a Regulatory Technology From Code is Law to Law is Code”, **First Monday**, Vol.21, No.12, (2016), Introduction; <https://firstmonday.org/ojs/index.php/fm/article/view/7113/5657> (31.12.2024).

⁴⁵² Yazar ayrıca bir klasik dönem tartışması olarak kalan, siber uzayda çitlerin olamayacağı iddiası için “artık çok geç” olduğunu vurgulayarak; insanların tıpkı çevrimdışıyken çocuklar, kişisel veriler ve mahremiyet gibi hususları koruma sebepleri olduğu gibi çevrimiçiyken de bunların geçerli olduğunu savunmuştur; *Rusch*, s.587.

edilmiştir.⁴⁵³ Yazar, içeri alma (*fencing in*) ve dışarıda bırakma (*fencing out*) olarak ifade ettiği bu yaklaşımların siber uzaydaki karşılığını değerlendirecektir. Öncelikle çocukların internetteki cinsel içeriklerden korunması örneği üzerinden hareket etmiştir.⁴⁵⁴ Ebeveynlerin çocukları zararlı içerikten koruma ve bunun için önlemler alma yükümlülüğü, genel kabul görmüş bir esastır; bu esas, zararlı içeriğin “dışarıda bırakılması” anlamına gelir. Fakat içerik sağlayıcıların da bu tür içerikleri çocukların erişimini engelleyecek şekilde “içeri alma” yükümlülüklerinden de bahsedilmesi gereklidir. Bu yükümlülük, fiziksel uzayda faaliyet gösteren ve yetişkinlere yönelik ürünler satan mağazaların çocukların erişimine izin vermeyecek şekilde tasarlanıp çalışmasına benzer. Yapılması gereken, siber uzay mimarisinin -olabildiğince etkili şekilde- buna göre tasarlanmasıdır. *Rusch* ayrıca dolandırıcılık ve ısrarlı takip (*stalking*) gibi siber suçlar için de filtreleme gibi önlem örnekleri üzerinden aynı mekanizmanın işletilebileceğini savunmuştur.⁴⁵⁵

Rusch’un, siber uzayın ayrı bir mekân olarak kabulünün siber uzay için özerk bir siber hukuk ihtiyacı kabulünü de bünyesinde barındıracağına ilişkin görüşüne yukarıda değinilmişti. Aynı zamanda yine yukarıda görüldüğü üzere, düzenlemeci ve özgürlükçü tarafların siber uzayı ayrı bir mekân olarak görmekte genelde mutabık oldukları da bir gerçektir. *Rusch* ise bu yaklaşımı eleştirmiştir. Siber uzayı fiziksel uzaydan ayrı ve özgün kanunları olan bir mekân olarak kabul etmenin ampirik destekten yoksun olduğunu ileri sürmüştür.⁴⁵⁶ Öncelikle siber uzay, varlık ve işleyiş olarak fiziksel uzayın bir parçasıdır ve gerçek dünyaya hâkim olan fizik kurallarıyla mükemmel bir uyum içindedir. Diğer yandan, insanların davranışlarını belirleyen psikoloji ilkeleri de çevrimiçi ve çevrimdışı davranışları için değişiklik arz etmemektedir. Fiziksel ve psikolojik esaslar üzerinden iddiasını destekleyen yazar, gerçek uzayda geçerli olan hukukun siber uzayda da uygulanabileceği ve burada çitlerin nasıl çekileceğini de belirleyebileceği sonucuna varmıştır.⁴⁵⁷

⁴⁵³ Ibid., s.583.

⁴⁵⁴ Ibid., ss.587-588.

⁴⁵⁵ Ibid., s.589.

⁴⁵⁶ Ibid., s.592.

⁴⁵⁷ Yazarın bu kurgusundan anlaşılacağı üzere siber uzayda çekilecek çitler mecazen ifade edilmiştir. *Rusch*, sanal bir mekândaki sanal çitleri kastetmemiştir. Analogilere sıkça başvursa da siber uzaya aslında realist yaklaştığını söylemek mümkündür.

Kodun düzenleyici gücü, devletin hukuk vasıtasıyla kodu düzenleyebileceği ve böylece siber uzayda devlet egemenliğinin sağlanacağı sonucuna yazarları ulaştırabilirken; siber uzayın hukuki özerkliğini savunanlar için de kodun ve mimarının asli hukuk kaynağı olarak görülmesine gerekçe olmuştur. *Netanel*, “siberyalılar (*cyberians*)” olarak adlandırdığı bu yazarların görüşlerini analiz ederek eleştirmiştir.⁴⁵⁸ *Netanel*’e göre kod ve siber uzayda geçerli sosyal normlar, siber uzaydaki ticaret ve insan etkileşimi olanaklarını belirleme açısından devletlerin çıkardığı kanunlarla hemen hemen aynı etkiye sahiptir.⁴⁵⁹ Siberyalıların özerkliğin daha verimli olacağı ve siber uzayın devletlerce düzenlenemeyeceği iddialarına literatürde çokça cevap verildiğini hatırlatan *Netanel*, kendi cevabını ise “liberal mükemmellik iddiası” olarak adlandırdığı siberyalı argümanına karşı inşa etmiştir.⁴⁶⁰ Kodun ve siber uzaydaki sosyal normların başlı başına bir hukuk kuracağı düşüncesiyle siber uzayın devlet düzenlemesinden azade tutulması ancak çoğunlukçu, eşitsizlik doğurucu ve mahremiyet ihlallerine kapı açıcı bir düzen ile sonuçlanacaktır.⁴⁶¹

Netanel’in anlatısında, bir modern dönem özelliği olarak, kodun normatif fonksiyonlarının yanı sıra sosyal-siyasal inşa fonksiyonuna da önem verilmiştir. Kod ve mimarının hukuk normlarıyla -hiyerarşik olsun ya da olmasın- bir ilişki içerisinde olması kaçınılmazdır. Bu ilişkiye hâkim olacak modelin tercihi, sadece hal ve fiillerin hukuki hükümlerini belirlemekle kalmayacak; siber uzayın sosyal-siyasal yapısını da belirleyecektir. *Lessig* de bu gerçeğe fikri mülkiyet üzerinden değinerek; Web’in kuruluşundan itibaren fikri mülkiyeti dışarıda bırakan doğasının, geline nokta yoğun hukuk müdahalesiyle yok edilmek üzere olduğu eleştirisinde bulunmuştur. Bu, siber

⁴⁵⁸ Siber uzayın etki alanının genişlemesi, gerçek uzaydaki hal ve fiillerin giderek artan şekilde siber uzayda da karşılık bulmasına neden olmuştur. Devletler de doğal olarak çözümü gerçek uzay için ihdas ettikleri hukuk normlarını bu hal ve fiiller üzerinde uygulamakta bulmuştur. *Netanel*’in deyişiyle “siberyalılar” görüşleri bu yöntemin yanlışlığı üzerinedir. Onlar, siber uzayın özgün mimarisi ve dinamikleri sebebiyle ancak aşağıdan yukarıya oluşan bir kural setiyle düzenlenebileceği düşüncesindedirler. Siber uzay er ya da geç devletlerin yukarıdan aşağıya işlettikleri hukuk ve ağır bürokrasiden kendisini kurtaracaktır. *Netanel*, siberyalıların bu yaklaşımlarının üç temel argümana dayandığını tespit etmiştir. Öncelikle hantal devlet işleyişinden uzaklaştığı takdirde siber uzay daha iyi gelişecek ve alan tanıdığı faaliyetlerle genel refahı arttıracaktır. İkinci olarak; devletin düzenleme girişimleri beyhude kalacak, siber uzayda her zaman kanundan kaçmak mümkün olacaktır. Son olarak da özerk bir siber uzay, liberal demokratik ideallere erişmek açısından liberal demokrat bir devletten daha başarılı olacaktır; Neil W. Netanel, “Cyberspace Self-Governance: A Skeptical View From Liberal Democratic Theory”, *California Law Review*, Vol.88, No.2, (2000), ss.401-402.

⁴⁵⁹ *Ibid.*, s.400.

⁴⁶⁰ *Ibid.*, s.402.

⁴⁶¹ *Ibid.*, s.498.

uzayı öldürmek anlamına gelecektir.⁴⁶² Gerçekten de yoğun hukuki düzenlemelere ve sonuçlarına ilişkin tartışmalar, modern dönemin bir başka alametifarikası olarak görülebilir.

“Kod, yasadır” söylemi, son zamanlarda “hukuk, koddur” ifadesinin bir nebze ironik şekilde türetilmesine de kaynaklık teşkil etmiştir. Kodun siber uzay için yasa olduğu, önde gelen birçok yazarca kabul görmüş olmakla birlikte; blok zinciri ve akıllı sözleşme (*smart contract*) gibi teknolojik gelişmelerle hukukun dijitalleştiği, yani artık yasanın kod haline geleceği görüşü, bu ifadenin alt metnini oluşturmaktadır.⁴⁶³ Bu söylem aslında hukukun dijitalleşmesini ifade etmektedir. Bu noktada hukuk disiplinine düşen yeni bir yükümlülük de “hukukun dijitalleşmesinin hukuku” olarak adlandırılabilir ilke ve normlar dizisinin tespiti olacaktır.⁴⁶⁴ Bu konu literatürde “kod, yasadır” söylemine atıfla işlense de eldeki çalışmanın kapsamı dışında kaldığından böylece değinmek yeterli olacaktır.

2. Mekânsallığın Dönüşümü

Siber uzayın gerçek uzaydan ayrı bir yer olduğu varsayımı, hem bu yerin kendi hukukunu inşa etmesi gerektiği yönündeki klasik dönem siber hukuk yaklaşımının hem de devletlerin burada geçerli hukuk ihdas etmesi gerektiği yönündeki düzenlemeci yaklaşımın ortak kabulü görünümündedir. *Hunter*, yaşanan dönüşümü ve gelinen vaziyeti şu sözlerle ifade etmiştir:⁴⁶⁵

“İlk dönem akademisyenlerinden bazıları siber uzayın hukuk ve düzenleme açısından ayrı bir alan olduğunu savunmuş ancak saflıkları nedeniyle kısa sürede alay konusu olmuşlardır. Geçen yüzyılın sonuna gelindiğinde, genel kabul gören görüşe göre, hiç kimse siber uzayın bir yer olduğunu iddia edecek kadar aptal olamazdı.

Bununla birlikte, genel kabul gören anlayış; siber uzayı bir yer olarak düşünüp düşünmediğimize ilişkin tanımlayıcı soruyu, siber uzayı ulusal yasalardan bağımsız bir rejim olarak düzenlememiz gerek-

⁴⁶² Lawrence Lessig, “The Death of Cyberspace”, *Washington and Lee Law Review*, Vol.57, Iss.2, (2000), ss.346-347.

⁴⁶³ Rolf H. Weber, “‘Rose is a Rose is a Rose is a Rose’ – What about Code and Law?”, *Computer Law & Security Review*, Vol.34, Iss.4, (2018), ss.704-706; De Filippi ve Hassan, Başlık.II. Law is code;

⁴⁶⁴ Oster, hukukun “ne ölçüde dijitalleştirilebileceği” sorusu teknolojinin alanına girerken; “ne ölçüde dijitalleşmesi gerektiği” sorusunun hukukun alanına girdiğini belirtmiştir. Bunlardan ilkinin “hukukun dijitalleşmesi”, diğerini “dijitalleşmenin hukuku” olarak tanımlamıştır; Oster, s.103. Fakat aslında Oster’ın eserinde dijitalleşmenin hukuku ile kastedilen hukukun dijitalleşmesinin hukukudur.

⁴⁶⁵ Dan Hunter, “Cyberspace as Place and the Tragedy of the Digital Anticommons”, *California Law Review*, Vol.91, No.2, (2003), s.443.

gerekmediği şeklindeki normatif soruyla karıştırmıştır. Bunlar kavramsal olarak birbirinden farklı iki sorudur. Normatif sorunun cevabı ne olursa olsun, bilişsel bilim araştırmaları sadece tanımlayıcı bir gözlem olarak, siber uzayı bir yer olarak düşündüğümüze dair bol miktarda kanıt sunmaktadır. Siber uzayı bir yer olarak düşünmek yargıçları, yasa koyucuları ve hukuk akademisyenlerini, mülkiyetle ilgili fiziksel varsayımları bu yeni, soyut uzayda uygulamaya yöneltmiştir”

Gerçekten de insan algıları itibariyle metaforik yaklaşımın bir sonucu olarak siber uzayın fiziksel uzaydan ayrı bir yer gibi görüldüğü açıktır. Öyle ki insan fiziksel uzayda zorunlu olarak beden ve konum sahibi bir varlıktır. Dolayısıyla sanal iletişimi de beden ve konuma dayalı zihin filtresinden geçirerek anlayacaktır.⁴⁶⁶ *Hunter*’ın çalışmasında düşüncelerinin çağ dışı kaldığını belirttiği yazarlar ise tabii ki *Johnson* ve *Post*’tur. Dolayısıyla yönelttiği eleştiri de siber uzayın tanım itibariyle ayrı bir mekân olarak görülmesi değil; mer’i hukuk için bir istisna alanı olarak görülmesidir. *Hunter* ayrıca metafor yönteminin hukuk ciddiyetine ve belirlilik ilkesine aykırı düşeceği, sadece retorik olarak önem arz edebileceği yönündeki görüşe de karşı çıkmıştır. Zira metaforlar hukuk disiplini içerisinde birçok yerde kullanılmaktadır ve hem anlaşılabilirlik hem isabetli sonuca ulaşabilmek açısından gereklidir.⁴⁶⁷ Dolayısıyla belki siber uzay için bir hukuki özerklikten bahsetmek mümkün değildir; fakat hukukçuların, fiziksel uzayın belirlilik arz eden konularına istinaden ihdas edilmiş ve yerleşik hale gelmiş hukuk normlarını, siber uzaydaki konular üzerinde hüküm inşa ederken kullanmaları söz konusu olacaktır. Bu da söz gelimi siber uzaydaki sanal unsurlar üzerinde gayrimenkul mülkiyetine ilişkin hukuk kurallarının işletilmesi gibi sonuçlar doğurmaktadır.⁴⁶⁸

Tüketimi için rekabet yaşandığı gibi tüketimden dışlama imkânı da bulunmayan kamusal varlıkların sürdürülebilirliği sorununu konu edinen “ortak malların trajedisi” kavramı, madalyonun bir yüzü olarak kabul edilirse; diğer düzünde de “ortak olmayan malların trajedisi” bulunmaktadır. Bilhassa fikri mülkiyet tartışmaları üzerinden yükselen bu teori, tüketiminde rekabet olmayan -hatta tükenmesi söz konusu olmayan-⁴⁶⁹ bir

⁴⁶⁶ Julie E. Cohen, “Cyberspace as/and Space”, *Columbia Law Review*, Vol.107, No.1, (2007), s.213.

⁴⁶⁷ *Ibid.*, s.459.

⁴⁶⁸ *Ibid.*, s.445.

⁴⁶⁹ ABD’nin üçüncü başkanı olan Thomas Jefferson, fikirlerin ve buluşların kullanıldıkça ve paylaşıldıkça tükenmeyeceği gerçeğinden hareketle; doğanın fikirlere “hayırseverce” sağladığı bu ayrıcalığın gereği olarak fikirlerin özel mülkiyete konu edilemeyeceğini savunmuştur; Lessig, 2000, ss.337-338.

varlığın özel mülkiyete konu edilip tüketimden dışlanması sonucunda yaşanacak kolektif kaybı konu edinmektedir.⁴⁷⁰ *Hunter*'ın nihai uyarısı da siber uzayın gerçek uzaya benzer şekilde mekansallaştırılması ve içindekilerin mülkiyete konu edilmesinin ortak olmayan dijital varlıkların trajedisini doğuracağı yönündedir.⁴⁷¹ Tam da siber uzaydaki bu mülkiyet yaklaşımının hukuka yansımalarını incelemek isteyen *Olson*; klasik tabirle haneye tecavüzü ifade eden “*trespass*” kavramından hareketle bugün “bilgisayara izinsiz erişim (*computer trespass*)” şeklinde hukuk diline yerleşmiş olan eylemi “*cybertrespass*” ifadesiyle ele almıştır.⁴⁷² Siber uzaydaki bazı sanal unsurlar kimilerine göre gayrimenkul mülkiyetine ilişkin hukuk kurallarına tabi olmalı ve bunlara yönelik ihlaller gayrimenkule izinsiz giriş hükmünde olmalıydı. Siber uzayı bir mekân olarak kabul etmek, doğal olarak söz gelimi bir Web “sitesinin” de sıradan bir menkul gibi değil; bir gayrimenkul gibi değerlendirilmesi sonucuna ulaştırabilecektir.⁴⁷³ Amerikan hukuk kültüründe gayrimenkul üzerindeki özel mülkiyetin ifade ettiği anlam göz önüne alınırsa, böyle bir yaklaşımın doğuracağı radikal sonuçları öngörmek zor olmayacaktır.

Dijital unsurların fiziki varlıklarımsıçasına mülkleştirilip maliklere dağıtılması eğilimi, mekansallık açısından yeni bir metafora kapı açmıştır. *Yen*'in ortaya attığı “feodal toplum” metaforu, artık özel mülkiyete dayalı sınırların çizildiği yeni bir döneme girilmesiyle klasik dönemde kabul gören Vahşi Batı benzetmesinin geride kaldığı görüşüne dayanmaktadır. Zira yazara göre internet yönetiminde sivil toplum kuruluşlarının ve şirketlerin devletlerle yarışan iktidarları, siber uzayda bir feodal düzenin doğuşunu yansıtmaktadır.⁴⁷⁴ Esasen böyle bir teorinin doğuşu, *Hunter*'ın kaygılarına ve *Olson*'un tespitlerine gerekçe olan vakıanın bir başka sonucundan ibarettir. Siber uzayın

⁴⁷⁰ James M. Buchanan ve Yong J. Yoon, “Symmetric Tragedies: Commons and Anticommons”, *The Journal of Law and Economics*, Vol.43, No.1, (2000), s.3.

⁴⁷¹ *Hunter*, s.513; Günümüzde, internet erişimine açılma imkânı bulunmasına rağmen spor müsabakalarının kayıtları, geçmiş dergi sayıları, işitsel ve görsel medya içerikleri gibi birçok kültür varlığına; telif koruma sürelerinin uzunluğu, hak sahibi veya varisi tespit edilemeyerek “yetim eser” durumuna düşmesi, hak sahiplerinin ilgisizliği, unutkanlığı veya dijitalleştirme maliyetine katlanmak istememesi gibi birçok sebeple herhangi bir şekilde ulaşılması mümkün olamamaktadır. Dijitalleşmiş eserlerin “tükenmesinin” söz konusu olmadığı mevcut şartlarda mevzubahis durum, -basit bir nostalji kaygısının ötesinde, kültür mirasının aktarımına olumsuz etkisi bakımından- ortak olmayan malların trajedisini yansıtmaktadır. Diğer taraftan, erişilebilir nitelikteki bazı dijital içeriklerin de birtakım erişim zorlukları ve kullanım engelleri nedeniyle tüketimden dışlanması da bu kapsamdadır.

⁴⁷² Kathleen K. Olson, “Cyberspace as Place and the Limits of Metaphor”, *Convergence – The International Journal of Research into New Media Technologies*, Vol.11, No.1, (2005), s.12.

⁴⁷³ *Ibid.*, s.14.

⁴⁷⁴ Alfred C. Yen, “Western Frontier or Feudal Society?: Metaphors and Perceptions of Cyberspace”, *Berkeley Technology Law Journal*, Vol.17, No.4 (2002), s.1232 vd.

devlet egemenliğine konu oluş hikayesi de mekânsallaşmadan ve mülkiyet yaklaşımlarından bağımsız düşünülemez.

Lemley, siber hukuk savunucularının siber uzayda özerk bir hukuk rejimi inşası gerekliliği iddialarına dayanak olarak gösterdikleri, siber uzayın ayrı bir mekân olduğu kabulünün ironik bir sonuç doğurduğuna işaret etmiştir. Zira *Hunter*'ın da ele aldığı üzere gelinen noktada devletler, mevcut geleneksel hukuk normlarını siber uzayda uygulamaya girişmiş ve bunu da siber uzayı bir mekân olarak kabul ederek analoji yapmak suretiyle gerçekleştirmiştir.⁴⁷⁵ *Lemley*'in siber uzaya “realist” yaklaşan tarafta olduğunu söylemek mümkündür. Yazar, siber uzayı bir mekân olarak görmenin ve internet özelinde ortaya çıkan konularda hukuk uygularken metaforlara başvurma mantıksal hatalar doğuracağını ileri sürmüştür. Örnek olarak, bir kullanıcının bir Web sitesini “ziyaret etmesi” aslında gerçek değildir. Kullanıcı, sağlayıcıya bir talep gönderir ve sağlayıcı, kullanıcıya veri ile dönüş yapar. “Ziyaret edilen” Web sitesi aslında bu verilerdir.⁴⁷⁶ *Lemley*'in konu hakkındaki görüşleri ve tespit ettiği hususlar dikkat çekicidir.⁴⁷⁷

“Belki de Hunter haklıdır ve kendimizi interneti mekânsal terimlerle düşünmeye o kadar şartlandırmışızdır ki artık geri dönüşü yoktur. Bu doğru olsa bile, siber uzay ile fiziksel dünya arasında bire bir örtüşme olduğunu körü körüne kabul etmemiz gerektiği anlamına gelmez. İşlerin fiziksel dünyada işleyiş şekli ile çevrimiçi işleyiş şekli arasında bariz farklar vardır. İşte sadece birkaç örnek:

-Fiziksel dünyada aynı anda sadece tek bir yerde bulunabilirken, internette ben -ya da en azından verilerim- aynı anda her yerde olabilirim (ve aslında bunu yapmaktan kaçınmak çoğu zaman zordur).

-Fiziksel mağazalar, mağazaya girebilecek müşteri sayısını sınırlayan mekânsal kısıtlamalara sahiptir. Bir web sitesinin veya internetin kendisinin eşzamanlı kullanımında bazı kısıtlamalar olsa da çoğu kullanıcı ve çoğu amaç için bant genişliği etkin bir şekilde sonsuzdur.

-Fiziksel mekânlar birbirlerine yakın yerlerde bulunur ve insan duyuları yan tarafta neler olduğunu algılayabilir. Buna karşın siber uzayda “kapı komşusu” yoktur. Belirli bir internet alanında meydana gelen davranışların gözlemlenebileceği halka açık bir cadde veya kaldırım da yoktur.

-İnternetin içeriği sadece bilgidir ve bilgi bir kamu malıdır. Bir web sitesinin kopyalanması önemsizdir ve kopyalanması, onu oluşturan orijinal sitenin kullanımından mahrum bırakmaz. Buna karşın,

⁴⁷⁵ Mark A. Lemley, “Place and Cyberspace”, *California Law Review*, Vol.91, No.2, (2003), s.521.

⁴⁷⁶ Ibid., s.524.

⁴⁷⁷ Ibid., ss.525-526.

menkul malların kopyalanması çok daha zordur ve gayrimenkul malların kopyalanması tanım gereği imkansızdır. Bir başkasının gayrimenkulünü kullanabilmek için, onu gayrimenkul üzerindeki kontrolünden mahrum bırakmam gerekir.”

Sonuç itibariyle *Lemley*'in, metaforun genel gerekliliğini kabul etmekle birlikte; siber uzayın kendine has nitelikleri göz önüne alınarak yapılacak hukuki analizin metafor yönteminden daha önemli olduğunu ve siber uzayla ilişkili olduğu düşünülen hususların gerçekçi şekilde ele alınması gerektiğini savunduğu görülmektedir.

Mekansallık konusunda yukarıda arz edilen görüş farklılıklarını *Kerr*, “perspektif problemi” başlığında değerlendirmiştir. Yazara göre “dahili perspektif”, siber uzayı fiziki bir arayüz vasıtasıyla erişilen sanal bir dünya olarak kabul eder ve alışverişe gitmek, sohbet odasına katılmak, posta yollamak gibi fiziksel uzayda da karşılığı bulunan eylemlerin orada sanal olarak gerçekleştirilmesine odaklanır. “Harici perspektif” ise siber uzayı, birler ve sıfırların fiziksel unsurlar vasıtasıyla belirli protokoller kullanılarak işlenmesi sürecinin toplamı şeklinde analiz etmeye odaklanmıştır. Siber uzaya harici perspektifle yaklaşanlara göre, insanların siber uzayı zihinlerinde nasıl algıladıklarının bir önemi yoktur; asıl olan teknik işleyiş ve içeriktir.⁴⁷⁸ Yazar ise teknolojinin aslında iki internet birden doğurduğunu kabul etmiştir; birisi fiziksel, diğeri sanal.⁴⁷⁹ Siber uzay hukuka konu edileceği zaman da vakıya hangi perspektiften yaklaşıldığı önem arz edecektir. Bu ayrım bazı durumlarda varılan sonucu değiştirmeyecek olsa da usule ilişkin farklılıkların hukuk adına her zaman öncelikli mesele olarak kabulü gereklidir. Örneğin bir alışveriş sitesine erişme eylemi, dahili perspektiften ele alındığında, bir mağazayı ziyaret etmeye benzeyecektir. Harici perspektife göre ise bu eylem, bir sunucuya talep gönderip oradan bilgi almak şeklinde gerçekleştiği için; bir satıcıya telefon açıp, ondan katalog göndermesini isteyip, sonrasında gönderilen katalogu açıp incelemeye benzeyecektir.⁴⁸⁰ *Kerr*'in bu şekilde örneklediği farklılık gerçekten de hukuken düzenlenmiş fiziksel uzay olgularına göre sonradan ortaya çıkmaları itibariyle analogik yaklaşıma muhtaç olan siber uzay olgularının hukuka “nasıl” konu edileceği noktasında

⁴⁷⁸ Orin S. Kerr, “The Problem of Perspective in Internet Law”, *Georgetown Law Journal*, Vol.91, Iss.2, (2003), ss.359-360.

⁴⁷⁹ *Ibid.*, s.361.

⁴⁸⁰ *Ibid.*, s.363.

kritik bir tercih zarureti doğurmaktadır. İki perspektif arasında tercihte bulunmaktan kaçınan yazar, teknolojinin gidişatının zamanla insanların tercihlerini herhangi bir yönde şekillendireceğini öngörmekle yetinmiştir.⁴⁸¹ Eldeki çalışmanın ilerleyen kısımlarında incelenecek olan hukuki problemler ve normların da bu tercihlerin sonuçlarıyla şekillendiği görülecektir.

3. Devletin Fiziksel Cebri

Özellikle Web'in doğuşunun SSCB'nin dağılmasına denk düşmesi itibariyle; siber uzayın ve en önemli bileşeni olan internetin küreselleşme üzerindeki katalizör etkisi, klasik dönem siber hukuk düşüncesine ve küreselci yaklaşıma coşkulu bir süreç yaşatmıştır. 1990'ların düşünce dünyası, -Fukuyama'da temsil edildiği üzere- ulus devletlerin gücünün gerileyerek liberalizm temelinde küresel çapta hakimiyet kazanacak ortak bir kültür, siyaset ve hukuk anlayışına duyulan inancı beslemiştir.⁴⁸² Modern döneme dek düşünürler, teknoloji yazarları ve hukukçular nezdinde süregelen tartışmalar; siber uzayın hukuk karşısındaki pozisyonuna dair “düzenlenemez”, “ancak kendi kendini düzenleyebilir” yahut “düzenlenmemelidir” gibi yaklaşımlardan uzaklaşılması yönünde seyretmiştir.

Uygulamadaki en önemli gelişmelerden biri 2000 yılında Paris Asliye Hukuk Mahkemesi'nde (*Tribunal de Grande Instance de Paris*) görülen “LICRA v. Yahoo! Davası” olmuştur. Nazi hatıra ürünlerinin satışının gerçekleştiği Yahoo!'ya ait Web sayfasının Fransa'da yasa dışı olduğu iddiasına binaen mahkemeye yapılan başvuru ile söz konusu şirketten, bu sayfaya Fransa'dan erişilmesinin önüne geçmesi istenmiştir. Klasik dönemin kuvvetli argümanlarıyla talebe karşı çıkan Yahoo! tarafı, “imkânsızlık” savunmasını ileri sürse de hukuki süreç ilerledikçe Fransa Devleti karşısında uğrayacağı maddi zararlardan kaçınmak için, “gönüllü” olduğunu iddia ettiği bir hamleyle, ilgili sayfayı yayından kaldırmış; ayrıca sayfalara erişenleri coğrafi olarak tanımlayıp ayırt edecek bir sistemi işleyişlerine entegre edeceğini -reklam tutarlılığını sağlamak amacı

⁴⁸¹ Ibid., s.405.

⁴⁸² Fukuyama'nın “Tarihin Sonu” tezi, ilgili düşünce akımının en iddialı ürünlerinden olmuştur. Eserin, Soğuk Savaş sonucunda ilan edilen ABD modeli liberal demokrasinin zaferini küresel boyuta şamil kılma manifestosu olarak nitelendirilmesi mümkündür. Düşünce tarihinde bu yaklaşım genellikle diyalektik yöntemle karşı pozisyonundaki Huntington'a ait “Medeniyetler Çatışması” teziyle birlikte ele alınmaktadır; örnek olarak bkz.; Seifudein Adem Hussien, “On the End of History and the Clash of Civilization: A Dissenter's View”, *Journal of Muslim Minority Affairs*, Vol.21, No.1, (2001), s.25 vd.

taşıdığını belirterek- ilan etmiştir.⁴⁸³ Meşhur düzenlemeci yazarlar *Goldsmith* ve *Wu*, Yahoo!’nun bu dava sonrasındaki yıllarda, Çin’de iş yapabilmek için Çin hükümetinin sansür ve jurnal taleplerini eksiksiz uygulamış olmasını alaycı ve eleştirel bir üslupla vurgulayacaktır.⁴⁸⁴ Siber uzay için ayrı ve yeni bir hukuka ihtiyaç olduğu düşüncesine kesin şekilde karşı çıkan bu yazarların, tartışmada aldıkları pozisyon aşağıdaki ifadelerle özetlenecektir:

*“Çağımız en yeni "yeni şey" arayışına saplanmış durumda. Buna karşın bizim hikayemiz eski şeylerle ilgilidir: uluslar içinde hukuk ve siyasetin eski ilkeleri, uluslar arasında iş birliği ve çatışmalar, ülke ve fiziksel cebrin (physical coercion) kalıcı önemi. Bu, Thomas Hobbes'un Bill Gates kadar önemli olduğu bir hikayedir. Hoşunuza gitsin ya da gitmesin; bu eski şeyler, Net'in gelişimi için herhangi bir teknolojik ya da entelektüel atılım kadar, hatta onlardan daha fazla önemlidir.”*⁴⁸⁵

*“Ülkesel hükümet; insanlığı çeşitliliği ile barındıran ve onun gelişmesine izin veren, insanlık tarihinin kalıcı bir gerçeğidir. İnternetin sis ve büyüünün ardında, geçerliliği kaçınılmaz olan daha eski ve daha güçlü bir düzen yatmaktadır.”*⁴⁸⁶

Yahoo! gibi döneminin en büyük internet devinin ulus devlet karşısında yaşadığı “mağlubiye” siber uzayda hukuk düşüncesi adına önemli bir kilometre taşı olmuştur. İnternetin mimarisi gereği düzenlenemeyeceğini ve işleyişine müdahale edilemeyeceğini düşünenler, devletin fiziksel cebir avantajını göz ardı etmiş görünmektedir. Zira siber uzay sadece kodlardan ve onların bir nevi sanal gerçeklik halinde algılanış biçiminden daha fazlasıdır. Siber uzayın taşıyıcı sütunu olan fiziksel altyapı, orada faaliyet gösteren gerçek ve tüzel kişiler ile onların malları, doğrudan devlet egemenliği altındadır. *Goldsmith* ve *Wu*, *Lessig* ile mutabık şekilde, davranışlar üzerinde sosyal normlar, piyasa ve mimarinin belirleyici faktörler olduğunu kabul etmiş fakat tüm bunların hukuktan, devletin ülkesel egemenliğinden ve fiziksel cebrinden azade olamayacağını savunmuştur.⁴⁸⁷ Nitekim *Lessig* de kodu ve siber uzayın diğer yasalarını ele aldığı 1999 tarihli eserini yedi yıl sonra “Versiyon 2.0” olarak güncellerken, bu iki yazarın aynı yılda

⁴⁸³ Dava süreci, ileri sürülen argümanlar ve o dönem mahkeme dışında yaşanan alakalı gelişmeler hakkında detaylı bilgiler içeren anlatım için bkz.; Jack Goldsmith ve Tim Wu, **Who Controls the Internet? Illusions of a Borderless World**, New York: Oxford University Press, 2006, ss.1-10.

⁴⁸⁴ Ibid., ss.9-10.

⁴⁸⁵ Tim Wu, “Is Internet Exceptionalism Dead?”, Berin Szoka ve Adam Marcus (Ed.), **The Next Digital Decade: Essays on the Future of the Internet** içinde (179-188), Washington, D.C: TechFreedom, 2011, s.181.

⁴⁸⁶ Goldsmith ve Wu, s.ix.

⁴⁸⁷ Ibid., s.181.

yayımlanmış söz konusu eserini, kendi argümanlarını başarıyla tamamladığını ifade ederek önsözünde selamlayacaktır.⁴⁸⁸

D. Genel Değerlendirmeler

Israrlı “siber hukuk” savunucularından *Post*’un “şakayla karışık” şerhiyle aktardığı “*mükemmel bir hukuk bilimi eserinde, her cümleinin sonunda bir dipnot bulunur; son cümle hariç*”⁴⁸⁹ görüşüne uygun şekilde, bu başlıkta kanaat bildirmek ve pozisyon belirlemek suretiyle teorik sürecin toplaması yapılacaktır.

Öncelikle tanım yapılırken belirtildiği üzere, siber uzay Web’den veya internetten ibaret değildir. Ayrıca sadece mantıksal boyuttan veya insan zihninde oluşan sanal bir gerçeklikten de ibaret değildir. Günümüzde hukuk, siber uzayı konu edinirken bu unsurlardan çok daha fazlasını kapsamaktadır.

Siber uzayın birincil sürücüsü olan “teknoloji”, tabiatı gereği sık sık “yeni” olgular doğurduğundan, siber uzay da kadim usul olan kıyasın en çok uygulandığı konulardan biri haline gelmiştir. Analoginin hukukun karşılaştığı her yenilikte ilk akla gelen yöntem olması tabii ve makuldür. Fakat bu yöntem, pratik amaçlarla, “siber uzay nedir” sorusundan ziyade “siber uzay neye benzer” sorusuna odaklanır.⁴⁹⁰ Yeni karşılaşılan olgular için “neye benzer” sorusu, hukuk adına doğru bir sorudur; fakat olgular düşüncede ve pratikte insan hayatına yerleştikçe, “ne olduğu” hakkında tanımsal çerçeve çizilecek ve genellikle müstakil normlar belirginleşecektir.

Bilgisayarın icadıyla sağlanan işlem gücü ve internetin icadıyla bu kudrete sahip cihazların birbirine bağlanması, insan zihni için klasik iletişim metotlarından çok farklı bir deneyimi doğurmuştur. Tıpkı televizyonun sadece aletlerden bir alet olduğu yönündeki “resimli tost makinesi”⁴⁹¹ ya da “radyonun resimlisi”⁴⁹² benzetmelerinde olduğu gibi siber uzayın da telefonun hatta dumanla haberleşmenin yeni bir formundan

⁴⁸⁸ Lawrence Lessig, **Code: Version 2.0**, New York: Basic Books, 2006, s.xi.

⁴⁸⁹ David G. Post, **In Search of Jefferson’s Moose: Notes on the State of Cyberspace**, New York: Oxford University Press, 2009, s.xiv.

⁴⁹⁰ Darrel C. Menthe, “Jurisdiction in Cyberspace: A Theory of International Spaces”, **Michigan Telecommunications and Technology Law Review**, Vol.4, Iss.1, (1998), s.70.

⁴⁹¹ Sunstein, s.1757.

⁴⁹² Kurtuluş Özyazıcı, “Beyazperdede Radyolu Filmler”, **TRT Akademi**, Cilt.5, Sayı.9, (2020), s.418.

ibaret olduđu yönündeki karşıt radikal görüşler, aslında bu farklı deneyimin siber uzay için düşündürdüklerine karşı bir reaksiyon niteliğindedir. İlk bakışta; “bir ekran ve çevresindeki diğer donanımlar vasıtasıyla, mesafe ve zaman mefhumlarını önemsiz hale getirecek şekilde bir satıcının ürününü inceleyip satın almak” eyleminin zihinsel karşılığı, satıcıya telefon açıp sipariş vermekten elbette farklı olacaktır. İnsanın bilişsel özellikleri bu tür deneyimleri mekâna ve zamana bağlı algılama eğilimindedir. Sonuç itibarıyla -sanal olarak- bir mağazaya “girilip” “alışveriş yapıldığı”, “orada” vakit geçirildiği varsayımı, yukarıda *Hunter*’dan aktarıldığı gibi “tanımlama itibarıyla” isabetli bir yaklaşımdır. Dolayısıyla siber uzayın orijininde *Gibson*’un kurguladığı sanal gerçeklik konseptinin yaşatılması, sosyal ve düşünsel pratikler açısından fonksiyoneldir. Fakat hukuk disiplini gündeme geldiğinde hukuka konu olacak olgunun mümkün mertebe müphemlikten uzak tutulması gerekecektir.⁴⁹³ Siber uzayın boyut ve unsurlarıyla teorileştirilmesi tam da bu bakımdan önem arz etmektedir. Kablolar ve disklerden, sanal gerçeklik cihazlarında gözlemlenen görüntülere kadar tüm unsurlarıyla siber uzay bir bütündür. Hukuk, gerek duyulduğunda bu bütünün her bir cüzü için isabetli normları ihdas ve hükümleri inşa edebilecek kabiliyete erişmekle mükelleftir. Bugün geline nokta, Web üzerinden alışveriş yapmak veya dünyanın dört bir yanından katılımcılarla video konferans gerçekleştirmek otuz yıl öncesinde olduğu kadar yeni ve şaşırtıcı değildir. Dolayısıyla siber uzayın birçok yönü için analogik dönemden çıkılıp, özgün normlar ihdas edebilecek teorik ve pratik birikim edinilmiştir. Bir Web sitesi aracılığıyla alışveriş yapmanın “neye benzediğini” düşünmektense “ne olduğunu” tespit edip kanun yoluyla düzenlemek daha isabetli olacaktır. Bunu yapmak, bir “at hukuku” ihdas etmek değildir. Ayrıca klasik anlamda siber liberteryenlikle takviye edilmiş bir siber istisnacılık (*cyber exceptionalism*) da değildir.⁴⁹⁴ Siber uzayın hukuk için yeni durumlar doğurduğunu ve bunlara yönelik özel düzenlemeler yapılması ihtiyacını kabul etmek; siber uzayı, özerk hukukunu inşa edip uygulaması gerektiğinden bahisle, devlet kaynaklı hukukun bir istisnası olarak görmekten farklıdır. Zira Bilişim Hukuku’nun (Bilgi Teknolojileri Hukuku – *IT Law*)

⁴⁹³ Örnek olarak fiziksel mağazalarda gerekli ikaz şartları sağlanmak suretiyle kameralarla müşteri hareketleri kayıt altına alınabilmektedir. Müşterinin evine katalog gönderilmesi durumunda ise müşterinin hangi ürünü ne kadar incelediği, bir üründen sonra hangi ürüne baktığı gibi birçok bilgiye erişilmesi -eve gizlice girilip takip edilmediği veya katalogla gelen bir görevlinin izin alarak izleme yapmadığı müddetçe- mümkün değildir. Alışveriş maksatlı bir Web sitesindeki ürünleri inceleyen kullanıcı hareketlerinin takibinin hukuki durumu, bu iki analogiyle farklı şekilde tespit edilecektir.

⁴⁹⁴ Clara Iglesias Keller, “Exception and Harmonization: Three Theoretical Debates on Internet Regulation”, *Humboldt Institut für Internet und Gesellschaft (HIIG) Discussion Paper Series*, 2020(2), s.14.

artık küresel kabul görmüş bir hukuk dalı haline gelmiş olması ve çok sayıda devletin siber uzaya ilişkin hususlarda özel kanunları yürürlüğe koyması, burada ifade edilen düşüncenin hayata geçişinin göstergesidir.

Mevcut durumda, uygulamadaki bütün zorluklara rağmen siber uzayın hukuk yoluyla düzenlenmesi imkânsız olarak görülmemektedir. Klasik dönemde kalan, siber uzayın “düzenlenemez” olduğu görüşü terk edilmiştir. “Siber hukuk” görüşü ise zamanla devlet kurumunun kudretiyle yüzleşip, aşağıda anlatılacak olan “küresel yönetim” konseptine doğru evrilmiştir. Özünde bizatihi kontrol ve sistem teorisine ilişkin sibernetik kavramını taşıyan siber uzayın düzenlenemez olduğunu iddia etmek artık makul görülmemektedir. Zira güncel tartışmalar da artık siber uzay “nasıl ve neye göre düzenlenmeli” sorusu üzerinde yoğunlaşmıştır. Cevabın doğal hukuka bakan kısmı hiç şüphe yok ki muhatapların inanç ve kabullerine bağlı olarak değişkenlik gösterecektir. Usul ve yöneme bakan yönü ise ilk bölümde bahsedilen iktidar ilişkilerinin bir sonucu olarak şekillenecektir. Bu noktada belirleyici olan üç ana vektör söz konusudur:

1. Siber uzayın değişken mimarisini sürekli belirleyen mimarlar topluluğu⁴⁹⁵
2. Modern egemenlik anlayışının ilke ve esaslarına dayanan devletler (temsil ettikleri uluslar)
3. Siber uzaya muhatap egemen devletlerden müteşekkil uluslararası topluluk

Kodun ve hukukun siber uzaydaki düzenleyici gücü bir bakıma rekabet halindedir. İçinde yaşadığımız fiziksel uzayın “yasası” insan eliyle belirlenmemiştir. İnsan, dünyaya geldiğinde bu yasayı verili olarak bulmuştur. Fiziksel uzaydaki mimari de bu yasaya uygun olarak insan eliyle inşa edilmiştir. Fiziksel uzayı düzenleyen hukuk, böyle bir ilişkinin sonucunda tekâmül etmiştir. *Küzeci*’nin örneklediği gibi; “*gökdeleni çalınamaz, arabayı çalınabilir kılan mimari yapılarıdır*”.⁴⁹⁶ Siber uzayda ise durum daha karmaşıktır. Siber uzayın boyut ve unsurları en başta tabii ki fizik kurallarına tabidir. Fiziksel boyut enerji, sıcaklık, basınç gibi çok sayıda kısıtla karşı karşıyadır. Mantıksal

⁴⁹⁵ Mimarın sadece “yazılımcı” olarak algılanmaması gerektiğini vurgulamakta fayda görüyorum. Yazılım geliştiricileri, cihaz üreticileri, teknoloji şirketleri, sivil toplum kuruluşları vb. aktörlerin hepsi bu mimarlar topluluğunun unsurlarıdır.

⁴⁹⁶ *Küzeci*, s.399.

boyut ve veri ise fiziksel boyutun kısıtlarına bağılı olarak vardır. Fakat burada insan eliyle belirlenebilen mimari, fiziksel uzaya göre dramatik ölçüde daha esnektir. Siber uzaydan bahsedildiğinde, fiziksel uzaydaki kesinlik ölçüsünde “gökdelenler çalınamaz” demek mümkün değildir. Özellikle siber uzayın mantıksal boyutuna bakılırsa, kod gerçekten insan eliyle kurgulanmış bir “yasa” gibi işlemektedir. Fakat hukuk öyle bir yapıdır ki insan fiillerinin tamamını kapsayabilmektedir. “Yasayı belirleyen insan fiilleri” de hukuka tabidir. Hukuk; inanç ve kabullere dayalı sosyal ve siyasi süreçler sonucunda, belli bir usul dairesinde oluşan köklü bir kurumdur. Ayrıca hukuk için şeffaflık ve belirlilik esastır; erişilmesi mümkün olmayan gizli bir hukuk kuralının bağlayıcılığından bahsedilemez. Kod ise -neredeyse- tamamen onu üreten geliştiricinin (mimarın) tek taraflı iradesinin ve fiillerinin sonucudur. Ayrıca mimar, kodu gizleyebilir ve kod bu haliyle de etkinlik vasfını yitirmez. Yine kod eğer fiilen çalışıyorsa hukuki olup olmaması da onun işlerliğini ve kullanımını etkilemez. Sonuç olarak evet; siber uzay için “kod, yasadır”. Hukukun bu yasa üzerindeki etkinliği de devletin denetim ve cebir kabiliyetlerine -yani egemenlik kaynaklı yetkilerinin bütüncül kullanımına- bağılıdır.

Siber uzayın sınır aşan yapısı, buraya kadar anlatılan iktidar ilişkisini doğal olarak uluslararası seviyeye çıkarmaktadır. Devlet egemenliğinin hayati fonksiyonu olan kural koyma ve uygulama yetkisi siber uzayı konu edineceğinde “iç yetki alanı” sınırları bulanıklaşmaktadır. Sınır aşan her hususta olduğu gibi siber uzay için de belirleyici mücadele alanı uluslararası hukuk olacaktır.

II. ULUSLARARASI TOPLULUK NEZDİNDE SİBER UZAYIN DÜZENLENMESİ VE YÖNETİMİ

A. İnternetin Küresel Yönetişimi ve Çok Paydaşlılık

Herhangi bir olguya dair ilke ve kuralların belirlenmesi, uygulanması ve denetimi muhakkak ki sosyal bilimlerin bütün alanlarına sirayet edecek genişlikte bir süreçtir. Bir şeyin düzenlenmesinin hakikati, düzenleyicinin etkin ve düzenlenenin edilgen şekilde bulunduğu basit bir emir-komuta mekanizmasından çok daha karmaşık yapıdadır. Düzenlenen perspektifinden bakıldığında; tabiat kanunları, sosyal etkiler, iktidar sahibinin belirlediği kurallar ve kuralları uygulamadaki irade ve kudreti gibi dış

faktörlerin yanı sıra; düzenlenenin irade sahibi olduğu hallerde kendi inanç ve kabulleri, sahip olduğu fiziki imkanlar, psikolojik ve bedensel durumu gibi iç faktörlerin de müdahil olduğu ve hepsinin birbirini etkilediği bir süreçten bahsetmek gerekecektir. Bu süreci çözümlmek için Sistem Teorisi’ni geliştiren sibernetiğin kurucuları, sözgelimi insan vücudunu tek tek uzuvların veya hücrelerin özellikleriyle ele almak yerine, “organizmanın organizasyonuna” yani unsurlar arası ilişkilerin bütününe odaklanmıştır.⁴⁹⁷ Böylece her bir sistemin analizi, oldukça çok-disiplinli çalışmayı gerektirmektedir. Eldeki çalışmanın kapsamı itibariyle sürecin hukuki yönünden fazla uzaklaşmamayı tercih ediyorum. Ancak hukukun, bir olgunun “idaresine” ilişkin düzenleyici fonksiyonu söz konusu olduğunda, sürece dahil olan diğer faktörlerle ve bizzat olgunun kendisiyle etkileşimini ihmal etmemek gerekecektir. Yani düzenlemeye konu olan “zavallı nokta (*pathetic dot*)”,⁴⁹⁸ aslında o kadar da “zavallı” olmayabilir. Nitekim *Murray* bu noktanın, düzenleyici seline pasif vaziyette maruz kalan bir alıcıdan ibaret görülmesinin yanlış olacağından bahseder; düzenlemeye konu olan noktalar, “düzenleyici çevrenin (*regulatory environment*)” bir parçasıdır ve bu çevre üzerinde düzenleyici faktörler kadar etki sahibidir.⁴⁹⁹

Siber uzayın düzenlenmesi gündeme geldiğinde, bunun bir devletin kendi içindeki yasama faaliyetinden ibaret kabul edilmesi, açıkça görülmektedir ki mümkün değildir. Bu durumda tabii olarak akla devletler arasındaki düzenleyici faaliyetin birincil alanı olan uluslararası hukuk gelecektir. Fakat siber uzay küresel bir olguyken uluslararası hukuk esasen “küresel” değil “uluslar-arası” niteliktedir ve bu durum siber uzayı tam kapsayacak uluslararası hukuk normlarının ihdasını güçleştirmektedir.⁵⁰⁰ Dolayısıyla uluslararası hukuk, siber uzayın yönetim ve düzenlenmesinde henüz oldukça sınırlı etkiye sahiptir. Mevcut durumu değerlendiren bazı yazarlar, siber uzaya hâkim düzenleyici çevreyi “yönetişim (*governance*)” kavramıyla açıklamayı tercih etmişlerdir.

⁴⁹⁷ Yaklaşımına dair detaylı izah için bkz. Ludwig von Bertalanffy, **General System Theory: Foundations, Development, Applications**, New York: George Braziller, 1969, s.89 vd.

⁴⁹⁸ Lessig, 2006, s.122.

⁴⁹⁹ Andrew D. Murray, **The Regulation of Cyberspace: Control in the Online Environment**, Routledge-Cavendish, 2007, s.51.

⁵⁰⁰ Kulick, s.560.

“Yönetme, çekip çevirme; güdüm, yönetim”⁵⁰¹ tanımından farklı olarak yönetim; “resmî ve özel kuruluşlarda idari, ekonomik, politik otoritenin ortak kullanımı”⁵⁰² anlamını taşımaktadır. Uluslararası İlişkiler disiplini içerisinde sıklıkla kullanılan yönetim kavramının müphemliğinden bahisle Finkelstein, “Uluslararası sistem, hiyerarşi ve yönetimden (government) yoksunluğuyla meşhur olduğundan, bunun yerine daha belirsiz bir kelime olan yönetim (governance) kullanılıyor. ...Başka bir deyişle; ‘yönetişim’ diyoruz çünkü olup bitene ne isim vereceğimizi gerçekten bilmiyoruz” ifadelerini kullanmıştır.⁵⁰³ “Küresel yönetim” ise Dingwerth’in analizine göre bir tez olarak dört iddiayı bünyesinde barındırmaktadır:⁵⁰⁴

- “1. Düzenleme, gittikçe ulusal düzeyden devlet ötesindeki politika düzeylerine kaymıştır. (Uluslararasılaşma)
2. Devlet ötesindeki yetki alanları çoğalmıştır. (Yetkinin yayılması)
3. Devlet ötesindeki düzenlemelerin dayandığı usul normları değişmiştir. (Yönetişim normlarının değişmesi)
4. Etkin ve verimli bir şekilde yönetmek için gereken kaynaklar, giderek artan sayıda aktör arasında dağıtılmaktadır. (Yönetişim kaynaklarının dağıtımı)”

“Siber uzayın küresel yönetişimi” düşüncesini de bu zemin üzerinden okumak mümkündür. Literatürde ise daha çok siber uzayın en önemli parçası sayılabilecek internet için küresel yönetişimin konu edildiği görülmektedir. Konuyu bu bağlamda ele alan yazarlardan Mueller, yukarıdaki dört iddia ile örtüşecek şekilde internetin ulus devlete beş farklı şekilde baskı oluşturduğunu ileri sürmüştür. Yazara göre internet, (1) iletişimin kapsamını küreselleştirmiş; (2) iletişimin ölçeğinde büyük bir sıçramaya sebep olmuş; (3) üzerindeki kontrolü merkezsizleştirmiş ve dağıtmış; (4) devletler haricinde otorite sahibi yeni kurumlar doğurmuş; (5) kolektif eylem yeteneklerinde meydana getirdiği radikal değişim sonucunda yönetime dair politikayı değiştirmiştir.⁵⁰⁵ Dolayısıyla standartlar ve kritik internet kaynakları üzerinde karar alma yetkisi, internet ile birlikte organik olarak ulus-devlet sisteminin dışında ortaya çıkan “ulusötesi aktörler ağının”

⁵⁰¹ Güncel Türkçe Sözlük, “idare”, Türk Dil Kurumu, <https://sozluk.gov.tr> (31.12.2024).

⁵⁰² Güncel Türkçe Sözlük, “yönetişim”, Türk Dil Kurumu, <https://sozluk.gov.tr> (31.12.2024).

⁵⁰³ Lawrence S. Finkelstein, “What is Global Governance?”, **Global Governance**, Vol.1, No.3, (1995), ss.367-368.

⁵⁰⁴ Klaus Dingwerth, “From International Politics to Global Governance? The Case of Nature Conservation”, **GARNET Working Paper No. 46/08**, Institute for Intercultural and International Studies, University of Bremen, 2008, s.4.

⁵⁰⁵ Milton L. Mueller, **Networks and States: The Global Politics of Internet Governance**, The MIT Press, 2010, ss.4-5.

elindedir.⁵⁰⁶ “Çok paydaşlılık (*Multistakeholderism*)” ise bu ağın niteliğini yansıtmaktadır. Yönetişime katılan aktörlerin birden fazla olması ve nitelik itibarıyla çeşitlilik arz etmesi, modelin esaslı unsurudur.⁵⁰⁷ Devletler ve uluslararası örgütlerin yanı sıra sivil toplum kuruluşları, şirketler, kamusal çıkarları savunan gruplar ve internet üzerinde politika yapım sürecine dahil olabilecek bütün odaklar bu çok paydaşlı yönetişimin paydaşlarıdır.⁵⁰⁸ *Raymond ve DeNardis* de bu aktörleri “devletler”, “uluslararası örgütler”, “şirketler” ve “sivil toplum aktörleri” şeklinde dört sınıfa ayırarak kategorize etmiştir.⁵⁰⁹

Bilhassa ICANN gibi etkin bir sivil toplum kuruluşu tarafından icra edilen yönetsel fonksiyonlar⁵¹⁰ ve devlet dışı aktörlerin teknik standartlar üzerinde süregelen belirleyiciliği üzerinden, “çok paydaşlı yönetişim” konsepti internet için sıklıkla dile getirilmektedir. Belirtmek gerekir ki yönetişim, internet için esasen bir vakıadır; internetin yapısında zorunlu olarak mündemiç değildir. ARPANET’ten bu yana devam eden tarihsel süreç; teknik, sosyal, ekonomik, politik vs. nedenlere bağlı olarak interneti mevcut yönetişim modeline tabi kılmıştır. Devletlerin de bu modele bakışları farklılık arz etmektedir. Modern uluslararası sistemin yapısı dikkate alınırsa, internet için gelecekteki gelişmelerin, devletlerin tutum ve girişimlerine bağlı olarak şekillenmesinin kaçınılmaz olduğu düşünülebilir.

Son olarak internetin siber uzayın bir cüzü olduğunu tekrar belirtmek gerekir. Siber uzaya yönelik ulusal politikalar hem uluslararası hukuku hem küresel yönetişimi etkileyecektir. Bu bağlamda yaşanacak temel çatışmanın, doğrudan eldeki çalışmanın konusu üzerine odaklanacağı kanaatindeyim. Devletlerin iç yetki alanlarını gün geçtikçe bulanıklaştıran küreselleşme ile modern ulus devlet egemenliği arasındaki soğuk ilişki, pozitif hukukta sonuçlarını doğurmaya devam edecektir. 1997’nin coşkulu ortamında *Touraine*, ulus devletin kuvvetli küreselleşme dalgasına karşı kaygılı bir reaksiyon olarak otoriterleşme yönünde direnç göstereceği öngörüsünde bulunmuştur.⁵¹¹ Siber uzay ve

⁵⁰⁶ Ibid., s.4.

⁵⁰⁷ Mark Raymond ve Laura DeNardis, “Multistakeholderism: Anatomy of an Inchoate global Institution”, *International Theory*, Vol.7, Iss.3, (2015), s.573.

⁵⁰⁸ Mueller, 2010, ss.7-8.

⁵⁰⁹ Raymond ve DeNardis, s.576.

⁵¹⁰ Aşağıda bkz. “İnternet Tahsisli Sayılar ve İsimler Kurumu (ICANN)”

⁵¹¹ Alain Touraine, *Demokrasi Nedir?*, Olcay Kunal (Çev.), İstanbul: Yapı Kredi Yayınları, 1997, s.202.

internetin büyüyen etkisine karşı devletin alacağı pozisyon da pek tabii bu sürecin izdüşümü olacaktır. Genel olarak devletlerin siber uzay ile kurdukları ilişki, küreselleşme ile olan ilişkileriyle paralellik arz etmektedir. Geçen zaman, en azından bazı önemli devletler adına *Touraine*'i haklı çıkarmaktadır. Devam eden bölümlerde örnekleri inceleneceği üzere devletlerin bu iki husus karşısındaki tutumları, sahip oldukları resmî ideoloji ve politikaya göre şekillenmektedir. Bununla birlikte devlet, siber uzay üzerinde iddia ettiği yetkiyi (meşruiyetinden bağımsız olarak) fiziksel kabiliyetlerini kullanmak suretiyle icra etme imkanına sahip olsa da uluslararası alanda siber uzayın sınır aşan özgün özelliklerinden mütevellit birtakım teorik ve pratik sorunların mevcudiyetini de göz ardı etmemek gerekir. Devletlerin, uluslararası örgütlerin, sivil toplum kuruluşlarının, şirketlerin ve nihayet başta teknoloji uzmanları ile kullanıcıları olmak üzere gerçek kişilerin beklenti ve kabiliyetleri, siber uzaydaki denge arayışının vektörleridir. Uluslararası hukukun her başlığında olduğu gibi siber uzay konusunda da hukuk ihdası, bu vektörlerin devletler nezdinde sağladığı irade uyuşmasıyla gerçekleşecektir.

B. Birleşmiş Milletler Nezdinde Yürütülen Başlıca Süreçler

1. Birleşmiş Milletler Yolunda İlk Adımlar

İsmi doğduğu topraklarda alan ve hukuka da ilk burada konu olan siber uzay hakkında ilk tartışmalar bilgisayar korsanlığı ve fikri mülkiyete yönelik gelişmiştir. Erken ve klasik dönemde ABD'li hukukçular, gerçek kişiler arasındaki siber uzaya dair uyuşmazlıkların nasıl çözüme kavuşturulabileceği konusu üzerine epeyce eğilmişlerdir. Sonrasında bilgi teknolojilerindeki gelişim sonucunda, siber uzayın diğer devletler arasında gündeme gelmesi ve uluslararası hukuka konu edilmesi fazla zaman almamıştır. Konunun BM'ye yansması da böyle bir sürecin sonucunda gerçekleşmiştir.

1995'te bir Avrupa Birliği (AB) organı olan Avrupa Komisyonu tarafından düzenlenen “Bilgi Toplumu hakkında G7 Bakanlar Konferansı” sonucunda; yine Avrupa Komisyonu’nun önerisi üzerine, tüm ülkelerin “küresel bilgi toplumuna”⁵¹² katılımlarının

⁵¹² Bilgi toplumu (*information society*), alt metninde yeni bir küresel sosyal evreyi işaret etmektedir. Avcı-toplayıcı toplum, tarım toplumu, sanayi toplumu gibi dönemsel sınıflandırmaların devamı olarak ortaya çıktığı görülmektedir. Bu açıdan bakıldığında; bilgiyi işleme ve depolama imkanlarının tarihe nispetle radikal ölçüde gelişmesinin, toplumsal yapıyı eğitim, ekonomi, endüstri gibi alanlarda köklü bir değişime uğratacağından bahisle bu değişimi belli ölçüde yaşayan toplumların küresel bilgi toplumunun parçası haline geleceği söylenebilecektir.

sağlanması gerekliliğine binaen kapsamlı bir konferans düzenlenmesi kararı alınmıştır.⁵¹³ 1996'da Güney Afrika'da düzenlenen “Bilgi Toplumu ve Kalkınma Konferansı’nda (*Information Society and Development Conference (ISAD’96)*)”; gelişmiş, gelişmekte olan ve geçiş sürecindeki devletlerin aralarındaki teknolojik açığın kapatılması adına iş birliğinin ve kalkınma için hem kamu hem özel sektörün ortaklaşa çalışmasının gerekliliği vurgulanmıştır. Kalkınmaya esas ilkeler ise aşağıdaki şekilde tespit edilmiştir:⁵¹⁴

- Evrensel hizmet
- Açık düzenleyici çerçeve
- Sürdürülebilir sosyoekonomik kalkınma
- İstihdam yaratma
- Küresel iş birliği ve rekabet gücü
- Uygulama ve içerik çeşitliliği
- Dil ve kültür çeşitliliği
- Teknolojide iş birliği
- Özel yatırım ve rekabet;
- Fikri mülkiyet haklarının korunması
- Mahremiyet ve veri güvenliği
- Altyapı açığının kapatılması
- Araştırma ve teknolojik geliştirmede iş birliği.

Kalkınma motivasyonu ile başlayan uluslararası süreç, çok kısa süre içerisinde modern uluslararası hukukun esas motivasyonu olan barış ve güvenliğin korunmasına da yönelmiştir. ISAD’96 çıktılarına, Rusya Dışişleri Bakanlığı’nın BM Genel Sekreterliği’ne hitaben yazdığı 23 Eylül 1998 tarihli mektuba eklenen karar taslağında atıfta bulunulacaktır.⁵¹⁵ Rusya’nın bu girişiminin temelinde teknolojik kalkınmadan ziyade barış ve güvenlik kaygıları bulunmuştur. Birkaç yıldır BM Genel Kurulu oturumlarında “uluslararası güvenlik, silahsızlanma ve diğer ilgili alanlar bağlamında bilim ve teknolojinin rolü” başlıklı maddenin değerlendirildiği hatırlatılan mektupta, bu konunun güncelliğini koruduğu ve hatta bilginin artık en değerli stratejik kaynak haline geldiği vurgulanmıştır. Bununla birlikte söz konusu alandaki gelişmelerin, mektubun yazıldığı dönem için “*şimdilik potansiyel ancak yine de ciddi*” olarak ifade edilen şekilde,

⁵¹³ The Community Research and Development Information Service (CORDIS), “Information Society and Development”, <https://cordis.europa.eu/event/id/5905-information-society-and-development> (31.12.2024).

⁵¹⁴ CORDIS, “Conclusions of Information Society and Development Conference”, <https://cordis.europa.eu/article/id/6191-conclusions-of-information-society-and-development-conference> (31.12.2024).

⁵¹⁵ UN/General Assembly, Letter dated 23 September 1998 from the Permanent Representative of the Russian Federation to the United Nations addressed to the Secretary-General, A/C.1/53/3, 30.09.1998, s.3.

uluslararası istikrar ve güvenliğin korunmasıyla bağdaşmayacak amaçlarla kullanımı riskinin dikkate alınması gerektiği de belirtilmiştir.⁵¹⁶ Bilgi teknolojilerinin suç ve terörizm amaçlı kullanımına ilişkin gerçek bir tehdit olduğu düşüncesi de yine önemli başlıklardandır.⁵¹⁷

2. Hükümet Uzmanları Çalışma Grubu

Rusya tarafından iletilen talep BM’de karşılık bulmuş ve mektup ekindeki taslak yaklaşık üç ay sonra Genel Kurul kararı olarak kabul edilmiştir.⁵¹⁸ Sonraki süreçte aynı başlığı taşıyan kararlar her yıl alınmaya devam edecek; BM nezdinde bilişim ve iletişim alanında uluslararası güvenlik üzerine çalışmalar yapmak üzere 6 kez “BM Hükümet Uzmanları Çalışma Grubu (*United Nations Group of Governmental Experts (UNGGE)*)” kurulacaktır.⁵¹⁹ İlki 2004’te, sonuncusu ise 2019’da teşekkül eden çalışma gruplarından birincisi ve 2015’te kurulan beşincisi faaliyetlerini mutabakata varamadan sona erdirmiştir.⁵²⁰ Diğer dört grup ise çalışmalarını raporla sonuçlandırabilmiştir. Beşinci grubun mutabakata varamamasındaki temel neden, Küba temsilcisinin beyanatında görülmektedir. Küba’nın kaygılarından ilki, gruptaki özellikle batılı devletlerin tekliflerinin “siber uzayı bir askeri operasyon sahasına dönüştürme” ve bu bağlamda “bilgi ve iletişim teknolojilerinin (BİT) (*information and communication technologies (ICT)*) hukuka aykırı kullanımının mağduru olduğunu iddia eden devletler tarafından uygulanacak -yaptırımlar ve hatta askeri müdahaleler dahil- tek taraflı cezalandırıcı güç eylemlerini meşrulaştırma” amaçlarını yansıttığı yönündedir.⁵²¹ Ayrıca “BİT’nin kötü niyetli kullanımı ile BM Şartı uyarınca meşru müdafaa hakkı doğuracak bir ‘silahlı saldırı’ arasında eşdeğerlik kurmaya yönelik formülasyonların” kabul edilemez olduğu belirtilmiştir. Son olarak vurgulanan bir önemli husus da “uluslararası insancıl hukuk

⁵¹⁶ A/C.1/53/3, s.2; Mektupta kullanılan “bilgi silahları” ve “bilgi savaşları” kavramları da özellikle dikkat çekicidir.

⁵¹⁷ A/C.1/53/3, s.2

⁵¹⁸ UN/General Assembly, Developments in the field of information and telecommunications in the context of international security, A/RES/53/70, 04.01.1999.

⁵¹⁹ Tabriz Raufoglu, **Hukuki Yönleri ile Siber Alanda Yetki Sorunu: Evrensel İnternet Yönetimi Buhranı Işığında**, Ankara: Adalet Yayınevi, 2022, ss.53-54.

⁵²⁰ Anders Henriksen, “The End of the Road for the UN GGE Process: The Future Regulation of Cyberspace”, **Journal of Cybersecurity**, Vol.5, No.1, (2019), ss.2-3.

⁵²¹ Cuba’s Representative Office Abroad, 71 UNGA: Cuba at the Final Session of Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, 23.06.2017, <https://misiones.cubaminrex.cu/en/un/statements/71-unga-cuba-final-session-group-governmental-experts-developments-field-information> (31.12.2024).

ilkelerinin BİT için de uygulanabilir olduğuna yönelik düşüncenin, BİT bağlamında bir savaş veya askeri eylem senaryosunu meşrulaştıracığı” yönündeki kaygı olmuştur. Çin ve Rusya’nın da bu çalışma grubu sonuç taslağına onay vermedikleri görülmektedir.⁵²² Küba’nın tutumu eleştirilse de⁵²³ gelişmiş ülkelerin uğradıkları siber saldırıları gerekçe göstererek nispeten zayıf durumda olan ülkelere askeri müdahalede bulunmaları ihtimalinin -en azından meşruiyet kazanmasının- önüne geçme niyeti bir nebze makul görülebilecektir.

Altı kez teşekkül eden UNGGE’nin uluslararası hukuk açısından en önemli sonucu, egemen eşitlik, iç işlerine karışmama, toprak bütünlüğüne saygı, kuvvet kullanma yasağı, uyuşmazlıkların barışçıl çözümü, temel hak ve özgürlüklere saygı gibi uluslararası hukukun esaslı ilkelerinin siber uzayda da hâkim olduğunun kabul edilmesidir. Ayrıca bu ilkeleri yansıtacak şekilde, devletler için bağlayıcılık arz etmemekle birlikte normatif yapıda 11 maddelik bir teklif de 3. ve 4. çalışma grubu tarafından sunulup 6. grup raporunda tekrar teyit edilmiştir.⁵²⁴

3. Açık Uçlu Çalışma Grupları

BM nezdinde yürütülen en kapsamlı ve en güncel süreç ise Birleşmiş Milletler Açık Uçlu Çalışma Grubu (*United Nations Open-Ended Working Group* (UNOEWG)) faaliyetleridir. Siber uzaya ilişkin ilk UNOEWG, BM Genel Kurulu’nda alınan karar ile “*BİT kullanımında güvenliğe ilişkin BM müzakere sürecini daha demokratik, kapsayıcı ve şeffaf hale getirmek*” maksadıyla kurulmuştur.⁵²⁵ Kararda ayrıca UNGGE’nin yukarıda bahsedilen raporlarında sunulmuş, “devletler için sorumlu davranış kurallarına”⁵²⁶ atıfta bulunularak; kurulacak çalışma grubuna, konsensüs esasıyla hareket etmek suretiyle bu

⁵²² Aşağıda bu iki devletin siber uzaya ilişkin uluslararası politikaları anlatılırken gerekçelerinden bahsedilecektir.

⁵²³ Henriksen, s.3; Michael Schmitt ve Liis Vihul, “International Cyber Law Politicized: The UN GGE’s Failure to Advance Cyber Norms”, Just Security, 30.06.2017, <https://www.justsecurity.org/42768/international-cyber-law-politicized-gges-failure-advance-cyber-norms/> (31.12.2024).

⁵²⁴ Maddelere yönelik inceleme ve değerlendirme için bkz. Raufoğlu, ss.91-96; Ayrıca UNGGE yapılarının ve raporlarının detaylı incelemesi için bkz. Raufoğlu, s.59 vd; Tuba Eldem, “Uluslararası Siber Güvenlik Normları ve Sorumlu Siber Egemenlik”, *İstanbul Hukuk Mecmuası*, Cilt.79, Sayı.1, (2021), s.360 vd.

⁵²⁵ UN/General Assembly, Developments in the Field of Information and Telecommunications in the Context of International Security, **A/RES/73/27**, 05.12.2018, s.5.

⁵²⁶ İlgili kurallar, 2011 yılında Çin, Rusya, Tacikistan ve Özbekistan’ın BM Genel Sekreteri’ne ortak mektuplarıyla sunulmuş, 2015’te Kazakistan ve Kırgızistan’ın da dahil olduğu yeni bir mektupla revize edilmiştir; UN/General Assembly, Letter dated 9 January 2015 from the Permanent Representatives of China, Kazakhstan, Kyrgyzstan, the Russian Federation, Tajikistan and Uzbekistan to the United Nations addressed to the Secretary-General, **A/69/723**, 13.01.2015, s.1.

kuralları ve uygulama yollarını geliştirme görevi verilmiştir. Sadece devletler arası nitelikte olmayan, bünyesinde özel sektörden, sivil toplumdan ve akademiden temsilcilerin de bulunduğu UNOEWG; 2019’da faaliyete başlamış, 2020’de olması planlanan son oturumunu COVID-19 salgını sebebiyle 2021’de gerçekleştirmiş ve nihai raporu BM Genel Sekreteri tarafından Genel Kurul üyelerine sunulmuştur.⁵²⁷

Genel olarak UNGGE raporlarına paralel çıkarımların yapıldığı 2021 UNOEWG raporunda; temel uluslararası hukuk ilkelerine, devletlerin uluslararası hukuktan doğan yükümlülüklerine ve bağlayıcılık arz etmeyen sorumlu davranış kurallarına atıflar yapılmıştır.⁵²⁸ Eldeki çalışma adına dikkat çekici hususlardan biri; BİT’nin terör ve suç örgütleri dahil olmak üzere devlet dışı aktörlerce kötü niyetli kullanımının giderek artmasının rahatsız ediciliği yönündeki beyandır. Zira bu aktörlerden bazıları, daha önce yalnızca devletlerin sahip olduğu BİT yeteneklerine sahip olduklarını kanıtlamışlardır.⁵²⁹ Bu ifade ilk bakışta yalnızca terör ve suçla mücadele yönünde bir tutumu yansıtıyor görünse dahi devlet dışı aktörlerin siber uzayda artan etkinliğinin devlet egemenliğine karşı oluşturduğu tehdit algısı da son cümlemin alt metninde okunabilmektedir. Bir başka dikkate değer husus ise aşağıda Üçüncü Bölüm’de bahsedilecek olan “kritik altyapı (*critical infrastructure*)” ve “kritik bilgi altyapısı (*critical information infrastructure*)” kavramına atıfta bulunularak, bunlara yönelik saldırıların sadece güvenliğe değil bizatihi devlet egemenliğine karşı tehdit teşkil ettiği yönündeki beyandır.

2021’de nihai raporunu sunan ilk açık uçlu çalışma grubu “Uluslararası Güvenlik Bağlamında Bilgi ve İletişim Alanındaki Gelişmeler üzerine Açık Uçlu Çalışma Grubu” adıyla kurulmuşken; henüz 2021 raporu sunulmadan, BM Genel Kurulu’nda “Bilgi ve İletişim Teknolojilerinin Güvenliği ve Kullanımı üzerine Açık Uçlu Çalışma Grubu 2021-2025”⁵³⁰ adıyla yeni bir çalışma grubu kurulmasına da karar verilmiştir.⁵³¹ 2021

⁵²⁷ UN/General Assembly, Report of the Open-ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security, A/75/816, 18.03.2021, s.2.

⁵²⁸ Rapora ilişkin genel inceleme için bkz. Raufoğlu, ss.101-111.

⁵²⁹ A/75/816, s.7, para.16.

⁵³⁰ Buradan itibaren UNOEWG-2 kısaltmasıyla anılacaktır.

⁵³¹ UN/General Assembly, Developments in the Field of Information and Telecommunications in the Context of International Security, A/RES/75/240, 31.12.2020, s.3, para.1.

raporunda da UNOEWG, devletlere kapsayıcı ve şeffaf müzakere sürecini yeni çalışma grubunda devam ettirmelerini tavsiye ederek bir nevi bayrağı devretmiştir.⁵³²

UNOEWG-2, faaliyete geçmesini takiben yıllık ilerleme raporları sunmaya başlamıştır. İlk üç esaslı oturumun ardından 2022’de yayınlanan ilk yıllık ilerleme raporunda özetle; daha önceki UNGGE raporlarında ve ilk UNOEWG nihai raporunda elde edilen çıktıların muteber görüldüğü ve ilerleyen süreçte somut adımlar atılarak bunların geliştirilmesi yönünde bütün taraflara çağrıda bulunulduğu beyan edilmiştir.⁵³³ Dördüncü ve beşinci esaslı oturumların ardından da 2023’te ikinci yıllık ilerleme raporu yayınlanmıştır.⁵³⁴ Bu raporda da öncelikle -diğer raporlarda olduğu gibi- büyük ölçüde önceki raporların çıktılarının ikrar edildiği görülmektedir. Rapordaki önemli hususlardan biri, *“açıklığın teşvikinde; tedarik zincirinin bütünlük, istikrar ve güvenliğinin sağlanmasında; kötü niyetli BİT araçlarının/tekniklerinin yayılmasının ve zararlı gizli işlevlerin kullanımının önlenmesinde”* özel sektörün hayati rolüne dikkat çekilmiş olmasıdır.⁵³⁵ Ayrıca siber uzaya ilişkin meselelerde devletler ve özel sektör arasındaki iş birliğinin güçlendirilmesine ve özel sektörün uygun yollarla teşvik edilmesine yönelik iradenin giderek kuvvet kazandığı gözlemlenebilmektedir. Raporda beyan edilen önemli bir gelişme de ilk yıllık ilerleme raporunda halihazırda bölgesel seviyelerde işlediğine işaret edilerek önerilmiş olan küresel İrtibat Noktaları Dizini’nin (*Points of Contact Directory* (PoC)) kurulmasına karar verilmesi ve bu dizine ilişkin belli başlı esasların tespit edilmesidir.⁵³⁶ Öngörülen sisteme göre küresel ve hükümetlerarası nitelikte olacak PoC, devletlerin belirleyeceği diplomatik ve teknik temsilcilerin kaydedilmesiyle kurulacak; böylece siber uzaya dair hususlarda uluslararası iletişim, işbirliği ve güven ilişkisinin güçlendirilmesi amaçlanacaktır. Ayrıca bölgesel nitelikteki diğer PoC’ler ile de irtibat kanallarının sağlanması planlanmaktadır.⁵³⁷ PoC kurulması kararından günümüze kadar çok sayıda devlet irtibat noktası bildirimini yapmıştır. Son olarak raporun son ekinde, çalışma grubuna devletlerce sunulmuş pozisyon, fikir ve inisiyatif

⁵³² A/75/816, s.15, para.76.

⁵³³ UN/General Assembly, Report of the Open-ended Working Group on Security of and in the Use of Information and Communications Technologies 2021-2025, A/77/275, 08.08.2022.

⁵³⁴ UN/General Assembly, Report of the Open-ended Working Group on Security of and in the Use of Information and Communications Technologies 2021-2025, A/78/265, 01.08.2023, s.2.

⁵³⁵ A/78/265, s.8.

⁵³⁶ A/78/265, s.19.

⁵³⁷ A/78/265, ss.19-22.

bildiren belgelerin listesine yer verildiği görülmektedir.⁵³⁸ Bu belgelerin bazılarına, ilgili devletlerin siber uzaya dair en güncel resmi tutumlarını yansıtma ve mütevellit taşıdıkları önem sebebiyle, eldeki çalışmada da yer yer atıfta bulunulacaktır.

2025'e kadar devam etmesi planlanan UNOEWG-2 sürecinde son olarak altıncı, yedinci ve sekizinci esaslı oturumların ardından 2024 Temmuz ayında üçüncü yıllık ilerleme raporu yayınlanmıştır.⁵³⁹ Önceki raporlarda olduğu gibi bu raporda da uluslararası hukukun, devletlerin egemen eşitliğinin ve buna dayalı ilkelerin siber uzayda geçerliliği, uluslararası iş birliği, ihtiyaçlar ve tehditlerin tespiti gibi geçmiş süreçteki çok sayıda kazanım üzerindeki mutabakat tekrar edilmiştir. Ayrıca rapor, birtakım yeni ve önemli hususları da ihtiva etmektedir. Rapor öncesi süreçte başta Rusya, Küba, Kuzey Kore ve Venezuela'nın olduğu bir grup devlet, ortak beyan ile BM bünyesinde OEWG konseptinin uluslararası karar alma mekanizması olarak kalıcı hale getirilmesi yönünde talepte bulunmuşlardır.⁵⁴⁰ Bunun dışında çok sayıda devlet gerek gruplar halinde gerek tekil olarak benzer yönde talep ve planları bildirmiştir.⁵⁴¹ Üçüncü yıllık ilerleme raporunda da BİT konusunda düzenli ve kurumsal iş birliği zemini teşkil edecek daimi bir mekanizmanın kurulacağı vurgulanmıştır.⁵⁴² Önümüzdeki süreçte, bu planın içeriğinin belirlenmesi ve gerçekleşmesi yönündeki çalışmaların devamı öngörülmektedir. Rapordaki bir diğer yenilik ise yapay zekâ ve kuantum berimin getirdiği fırsatlar ve riskler ile kripto varlık hırsızlığının ilk kez gündeme getirilmesidir.⁵⁴³ Gelişen ve değişen teknolojinin getirdikleri, devletler nezdinde gündem edilmeye devam etmektedir. Son olarak rapor, yine yenilik arz eden üç ek ile hitama ermiştir. Bunlar; sorumlu devlet davranışı kurallarının uygulanması için gönüllülük esasına dayalı bir

⁵³⁸ A/78/265, ss.28-33.

⁵³⁹ UN/General Assembly, Report of the Open-ended Working Group on Security of and in the Use of Information and Communications Technologies 2021-2025, A/79/214, 22.07.2024.

⁵⁴⁰ UN/Open-ended Working Group on Information and Communication Technologies, Concept paper on establishing a permanent Open-Ended Working Group by Russian Federation (co-sponsors: Belarus, Burundi, Cuba, DPRK, Eritrea, Myanmar, Nicaragua, Syrian Arab Republic, Sudan, Venezuela, Zimbabwe), Working Papers, 15.12.2023. https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_2021/ENG_Concept_paper_on_a_Permanent_Decision-making_OEWG.pdf (31.12.2024).

⁵⁴¹ UN/Open-ended Working Group on Information and Communication Technologies, Working Paper: Towards a Regular Institutional Dialogue on International ICT Security by UNIDIR (United Nations Institute for Disarmament Research), Working Papers, 28.06.2024, s.6. https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_2021/UNIDIR_-_TOWARDS_A_REGULAR_INSTITUTIONAL_DIALOGUE_ON_INTERNATIONAL_ICT_SECURITY_3.pdf (31.12.2024).

⁵⁴² A/79/214, s.6 ve ss.20-21.

⁵⁴³ A/79/214, ss.8-9.

kontrol listesi (*checklist*),⁵⁴⁴ UNOEWG’nin başından bu yana gündemde olan gönüllü küresel güven arttırıcı önlemler için başlangıç niteliğinde bir liste⁵⁴⁵ ve uluslararası güvenlik bağlamında BİT güvenliğine ilişkin açık uçlu ve eylem odaklı daimî mekanizma için tespit edilmiş birtakım esaslardır.⁵⁴⁶

UNOEWG-2 süreci halihazırda devam etmektedir. PoC’lerin kurulması, uluslararası hukukun siber uzayda nasıl uygulanacağına dair devlet düzeyinde görüş teatilerinin hızlanması, devletler için iş birliği ve ortak kalkınma imkanlarının güçlenmesi, henüz taslak aşamasında olan ve hukuki bağlayıcılığı bulunmayan normatif çalışmaların teşekkülü gibi birçok önemli gelişme, söz konusu çalışma gruplarının meyvesi niteliğindedir. 2025’te son rapor sunulduktan sonra yine açık uçlu fakat bu kez kalıcı bir mekanizmaya geçilmesi planlanmaktadır. BM süreçleri, başladığı günden bu yana bilişim hukuku disiplini içerisinde ilgiyle takip edilmektedir.

C. Başlıca Devlet Pozisyonları

Hukuka konu olan her olgu, modern devletin yapısı gereği aynı zamanda devletin ve dolayısıyla politikanın konusudur. Devletlerin siber uzaya ilişkin doktrinleri, doktrinlerin üzerine inşa ettikleri politikaları, nihayetinde ihdas ettikleri hukuk normları ve tüm bunların uygulamadaki karşılıkları, siber uzay ve egemenlik ilişkisinin ana çerçevesini oluşturmaktadır. Zira konunun, hukuk alanında siber uzayın doğuşundan bu yana istikrarlı biçimde çalışıldığı, son 15 yıldır ise siyaset bilimi araştırmacılarının yoğun ilgisine mazhar olduğu görülmektedir.⁵⁴⁷ Çalışmanın bu kısmında, siber uzayda yüksek etkinliğe ve özgün politikalara sahip başlıca devletlerin uluslararası hukuk nezdinde sahip oldukları pozisyonlar ile uygulamaları ele alınacaktır. Ulusal hukuklarına dair politika ve düzenlemeleri ise Üçüncü Bölüm’de ilgili başlıklar altında değerlendirilecektir.

⁵⁴⁴ A/79/214, ss.22-36.

⁵⁴⁵ A/79/214, ss.37-39.

⁵⁴⁶ A/79/214, ss.40-43.

⁵⁴⁷ Milton L. Mueller ve Farzaneh Badiei, “Inventing Internet Governance: The Historical Trajectory of the Phenomenon and the Field”, Laura DeNardis ve Diğerleri (Ed.), **Researching Internet Governance: Methods, Frameworks, Futures** içinde (59-83), Cambridge, Massachusetts: The MIT Press, 2020, s.75.

1. Amerika Birleşik Devletleri

Çok sayıda “teknoloji devi” tabir edilen şirket merkezini ülkesinde barındırması itibarıyla özel sektör üzerinde büyük etkiye sahip olan ABD, başta askeri olmak üzere devlete tabi bütün enstrümanlarıyla birlikte büyük bir siber kapasiteyi yönetmektedir. Bu bakımdan ABD’nin siber uzayla ilgili en önemli devlet aktörü olduğunu söylemek mümkündür. Öyle ki ABD de uluslararası stratejisini, sahip olduğu siber kapasitenin sağladığı avantajı kullanarak sivil alanda ekonomik ve kültürel üstünlüğünü tahkim etme; askeri alanda ise istihbarat, güvenlik ve saldırı kapasitesini artırma yönünde inşa etmiştir.⁵⁴⁸ Fakat teknolojinin gelişim şeklinin ve hızının ABD’yi çeşitli açılardan kaygılandığı da görülmektedir. ABD’nin siber uzaya dair resmi pozisyonunu yansıtan en güncel metinlerden 2023 tarihli Ulusal Siber Güvenlik Stratejisi’nde dikkat çekilen bir husus; yaşanan gelişimin “*daha önce ABD’nin siber uzaydaki çıkarlarına zarar verme kabiliyeti olmayan ülkeleri*” ve organize suç örgütlerini de bu bağlamda güçlendirdiği yönündeki tespittir.⁵⁴⁹ Belgede ayrıca “*revizyonist niyetli otokrat devletler*” şeklinde tanımlanan Çin, Rusya, İran, Kuzey Kore ve diğerlerine yönelik ağır ithamlarda bulunulmuştur. Bu devletlerin, ABD’nin çıkarlarına ve genel kabul görmüş uluslararası normlara ters düşen hedefler için siber yeteneklerini agresif şekilde kullandıkları; hukukun üstünlüğü ile siber uzaydaki insan haklarını pervasızca göz ardı ettikleri ve ABD’nin ulusal güvenliği ile ekonomik refahını tehdit ettikleri ileri sürülmüştür.⁵⁵⁰ ABD’nin uluslararası hukuka dair tutumu da belgede, uluslararası hukuka bağlı kalarak ve sorumlu devlet davranışı normlarını güçlendirerek siber uzaydaki paydaşlarla ortak çıkarları korumak ilkesiyle karşılık bulmuştur.⁵⁵¹ BM sürecine ilişkin ise; henüz bağlayıcı normlar oluşmamış olsa da uluslararası topluluğun girişimleriyle ortaya konmuş ortak taahhütlerin ve genel çerçevenin olumlu etkilerinin görüldüğü belirtilmiştir.⁵⁵² Strateji belgesinden son olarak, ABD’nin siber uzayda uluslararası sorumluluk hukukuna dair

⁵⁴⁸ Semin Töner Şen, **Siber Uzay ve Uluslararası Hukuk**, İstanbul: On İki Levha Yayıncılık, 2022, ss.151-152.

⁵⁴⁹ US, White House, **National Cybersecurity Strategy**, Washington, 01.03.2023, <https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf> (31.12.2024), s.3.

⁵⁵⁰ Ibid.

⁵⁵¹ Ibid., s.31.

⁵⁵² Ibid., s.32.

yaklaşımını ifade etmek için aşağıdaki paragrafı doğrudan aktarmanın faydalı olacağı kanaatindeyim:⁵⁵³

“Amerika Birleşik Devletleri, yenilenen aktif diplomasisinin temel bir parçası olarak; taahhütlerini yerine getirmeyen sorumsuz devletleri mesul tutacaktır. Düşmanlarımızı etkili bir şekilde sınırlandırmak ve silahlı çatışma eşiğinin altındaki kötü niyetli faaliyetlere karşı koymak için müttefiklerimiz ve ortaklarımızla birlikte çalışarak, kınama açıklamalarını anlamlı sonuçların uygulanmasıyla eşleştireceğiz. Bu çabalar, diplomatik tecrit, ekonomik bedeller, karşı siber operasyonlar veya yasal yaptırımlar da dâhil olmak üzere, devlet yönetiminin tüm araçlarının iş birliği içinde kullanılmasını gerektirecektir.”

ABD’nin doğrudan siber uzayın uluslararası düzenlenmesine yönelik yaklaşımı, UNGGE’ye sunduğu katkılarda net ve güncel olarak görülebilmektedir. Rusya ve ABD dahil 15 devletin katkıları, derlenerek 2021 Temmuz ayında BM Genel Kurulu’na arz edilmiştir.⁵⁵⁴ Uluslararası hukukun BİT üzerinde nasıl uygulanabileceğini ele alan ABD katkı metni, “kuvvet kullanımını içeren siber faaliyetler” ve “kuvvet kullanma düzeyinin altındaki siber faaliyetler” için iki ayrı başlık altında kurgulanmıştır.

Başta belirtmelidir ki ABD, yeterli ağırlığa ulaşmış siber saldırıların “kuvvet kullanımı” statüsünde olabileceğini ve uluslararası hukukun *jus ad bellum* ve *jus in bello* hükümlerinin bu saldırılar için de geçerli olacağını kabul etmiştir.⁵⁵⁵ *Jus ad bellum* söz konusu olduğunda uluslararası hukukun en temel metinlerinden olan BM Şartı ve silahlı kuvvet kullanımını yasaklayan m. 2/4 hükmü ilk akla gelen düzenleme olacaktır. ABD de bu hükmün ve buna bağlı olarak meşru müdafaayı düzenleyen m. 51 hükmünün siber uzaydaki fiiller için de geçerli olacağını savunmuştur. Ayrıca ABD yaklaşımına göre meşru müdafa hakkı, bir fiziksel saldırıya siber eylemlerle karşılık vermeyi kapsayabileceği gibi bir siber saldırıya fiziksel eylemlerle karşılık vermeyi de kapsamaktadır; aranan şart, müdahalenin gerekli ve orantılı olmasıdır.⁵⁵⁶ *Jus in bello*

⁵⁵³ Ibid.

⁵⁵⁴ UN/General Assembly, Official compendium of voluntary national contributions on the subject of how international law applies to the use of information and communications technologies by States submitted by participating governmental experts in the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security established pursuant to General Assembly resolution, A/76/136, 13.07.2021, s.3.

⁵⁵⁵ A/76/136, s.136; saldırının kuvvet kullanımı seviyesine ulaşması için aranan kriterlere yönelik ABD tutumuna, Üçüncü Bölüm’de ayrıca değinilecektir.

⁵⁵⁶ A/76/136, s.137.

konusunda da uluslararası hukukta yerleşmiş insancıl hukuk ilkelerinin siber faaliyetler için de geçerli olduğu kabul edilmiştir.

ABD'nin uluslararası hukuk bağlamında siber uzayda devlet egemenliğine ilişkin tutumu da genel hükümlerin kabulünü içermekle birlikte, müphem noktalardan azade değildir. Zira siber uzayın karmaşık yapısına bir ön kabul olarak değinilmiş; ardından ülkesel yargı yetkisinin devam eden öneminin siber faaliyetler için dahi kabul edildiği fakat bunun sınırsız olmadığı ve -insan haklarına dair uluslararası yükümlülükler dahil- uygulanabilir uluslararası hukuk ile uyumlu olması gerektiği ifade edilmiştir.⁵⁵⁷ Kuvvet kullanımına varmayan siber müdahalelerde egemenlik mefhumu özellikle önem arz etmektedir. Nitekim kuvvet kullanımı, doğrudan meşru müdafaa hakkını doğuran, devletin varlığına ilişkin menfaatlerine zarar verirken; kuvvet kullanımına varmayan fiillerin, devletin egemenliğine ilişkin menfaatlerine zarar vereceği söylenebilecektir. Bu bağlamda müdahale etmeme ilkesinin, siber faaliyetler için özellikle üzerinde durulduğu görülmektedir. ABD, bir ülkedeki seçimlere BİT kullanımıyla müdahale edilmesini ve halk sağlığına zarar vermeye yönelik gerçekleştirilecek siber müdahaleleri bu ilkenin ihlallerine örnek göstermiştir.⁵⁵⁸ Bununla birlikte, bir devletin başka bir devlet ülkesindeki bilgisayarlara ya da bağlı cihazlara yönelik müdahalesinin “tek başına” uluslararası hukuku ihlal etmeyeceği ileri sürülmüş; ayrıca internetin tasarım itibarıyla devletlerin egemenlik yetkilerine bir miktar tecavüze sebep olabileceğinin kabulü ifade edilmiştir.⁵⁵⁹

Devletlerin kendi ülkelerinde işlenen fiillerden kaynaklı sınır aşan zararları önlemek adına özen özen yükümlülüğünün (*due diligence*), uluslararası hukukta devletler için genel bir yükümlük arz ettiği iddiasına ilişkin; ABD tarafından halihazırda destekleyici devlet uygulaması ve hukuki zorunluluk düşüncesi (*opinio juris*) tespit edilemediğinin belirtilmesi, UNGGE katkı belgesindeki dikkat çekici hususlardandır. Yine de bu tür bir durum oluşup ilgili devlet haberdar edildiğinde, söz konusu fiillere yönelik “makul adımların” atılması gerektiği kabulü arz edilmiştir.⁵⁶⁰

⁵⁵⁷ A/76/136, s.139.

⁵⁵⁸ A/76/136, s.140.

⁵⁵⁹ A/76/136, s.140.

⁵⁶⁰ A/76/136, s.141.

Uluslararası sorumluluk hukuku açısından ABD, kabul görmüş genel hükümlere uygun şekilde; siber faaliyetlerin, devletin bir uluslararası yükümlülüğüne aykırı olması ve devlete isnat edilebilir olması halinde uluslararası haksız fiil teşkil edebileceğini belirtmiştir.⁵⁶¹ Isnat edilebilirlik için ise Uluslararası Hukuk Komisyonu’nun hazırladığı 2001 tarihli “Uluslararası Haksız Fiilden Ötürü Devletin Uluslararası Sorumluluğu” başlıklı taslak maddeler belgesinde geçen esasların ikrar edildiği görülmektedir.⁵⁶² Siber uzay söz konusu olduğunda fiillerin devlete isnat edilmesi bir yana, failin tespit edilmesi dahi oldukça güçleşebilmekte ve hatta imkansız hale gelebilmektedir. ABD de bu bakımdan genel hükümlerle iktifa etmiş, siber faaliyetler üzerinde farklı bir kriter öngörmemiştir. Uluslararası haksız fiil teşkil eden siber faaliyetten zarar gören bir devletin başvurabileceği önlem ve yaptırımlar için de benzer şekilde genel hükümlerin ikrar edildiği görülmektedir.⁵⁶³

Son olarak belirtilmelidir ki; ABD’nin siber uzaya dair devlet politikasında belirlediği dört amaç söz konusudur. Bunlar “siber uzayda istikrar ve güvenliği desteklemek”, “dijital ekonomiyi geliştirmek”, dijital özgürlüğü geliştirmek” ve “dijital bağlanabilirliği ve küresel siber kapasiteyi inşa etmek” olarak sayılmıştır.⁵⁶⁴ Yukarıda incelenenlerle birlikte değerlendirildiğinde; ABD’nin küresel, erişilebilir ve özgürlükçü bir siber uzay inşasını amaçladığı, uluslararası hukukun genel hükümlerinin siber uzaydaki fiiller için de uygulanabilir olduğunu kabul ettiği, “hasım (*adversary*)”⁵⁶⁵ olarak gördüğü devletlerin otoriter tutumlarına karşı uluslararası insan hak ve özgürlüklerini sıklıkla ileri sürdüğü, siber uzayı askeri amaçlarla kullanma yönünde istikrarlı bir uygulaması olduğu ve ülkesinin siber güvenliği için silahlı kuvvet kullanımı da dahil olmak üzere bütün araçları kullanmayı meşru gördüğü anlaşılmaktadır.

⁵⁶¹ A/76/136, s.141.

⁵⁶² Konuyla ilgili detaylı bilgi için bkz. Hakkı Hakan Erkiner, “Uluslararası Hukukta Isnat Meselesi Bakımından Soykırım İddiaları ve Osmanlı Ermenileri Soykırımı İddiası’nın Değerlendirilmesi”, **Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi**, Cilt.27, Sayı.1, (2021), s.73 vd.

⁵⁶³ A/76/136, s.142.

⁵⁶⁴ U.S. Department of State / Bureau of Cyberspace and Digital Policy, “Key Topics”, <https://www.state.gov/key-topics-bureau-of-cyberspace-and-digital-policy/> (31.12.2024).

⁵⁶⁵ US, National Cybersecurity Strategy, s.32.

2. Çin Halk Cumhuriyeti

Soğuk Savaş yıllarından bu yana mukayeseli metinlerde ABD'den sonra Rusya'nın konumlanması gelenekselleşmiş bir tercihtir. Fakat siber uzaya yönelik istisnai tutumu ve sahip olduğu siber kapasite sayesinde bu tutumu sürdürmekteki sıra dışı başarısı sebebiyle, ikinci sırada bu kez Çin'in uluslararası hukuk yaklaşımını incelemenin daha isabetli olacağı kanaatindeyim. 21. yüzyılın geride bırakmak üzere olduğumuz ilk çeyreğinde Çin, siber uzay konusunda çok dinamik bir tutum izlediğinden, hakkındaki çalışmalar kısa sürede güncelliğini yitirmektedir. Yine de en azından Çin'in bir parti devleti olmasının ve ülkesi ile uyrukları üzerindeki egemenlik haklarını batılı yaklaşımlarla ters düşecek ölçüde geniş kapsamla yorumlayıp uygulamasının, bu süreçte değişmeyen birer vakıa olduğunu söylemek mümkündür.

Siber uzay konusunda Çin, ülkesi içerisinde sıkı egemenlik ve kullanıcılar üzerinde etkin kontrol düşüncesinde olsa da uluslararası iş birliğine açık ve uluslararası hukukun geliştirilmesi için oldukça istekli bir görüntü sergilemektedir. Çin'in siber uzayın mevcut yapısı ve işleyişine yönelik açık eleştirileri söz konusudur. Bu eleştirilerin temelinde yatan iddia da bilhassa Batı merkezli gelişen özel sektörün oluşturduğu kamusal tehditlerin mevcudiyetidir. Çin'in uluslararası hukuk adına talebi de bu tehditlerin ortadan kaldırılması için gerekli olan uluslararası iş birliğinin sağlanması yönündedir.

Yakın geçmişte ABD merkezli teknoloji şirketlerindeki kullanıcı verilerine erişmek için Ulusal Güvenlik Ajansı (*National Security Agency* (NSA)) tarafından bir arka kapı (*backdoor*) olarak PRISM kod adlı programın kullandığının ifşa edilmesi ile NSA yetkililerinin bu ifşaatı kınayan ve verilere devlet erişimini destekleyen açıklamalarda bulunması gibi olaylar,⁵⁶⁶ ABD'nin siber uzayın mevcut yönetim mekanizmasını kendi ulusal çıkarları lehine istismar ettiği yönündeki tartışmaları körüklemiştir.⁵⁶⁷ Zira sonraki süreç, sızıntının sorumlusunun *Edward Snowden*

⁵⁶⁶ Glenn Greenwald ve Ewen MacAskill, "NSA Prism Program Taps in to User Data of Apple, Google and Others", *The Guardian*, 07.06.2013, <https://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data> (31.12.2024); Josh Lederman, "Intelligence Chief Blasts NSA Leaks, Declassifies some Details about Phone Program Limits", *Associated Press*, 06.06.2013, <https://web.archive.org/web/20151222130621/http://news.yahoo.com/intelligence-chief-blasts-nsa-leaks-declassifies-details-phone-025804881.html> (31.12.2024).

⁵⁶⁷ Zeng, Stevens ve Chen, s.440.

olduğunun ortaya çıkması ve failin Hong Kong'da başlayan iltica arayışının Rusya'da karşılık bulup devamında Rus vatandaşlığını almasıyla sonuçlanacaktır.⁵⁶⁸ Çin ve beraberindeki devletlerin siber uzayın uluslararası yönetim usulüne yönelik güvensizlikleri ve eleştirilerinde bu tür süreçlerin etkisi yadsınamaz.

Siber uzaya ilişkin kontrolcü ve temkinli tutumunu en başından beri devam ettiren Çin, siber uzayda uluslararası hukukun rolü hususunda uzun süre çekimser kalmıştır. 2013 yılına kadar Çin'in, uluslararası hukuk kurallarını siber uzayda uygulamanın zorluğunu vurguladığı ve bunun yerine siber uzay için bir "uluslararası davranış kuralları" geliştirmeye odaklandığı görülmüştür. Net bir tavır konulması için artan uluslararası baskı sonucu Çin, uluslararası hukukun siber uzaya uygulanabilirliğini 2013 yılında kabul etmiştir.⁵⁶⁹ Bu gelişmenin devamında ise Çin ile ABD arasında yaşanan bir siber casusluk olayı⁵⁷⁰ sonrası iki ülke arasında siber uzaya dair ilk kez ikili bir anlaşma yapılmış, siber-etkin fikri mülkiyet hırsızlığına karşı mutabakat sağlanmıştır.⁵⁷¹

Uluslararası hukuk alanında Çin'in siber uzaya ilişkin pozisyonunu ifade eden güncel belgeler UNOEWG'ye sunulmuştur. 2021 sonunda yayınlanan belgede Çin'in siber uzayın uluslararası düzenlenmesine ilişkin resmi tutumu aktarılmıştır.⁵⁷² Belgedeki

⁵⁶⁸ TC Sottek ve Janus Kopfsstein, "Everything You Need to Know about PRISM: A Cheat Sheet for the NSA's Unprecedented Surveillance Programs", The Verge, 17.07.2013, <https://www.theverge.com/2013/7/17/4517480/nsa-spying-prism-surveillance-cheat-sheet> (31.12.2024); Associated Press, "Snowden Receives Russian Passport, takes Citizenship Oath", 02.12.2022, <https://apnews.com/article/putin-europe-united-states-moscow-edward-snowden-48d05f2699466f1c5c9b5d04f57d553b> (31.12.2024).

⁵⁶⁹ Julian Ku, "How China's Views on the Law of Jus ad Bellum Will Shape Its Legal Approach to Cyberwarfare", **Hoover Working Group on National Security, Technology, and Law**, Aegis Series Paper No.1707, (17.08.2017), s.3.

⁵⁷⁰ Çin ordusuna bağlı beş bilgisayar korsanı, ABD merkezli bazı şirketlerin sistemlerine sızmak suretiyle ticari ve ekonomik değeri olan bilgileri çaldığı gerekçesiyle yargılanmıştır. Bu olayın, devlet aktörlerine isnat edilebilecek ilk bilgisayar korsanlığı yargılaması olduğu belirtilmiştir; U.S. Department of Justice / Office of Public Affairs, "U.S. Charges Five Chinese Military Hackers for Cyber Espionage Against U.S. Corporations and a Labor Organization for Commercial Advantage", 19.05.2014, <https://www.justice.gov/opa/pr/us-charges-five-chinese-military-hackers-cyber-espionage-against-us-corporations-and-labor> (31.12.2024).

⁵⁷¹ John W. Rollins ve Diğerleri, **U.S.-China Cyber Agreement**, Library of Congress, Congressional Research Service (CRS), IN10376, 16.10.2015.

⁵⁷² UN/Open-ended Working Group on Information and Communication Technologies, China's Positions on International Rules-making in Cyberspace, Working Papers, 01.12.2021; <https://documents.unoda.org/wp-content/uploads/2021/12/Chinese-Position-Paper-on-International-Rules-making-in-Cyberspace-ENG.pdf> (31.12.2024).

içerik, siber uzayın mevcut durumuna yönelik eleştiriler ile başlamaktır. Eleştirilen hususlar aşağıdaki şekilde sıralanabilir:⁵⁷³

- 1- Siber uzayın devletler tarafından yeni bir savaş alanı olarak görülmesi ve kurulan askeri ittifaklar, kabul edilen yeni angajman kuralları gibi gelişmelerle gittikçe askerileştirilerek uluslararası barış ve güvenliği tehdit eder hale getirilmesi
- 2- Kritik altyapılar üzerindeki tehdidin büyümesi
- 3- Siber saldırıların, suçların ve terörizmin artması
- 4- Kişisel verileri istismar eden yalan haberlerin artması
- 5- Kritik İnternet kaynaklarının mevcut dağıtım ve yönetim sistemindeki dengesizlik ve adaletsizlik
- 6- Ülkeler ve bölgeler arasındaki dengesiz gelişme ve giderek büyüyen dijital uçurum
- 7- Devletlerin teknoloji ve siber güvenlik konularını siyasallaştırarak ve diğer devletleri bu alanda baskılayarak küresel kalkınma ve iş birliğini tehlikeye atması

Mevcut uluslararası hukuk kurallarının siber uzayda uygulanmasına yönelik kabul beyanı çekinceli bir şekilde tekrar edilmiştir. Zira Çin’e göre BM Şartı hükümleri ve Şart’ta mündemiç olan -başta devletlerin egemen eşitliği, kuvvet kullanma yasağı, uluslararası anlaşmazlıkların barışçıl yollarla çözülmesi ve iç işlerine karışmama olmak üzere- uluslararası hukuk ilkeleri siber uzay için de geçerlidir.⁵⁷⁴ Lakin “*devletler silahlı çatışmalar hukuku ile jus ad bellum’un uygulanabilirliğini ihtiyatlı bir şekilde ele almalı ve çatışmaların tırmanmasını veya siber uzayın yeni bir savaş alanına dönüşmesini önlemelidir*”⁵⁷⁵ ifadesinde de görüleceği üzere, uluslararası hukukta yerleşik olan *jus ad bellum* ve *jus in bello* kurallarının siber uzaydaki geçerliliği konusunda Çin’in ihtiyatlı tutumu devam etmektedir. Ayrıca teklifçileri arasında Çin’in de bulunduğu “sorumlu davranış kuralları” üzerindeki mutabakatın devletlerce dikkate alınarak uygulanması gerektiğine belgede tekrar işaret edilmiştir.⁵⁷⁶

⁵⁷³ China's Positions on International Rules-making in Cyberspace, s.1.

⁵⁷⁴ China's Positions on International Rules-making in Cyberspace, s.3.

⁵⁷⁵ China's Positions on International Rules-making in Cyberspace, s.3.

⁵⁷⁶ China's Positions on International Rules-making in Cyberspace, s.4.

Çin, uluslararası hukukun genel hükümleri dışında siber uzaya özgü belli başlı kural ve ilkelere de uyulması gerektiğini belirtmiştir. Sayılan kural ve ilkeler bir tutum göstergesi olduğu gibi aynı zamanda mevcut duruma yönelik eleştirilerin devamı niteliğinde mesajlar da içermektedir. Diğer yandan bunu normatif bir teklifin erken hali olarak düşünmek dahi mümkündür. Bahsedilen hususlar aşağıdaki gibi sayılmıştır:

i. Devletler barış, güvenlik, açıklık, iş birliği ve düzenin hâkim olduğu bir siber uzayı teşvik etmeli ve BİT’yi uluslararası barış ve güvenliğin korunması hedefleriyle bağdaşmayan faaliyetler yürütmek için kullanmamalıdır.

ii. Egemenlik ilkesi siber uzayda da geçerlidir. Devletler kendi ülkelerindeki BİT altyapısı, kaynakları, verileri ve BİT ile ilgili faaliyetler üzerinde yargı yetkisini kullanmalı ve bilgi sistemleri ile önemli verilerini tehdit, müdahale, saldırı ve sabotajdan kaynaklanan zararlara karşı koruma hakkına sahip olmalıdır. Devletler vatandaşlarının, işletmelerinin ve sosyal kuruluşlarının meşru çıkarlarını korumak için BİT ile ilgili kamu politikalarını, yasaları ve düzenlemeleri yapma hakkına sahiptir. Devletler, diğer devletlerin iç işlerine karışmak ve siyasi, ekonomik ve sosyal istikrarlarını baltalamak veya diğer devletlerin ulusal güvenlik ve kamu menfaatlerine zarar veren faaliyetler yürütmek için BİT kullanmaktan kaçınmalıdır. Devletler, uluslararası internet kaynaklarının yönetimine ve dağıtımına eşit temelde katılmalı; çok taraflılık, demokrasi ve şeffaflığa dayalı küresel bir internet yönetim sistemi oluşturmalıdır.

iii. Devletler kritik BİT altyapısının korunmasını geliştirmelidir. Devletler, diğer devletlerin kritik altyapılarına zarar veren, diğer devletlerin kritik altyapılarına ait önemli verileri bozan veya çalan BİT faaliyetlerine karşı durmalıdır. Devletler, kritik BİT altyapısının korunmasına ilişkin mevzuat, en iyi uygulamalar ve teknolojiler konusunda bilgi alışverişini artırmalı; personel eğitimi, teknolojik yenilik, erken uyarı ve önleme, acil müdahale, standart ve regülasyonlar ile bilgi paylaşımı konularında uluslararası iş birliğini teşvik etmelidir.

iv. Devletler veri güvenliğini kapsamlı, objektif ve kanıta dayalı bir şekilde ele almalıdır. Devletler açık, adil ve ayrımcı olmayan bir iş ortamını teşvik etmeli; küresel BİT ürün ve hizmetleri için açık, güvenli ve istikrarlı bir tedarik zinciri sağlamalıdır. Devletler, BİT kullanımı yoluyla kişisel bilgileri tehlikeye atan faaliyetleri önlemek ve sona erdirmek için harekete geçmeli; diğer devletlere karşı kitlesel gözetime ve BİT’nin bir araç olarak kullanılarak diğer devletlerin kişisel bilgilerinin izinsiz toplanmasına karşı çıkmalıdır. Devletler, şirketleri faaliyet gösterdikleri devletin yasa ve yönetmeliklerine uymaya teşvik etmeli; ülkeleri dışında üretilen ve elde edilen verileri kendi topraklarında depolamalarını yerli şirketlerden talep etmemeli veya başka devletlerde bulunan verileri şirketler ya da bireyler aracılığıyla bu devletlerin izni olmadan elde etmemelidir.

BİT ürün ve hizmet sağlayıcıları, faaliyet gösterdikleri devletin yasa ve yönetmeliklerine uymalı; kullanıcıların verilerini yasadışı yollardan elde etmek, kullanıcıların sistem ve cihazlarını kontrol veya manipüle etmek için ürün ve hizmetlerine arka kapılar kurmamalıdır. BİT şirketleri, kullanıcıların ürünlerine olan bağımlılığından faydalanarak gayrimeşru menfaat arayışında olmamalı; kullanıcıları sistem ve cihazlarını yükseltmeye zorlamamalıdır. Ürün sağlayıcıları, ürünlerindeki ciddi güvenlik açıklarını iş birliği ortaklarına ve kullanıcılara zamanında bildirme ve çözüm önerileri sunma taahhüdünde bulunmalıdır.

v. Devletler siber terörizme karşı iş birliğini yükseltmelidir. Devletler, terör örgütlerinin terörist ses ve video belgelerinin üretimi, yayımlanması, depolanması ve yayınlanması; şiddet içeren terörist söylem ve ideolojinin yayılması; fon toplama, üye toplama, terörist faaliyetleri teşvik etmesi vb. dahil terörist faaliyetler yürütmek üzere web siteleri, çevrimiçi forumlar ve bloglar kurmak için interneti kullanmalarını yasaklamalıdır. Devletler siber terörizmle mücadele için istihbarat alışverişi ve kolluk kuvvetleriyle iş birliği yapmalı; uluslararası örgütler, işletmeler ve vatandaşlarla iş birliğine dayalı ortaklıklar geliştirmelidir. Devletler internet servis sağlayıcılarından propaganda web sitelerini ve hesaplarını kapatarak, terörist ve şiddet yanlısı aşırılıkçı içerikleri silerek, terörist içeriğin çevrimiçi yayılma kanalını kesmelerini talep etmelidir.”

Çin’in beyanatına zemin teşkil eden esas kaygının, batılı devletlerin siber uzayda yükselen hakimiyetine karşı hukuka dayalı bir öz savunma mekanizması geliştirmek olduğu yorumunda bulunmak mümkündür. Nitekim siber uzayın özgün yapısının, gerekli ve yeterli teknolojiye sahip olan aktörlere devlet karşısında önemli avantajlar sağladığı aşîkardır. Konu siyasete ve iktisada geldiğinde, bu avantajların suiistimal edilmesi, devletleri egemenlik haklarını daha etkin savunmaya ve buna yönelik önlemler almaya yöneltecektir. Buna karşı bir yorum olarak, Çin’in bu şartları gerekçe göstermek suretiyle otoriter rejimini güçlendirmeye çalıştığını ileri sürmek de mümkündür. Ayrıca Çin’in egemenlik odaklı tutumunun, siber uzayda alternatif normlar geliştirme kapasitesini önemli ölçüde kısıtladığı yönünde eleştiriler de mevcuttur.⁵⁷⁷ Bu yöndeki eleştirilerin haklılık payı da yüksek olmakla birlikte, Çin’in yukarıda işaret ettiği hususların uluslararası hukukun amaçları açısından oldukça önemli olduğu kanaatindeyim. Bu düşüncenin oluşmasında, Çin’in izlediği rota ve usulde değişikliğe gitmesinin etkisi de göz ardı edilemez. Bu minvalde *Hong* ve *Goodnight*, Çin’in savunduğu siber egemenlik

⁵⁷⁷ Zeng, Stevens ve Chen, s.432.

doktrininin söylemsel gerekçesinin, milli güvenlik savunusundan ayrılıp olumlu hedeflere doğru kaydığı yorumunda bulunmuşlardır.⁵⁷⁸ “Küresel iletişimi Amerikan tarzı teknokratik korporatist hakimiyetten kurtarmak” motivasyonunu taşıyan siber egemenlik söylemi, artık klasik ülkesel yaklaşımından uzaklaşıp küresel kalkınmadan ve ortak refahtan bahseden bir noktaya gelmiştir.⁵⁷⁹ Yazarlar bunları belirttikten sonra ise şu sonuca varmıştır:⁵⁸⁰

“Sonuç olarak siber egemenlik, mutlak özerkliğe bir dönüşü kastetmiyor (siber küreye üyelik ilk etapta zaten Vestfalyacı egemenliği aşındırmıştır); ekonomik ve sosyal sorumlulukları yerine getirmek için gerekli olan devlet kapasitesini korumak adına uygulanabilir bir küresel yönetim seçeneği olarak öneriliyor.”

Çin’in veri güvenliği özelindeki tutumu da dikkatle incelendiğinde; siber uzaya ilişkin kontrolcü yaklaşımın Çin için basit bir otoriter rejim refleksinden ibaret olmadığı (insan hak ve özgürlükleri açısından tartışmalı sonuçlar doğurmakla birlikte) ve modern dönemde stratejik önemi radikal biçimde artan veri üzerinden elde edilecek menfaatin, rekabet içerisinde olduğu devletler lehine küresel dengeyi sarsacak şekilde kullanılmasının önüne geçme amacını yansıttığı anlaşılabacaktır. Şüphesiz, bu konuda da siyah ve beyazın varlığından bahsetmek mümkün değildir. Siyasi çıkar çatışmasının bir enstrümanı olarak istismar etmesi riskine rağmen, Çin’in kaygı ve eleştirilerinin yerinde olduğu kanaatindeyim. Önümüzdeki süreçte tarafların siber uzay için uluslararası iş birliği, sürdürülebilirlik, ortak menfaatler ve devletlerin egemenlik haklarına saygı zeminine oturan bir uluslararası hukuk inşa etmeleri adına tutarlılık ve iradeleri çokça sınanacaktır. Nüfusu, ekonomik gücü ve siber kapasitesi ile Çin, bu sınavda göstereceği performans ile siber uzayın geleceğinin belirleyicilerinden olma potansiyelini taşımaktadır.

3. Rusya Federasyonu

Çin, radikal politikaları uygulama başarısı ve hacim büyüklüğü ile dikkat çekerken; Rusya’yı öne çıkaran, bilgi güvenliğine ilişkin köklü politikası ve zaman içinde

⁵⁷⁸ Yu Hong ve G. Thomas Goodnight, “How to Think about Cyber Sovereignty: the Case of China”, **Chinese Journal of Communication**, Vol.13, No.1, (2020), s.18.

⁵⁷⁹ Ibid., ss.18-19.

⁵⁸⁰ Ibid., s.19.

olgunlaşmış doktrindir. Rusya için siber uzay, dezenformasyon ve toplum psikolojisi gibi birçok dalı kapsayan oldukça geniş bir çerçevede ele alınmış “bilgi ortamının” bir parçasıdır. Rusya’nın siber uzaya ilişkin politikasının da büyük ölçüde Çin ile benzerlik arz ettiğini söylemek mümkündür. Dolayısıyla devlet egemenliğini ön plana çıkaran yaklaşımı açısından “Dijital/Siber Vestfalya” savunucusu olarak değerlendirildiği de görülmektedir.⁵⁸¹

Rusya da Çin’e benzer şekilde uluslararası hukukun siber uzaya uygulanabilirliği ve yeterliliği konusunda önceleri muhalif veya çekimser kaldığı için, BM’deki tartışmaların başladığı 1998 yılından bu yana özellikle bilgi güvenliği konusunda yeni ve kapsamlı bir uluslararası antlaşma imzalanması gerektiği düşüncesindeydi.⁵⁸² Son dönemde ise bu gerekliliği savunmaya devam etmek ve yoğun girişimlerde bulunmakla birlikte; esas motivasyonunu, BİT için uluslararası hukukun otomatik ve yüzeysel bir şekilde uygulanmasındansa özgün nitelikleri göz önüne alınarak kapsamlı bir tartışma sonucunda mutabakat sağlanması yönünde belirlemiştir.⁵⁸³

Rusya, siber uzaya ilişkin konularda BM bünyesinde en aktif katkıda bulunan devlettir. Kurulmasına önyak olduğu UNGGE’nin bütün süreçlerine katılmış, 2004-2005 ve 2009-2010 dönemlerinde de başkanlığını yürütmüştür.⁵⁸⁴ UNOEWG formatı da yine başta Rusya’nın girişimleri sonucunda hayata geçmiştir.⁵⁸⁵ Rusya ve beraberindeki devletler UNOEWG’nin kalıcı hale getirilmesi adına çalışmalarını sürdürmektedir.⁵⁸⁶ Yine UNOEWG-2 bünyesinde yıllık ilerleme raporuna yönelik Belarus, Küba, İran, Nikaragua, Suriye ve Venezuela ile ortak sunduğu beyanda siber uzaya yönelik en güncel

⁵⁸¹ Chris Demchak and Peter Dombrowski, “Cyber Westphalia: Asserting State Prerogatives in Cyberspace”, **Georgetown Journal of International Affairs**, International Engagement on Cyber III, (2013), s.32; Julien Nocetti, “Contest and Conquest: Russia and Global Internet Governance”, **International Affairs**, Vol.91, Iss.1, (2015), s.117. Ayrıca bkz. aşağıda “Siber Vestfalyacılık”.

⁵⁸² Elaine Korzak, “Russia’s Cyber Policy Efforts in the United Nations”, **Tallinn Paper No.11**, NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE), 2021, s.14.

⁵⁸³ A/76/136, s.80.

⁵⁸⁴ Korzak, s.7.

⁵⁸⁵ Ibid. s.8.

⁵⁸⁶ UN/Open-ended Working Group on Information and Communication Technologies, Concept Paper on a Permanent Decision-Making Open-Ended Working Group on Security of and in the Use of Information and Communications Technologies, Working Papers, 08.03.2024, [https://docs-library.unoda.org/Open-Ended-Working-Group-on-Information-and-Communication-Technologies-\(2021\)/ENG-Concept-paper-on-a-Permanent-Decision-making-OEWG.pdf](https://docs-library.unoda.org/Open-Ended-Working-Group-on-Information-and-Communication-Technologies-(2021)/ENG-Concept-paper-on-a-Permanent-Decision-making-OEWG.pdf) (31.12.2024).

tutumunu yansıtmıştır. Metinde, rapora eklenmesi talep edilen hususlar aşağıdaki şekilde yer almıştır:⁵⁸⁷

“-Devletlerin egemenliklerinin BİT kullanımındaki tehditlere karşı korunmasının yanı sıra devletlerin farklı ulusal gerçeklikleri, kapasiteleri ve gelişmişlik seviyelerine göre modern BİT'ye erişimin ayrımcı olmayan şekilde sağlanması ve BM Şartı'nı ihlal eden tek taraflı zorlayıcı önlemlerden -bu tür hukuka aykırı önlemlerin BİT'ye erişim açısından doğrudan bir etkiye sahip olduğu gerçeğini göz önünde bulundurarak- kaçınılması;

-Mevcut 13 gönüllü norm setine ek olarak, hukuken bağlayıcı olanlar da dahil olmak üzere, BİT kullanımında sorumlu devlet davranışlarına ilişkin yeni kurallar, normlar ve ilkeler geliştirilmesi;

-Bilgi alanının sadece barışçıl amaçlarla kullanılmasının sağlanması; -ki bu nedenle, uluslararası insancıl hukuka ilişkin hükümlerin taslak rapora dahil edilmesini desteklemiyoruz-;

-BİT kullanımını düzenleyecek bir uluslararası hukuk belgesi de dahil, hukuken bağlayıcı yükümlülüklerin detaylı şekilde belirlenip hazırlanması;

-BİT kullanımında evrensel terminolojinin geliştirilmesi;

-Tedarik zinciri ve veri güvenliği için küresel olarak birbiriyle uyumlu ortak kural ve standartların geliştirilmesi ve uygulanması;

-İnternetin genel kullanılabilirliğinin, güvenli ve istikrarlı işleyişinin güvence altına alınması ve devletlerin bu yönetime eşit katılımının sağlanması;

-BM İrtibat Noktaları Dizini oluşturulması ve devletlerin yetkili makamları arasında doğrudan iletişimin kolaylaştırılması;

-Gelişmekte olan egemen devletlerin ihtiyaçlarına ve ulusal güvenlik çıkarlarına dikkat edilerek, kapasite geliştirmenin adil ve depolitize şekilde sağlanamaması;

-"Dijital uçurumun" üstesinden gelmeyi amaçlayan geliştirmekte olan devletlere adil ve depolitize bir temelde teknik yardım sağlamak için kapasite geliştirme alanında özel bir fon / yardım programı oluşturma olasılığının -diğer BM hedefli programların tecrübelerine göre- değerlendirilmesi;

- BİT güvenliği ve kullanımına ilişkin müzakere sürecinin, bu konuda BM himayesinde tek bir müzakere mekanizması çerçevesinde, yani OEWG bünyesinde sürdürülmesi.”

⁵⁸⁷ UN/Open-ended Working Group on Information and Communication Technologies, Joint Position of the Republic of Belarus, the Republic of Cuba, the Islamic Republic of Iran, Republic of Nicaragua, the Russian Federation, the Syrian Arab Republic and the Bolivarian Republic of Venezuela on the Draft Annual Progress Report of the Open-ended Working Group on Security of and in the Use of ICTs 2021-2025, Working Papers, 25.07.2022, <https://documents.unoda.org/wp-content/uploads/2022/07/Draft-Joint-Position-on-the-OEWG-draft-report-Final.pdf> (31.12.2024).

Ortak metinde görüldüğü üzere, bilhassa siber uzayda üstünlük sahibi olan devletlere karşı, gelişmekte olan devletlerin kapasitelerinin geliştirilmesi adına uluslararası destek arayışı, ilgili devletlerin öncelikli amacıdır. Şüphesiz ki bu arayış siyasi amaçlardan varestedir. Lakin yine de egemen eşit devletlerin siber uzayda adil varlık göstermeleri açısından, mevcut dezavantajların en azından törpülenmesi haklı bir talep olacaktır. Ayrıca insancıl hukukun siber uzayda uygulanmasına karşı muhalif tutumun bu devletler adına da devam ettiği görülmektedir. Zira Rusya burayı savaş (Rusça *война* (*voyna*); İngilizce *war*)” alanı olarak değil; bir yüzleşme (Rusça *противоборство* (*protivoborstvo*); İngilizce *confrontation*) ve mücadele alanı olarak değerlendirmektedir.⁵⁸⁸ Son olarak, Rusya’nın gerçekleşmesi yolunda uzun zamandır mücadele verdiği uluslararası antlaşma için çabalarını müttefikleriyle birlikte sürdürdüğü ve bunun zemini olarak da kalıcı hale gelecek bir UNOEWG’yi öngördüğü söylenebilecektir. Müstakbel “Uluslararası Bilgi Güvenliğinin Sağlanması Adına BM Antlaşması” için hazırlayıp UNOEWG’ye sunduğu temel esaslar da söz konusu politikanın en somut ve güncel örneklerindendir.⁵⁸⁹

Başta ABD, Rusya’nın bir uluslararası antlaşma vasıtasıyla bağlayıcı normlar oluşturma teklifine karşı temkinli davranmaktadır. Tavrına gerekçe olarak da antlaşma ile ortaya çıkacak sonucun serbest bilgi akışına hanel getirecek ölçüde hükümet kontrolü doğuracağı kaygısını sunmaktadır. ABD’ye göre küresel, güvenli ve adil bir gelişme, hükümet kontrolü ve sansürüyle değil; insan haklarına saygı ve serbest bilgi akışının sağlanmasıyla mümkün olacaktır.⁵⁹⁰ Rusya’nın “bilgi güvenliği” konseptinin geniş kapsamının, insan hakları adına kaygı uyandırdığı da ayrıca belirtilmektedir. Esasında Rusya ve müttefikleri, insan haklarının bu alandaki geçerliliğini reddetmemektedir. Fakat gelen eleştiri, bu devletlerin insan haklarına saygıyı ulusal bağlamda ele aldıkları, hak ve özgürlüklerin kullanımını da böylece sınırladıkları yönündedir. Örnek olarak “bilgi arama, edinme ve yayma” gibi uluslararası kabul görmüş hak ve özgürlüklerin

⁵⁸⁸ Janne Hakala ve Jazlyn Melnychuk, **Russia’s Strategy in Cyberspace**, Riga: NATO Strategic Communications Centre of Excellence, 2021, s.5.

⁵⁸⁹ UN/Open-ended Working Group on Information and Communication Technologies, Updated Concept of the Convention of the United Nations Ensuring International Information Security submitted by Russian Federation (Cosponsors: Belarus, DPRK, Nicaragua, Syria, Venezuela), Working Papers, 29.06.2023, [https://docs-library.unoda.org/Open-Ended Working Group on Information and Communication Technologies - \(2021\)/ENG Concept of convention on ensuring international information security.pdf](https://docs-library.unoda.org/Open-Ended Working Group on Information and Communication Technologies - (2021)/ENG Concept of convention on ensuring international information security.pdf) (31.12.2024).

⁵⁹⁰ UN/General Assembly, Developments in the Field of Information and Telecommunications in the Context of International Security, **A/59/116/Add.1**, 28.12.2004, s.3.

kullanılması, “ilgili ulusal yasa ve düzenlemelere uyma” şartına dayanmaktadır.⁵⁹¹ Eleştiriler, bu düzenlemelerin teoride sorun teşkil etmemekle birlikte uygulama noktasında bir baskı ve sansür aracı olarak kullanıldığı görüşü üzerine inşa edilmektedir.

Genel uluslararası hukuk normları açısından Rusya, başta BM Şartı ve Dostça İlişkiler Bildirgesi’ndekiler olmak üzere uluslararası hukukun evrensel kabul görmüş ilke ve normlarının siber uzaya uygulanabilirliği yönünde uluslararası mutabakat sağlandığını varsaymaktadır.⁵⁹² Rusya’nın UNGGE katkı belgesinde özellikle saymayı tercih ettiği ilkeler, genel politikasının önceliklerini tam olarak yansıtmaktadır:

“...devletlerin egemen eşitliği, kuvvet kullanma yasağı, uluslararası uyuşmazlıkların barışçıl yollarla çözümü, devletlerin iç işlerine karışmama, devletlerin birbirleriyle iş birliği yapma yükümlülüğü, halkların eşit hakları ve self determinasyon hakları, uluslararası yükümlülüklerin iyi niyetle yerine getirilmesi, devlet sınırlarının dokunulmazlığı ve devletlerin toprak bütünlüğü.”

Bunların yanı sıra uluslararası sorumluluk hukuku açısından; “bilgi uzayında” uluslararası hukuka aykırı eylemin devlete isnat edilmesinde, gerekli teknik delillerin hassasiyetle değerlendirilerek, devletlerin peşinen sorumlu tutulmasının önüne geçilmesi gerekliliğine özel olarak değinilmiştir.⁵⁹³

Rusya’nın da siber uzayın mevcut yönetim şekline yönelik eleştirileri söz konusudur. Bunların başında, “kritik internet kaynağı” olarak görülen DNS’yi yöneten ICANN’nin ABD yasalarına tâbi olmasından kaynaklı kaygılar yer almaktadır. Zira çok yakın dönemde ABD’nin .ru ve .su uzantılı alan adlarına erişimi küresel olarak engellemesi ihtimali ciddi şekilde tartışılmıştır.⁵⁹⁴ 1 Kasım 2019’da Rusya’da, Web’in bir acil durum veya dış müdahale sonucu erişilemez hale gelmesi ihtimalinde Rus kısmının işlemeye devam edebilmesi adına çalışmaları başlatan ve ulusal bir alan adı sistemi kurulmasını öngören düzenleme yürürlüğe girmiştir.⁵⁹⁵ Ukrayna’daki savaşın şiddetlenmesiyle birlikte 2022 yılında Ukrayna, Başbakan Yardımcısı ve Dijital

⁵⁹¹ Korzak, s.16.

⁵⁹² A/76/136, s.79.

⁵⁹³ A/76/136, s.80.

⁵⁹⁴ Ilona Stadnik, “Russia: An Independent and Sovereign Internet”, Blayne Haggart, Natasha Tusikov ve Jan Aart Scholte (Ed.), **Power and Authority in Internet Governance: Return of the State?** içinde (147-167), London, New York: Routledge, 2021, s.158.

⁵⁹⁵ Andrei Richter, “Sovereign Internet Law Adopted”, IRIS Merlin, 01.06.2019, <https://merlin.obs.coe.int/article/8603> (31.12.2024).

Dönüşüm Bakanı *Fedorov*'un mektubu vasıtasıyla ICANN'den Rus kaynaklı üst seviye alan adlarına (*top level domain* (TLD)) verilen sertifikaların iptalini ve Rusya'da bulunan DNS kök sunucularının kapatılmasını talep etmiştir.⁵⁹⁶ Böyle bir yaptırımın sadece teklifi dahi Rusya'nın kaygılarını haklı çıkaracak, uluslararası kamuoyunda internet tarafsızlığının sorgulanmasına neden olacak ve Web'in küresel yapısının devamlılığını sarsacak yeterliliktedir. Nitekim ICANN de çok kısa sürede bu teklifi olumsuz yönde cevaplamıştır. ICANN cevap yazısında, kuruluşun amacının interneti engellemek ve her ne sebeple olursa olsun siyasi saiklere uygun şekilde yaptırım uygulamak değil; yalnızca internetin doğru ve istikrarlı şekilde çalışmasını sağlamak olduğunu belirtmiş, politik ve teknik gerekçelerini de saymak suretiyle *Federov*'a ret beyanını iletmıştır.⁵⁹⁷ Diğer taraftan, ICANN'in böyle bir düşüncüyü hayata geçirmesinin bütün mevcut şartlara rağmen en başta ABD'nin milli menfaatlerine aykırı düşeceği yorumu da yapılmıştır. Öyle ki DNS yönetiminin tarafsızlığına yapılacak bir müdahale, internetin bölünmesine/bölgeselleşmesine sebep olacak ve ABD'nin internetin dünya çapında yayılması politikasını başarısızlığa uğratacaktır.⁵⁹⁸

Anlaşılabacağı üzere uluslararası hukukun genelinde olduğu gibi Web de devletler arasındaki bir denge üzerinde varlığını sürdürmektedir. Fakat Rusya bu dengenin ABD merkezli bir sivil yapı tarafından yürütülmesinden yine de memnun değildir. Rusya'nın bu bağlamdaki talebi, kritik internet kaynaklarının yönetiminin BM'ye ve özelde ITU'ya devredilmesidir.⁵⁹⁹ Bu politika dahilinde Rusya, internet yönetişiminde çok paydaşlılık olgusunun da suni şekilde fazla abartıldığından şikayetçidir. Özellikle uluslararası bilgi güvenliği söz konusu olduğunda, çok paydaşlılığın empoze edilmesiyle BM'nin merkezi rolünün aşındırıldığını ileri sürmüştür.⁶⁰⁰ Nihai olarak UNOEWG gibi bir girişimin öncüsü de olsa Rusya'nın, çok paydaşlılıktan ziyade hükümetler arasında çok taraflı bir

⁵⁹⁶ Jon Brodtkin, "Ukraine asks ICANN to Revoke Russian Domains and Shut Down DNS Root Servers", Ars Technica, 02.03.2022, <https://arstechnica.com/tech-policy/2022/03/ukraine-wants-russia-cut-off-from-core-internet-systems-experts-say-its-a-bad-idea/> (31.12.2024).

⁵⁹⁷ ICANN, Correspondence, 02.03.2022, <https://www.icann.org/en/system/files/correspondence/marby-to-fedorov-02mar22-en.pdf> (31.12.2024).

⁵⁹⁸ Stadnik, s.162.

⁵⁹⁹ Ibid., s.158.

⁶⁰⁰ UN/Open-ended Working Group on Information and Communication Technologies, Statement by the Representative of the Russian Federation at the Online Discussion of the Second "Pre-draft" of the Final Report of the UN Open-ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security, 15.06.2020, <https://front.un-arm.org/wp-content/uploads/2020/09/oewwg-informal-virtual-meetings-statement-by-the-russian-federation-15-june-2020.pdf> (31.12.2024).

siber uzay yönetiřimi tasavvurunda olduđu, bu tasavvurunu hayata geirebilmek iin de yönetiřimi BM eksenine ekmeye ve burada yapılacak bir uluslararası antlaşma ile normatif sonuçlar elde etmeye alıřtığı görlmektedir.

4. Türkiye Cumhuriyeti

lke ierisinde siber egemenlik doktrini inřa etme yolunda adımlar atan Türkiye, yakın dönemde yürrlge koyduđu ulusal normlarla siber uzay zerinde devlet denetimini arttırma abasındadır. Bununla birlikte uluslararası hukuk sahasındaki giriřimleri henz olduka mtevazı boyuttadır. Siber kapasitesi en geliřmiř devletler bir tarafa; Rusya ve in eksenindeki devletlere yahut Latin Amerika ve hatta bazı Afrika devletlerine dahi kıyasla Türkiye'nin siber uzay adına uluslararası hukuk alanındaki etkinliđinin dřk olduđu görlmektedir. Hal byle olsa dahi belli bařlı hususlara deđinmek faydalı olacaktır.

ncelikle Türkiye'nin bařta UNOEWG olmak zere BM bnyesinde gerekleřen alıřmaları ve alıřmaların ıktılarını genel olarak desteklediđini belirtmek gerekir. Ayrıca dođrudan Cumhurbaşkanlıđı nezdinde dile getirilen *“lkelerin tamamının uzlaşmayla kabul edip arkasında duracađı bir dijital hukuk dzeni kurulmadan bu sorunların özm mmkn deđildir”*⁶⁰¹ ifadeleri, Türkiye'nin uluslararası hukukta siber uzayı konu edinen normatif bir zeminin kurulması yönündeki talebini yansıtmaktadır. Bu dođrultuda Türkiye, sorumlu davranıř kurallarının kabul ve geliřtirilmesi, PoC kurulması, devletlerin siber kapasitelerinin geliřtirilebilmesi adına ulusal uygulama arařtırmalarının yapılması gibi hususlarda istekli ve desteki konumdadır.⁶⁰² 2021 yılında devam eden UNOEWG görřmelerinde ise Türkiye tarafının, rapor taslađında bulunan “internetin terr amaçlı kullanılması” ifadesi yerine “BİT'nin terr amaçlı kullanılması”

⁶⁰¹ T. C. Cumhurbaşkanlıđı, “zgn Teknolojilerimizi, Yazılımlarımızı Geliřtirmeden Geleceđimize Gvenle Bakamayız”, 21.03.2022, <https://www.tccb.gov.tr/haberler/410/136171-ozgun-teknolojilerimizi-yazilimlarimizi-gelistirmeden-gelecegimize-guvenle-bakamayiz-> (31.12.2024).

⁶⁰² UN/Open-ended Working Group on Information and Communication Technologies, Statement on Existing and Potential Threats by Turkey, Statements, 29.03.2022, <https://documents.unoda.org/wp-content/uploads/2022/03/Turkey-Statement-OEWG-29-March-2022.pdf> (31.12.2024); UN/Open-ended Working Group on Information and Communication Technologies, General Statement of Views by Turkey, Statements, 14.12.2021, <https://documents.unoda.org/wp-content/uploads/2021/12/STATEMENT-BY-TURKEY-OEWG-2021-2025-002.pdf> (31.12.2024).

ifadesini önermesi dikkat çekicidir.⁶⁰³ İnternetin siber uzayın temel bileşeni olan BİT'nin bir alt kümesi olarak kabul edilip, konunun daha geniş perspektiften ele alınması, kanaatimce isabetli bir düşünce olmuştur.

Ulaştırma ve Altyapı Bakanlığı, Bilgi Teknolojileri Kurumu (BTK) ve Ulusal Siber Olaylara Müdahale Merkezi'nin (USOM) uluslararası nitelikte organize ettiği Siber Kalkan (*Cyber Shield*) tatbikatlarıyla da Türkiye, uluslararası iş birliğine ve ortak siber güvenlik pratiklerinin geliştirilmesine katkıda bulunmuştur.⁶⁰⁴

Türkiye'nin siber uzay politikasının, yakın geçmişte doğrudan cumhurbaşkanlığı makamından beyan edilen “siber vatan”⁶⁰⁵ ve “Türkiye'nin verisi Türkiye'de kalmalı”⁶⁰⁶ gibi söylemler zemininde, egemenlik haklarını önceleyecek şekilde belirleneceği görülmektedir. Bu minvalde, uluslararası çalışmalarda sergilenen uyumlu tavır oldukça kıymetli olmakla birlikte; hukuki boyutta somut adımların atılabilmesi adına diğer aktörlerle iş birliklerinin geliştirilmesi ve çalışmalardaki aktivitenin yükseltilmesi, beyan edilen amaçlara daha çok hizmet edecektir.

D. Uluslararası Örgütler ve Sivil Toplum Kuruluşları

Siber uzayın sınır aşan özgün yapısı, hukuk ihdası ve uygulamasında klasik metotlarla sonuç alınmasını güçleştirmiştir. Üstelik devletler siber uzay doktrinleri açısından iki kutba ayrılmış görünmektedir. Dolayısıyla mevcut durumda uluslararası topluluğun farklı beklenti ve kaygılarına cevap verebilecek sistemin kurulmasına tabii ki

⁶⁰³ UN/Open-ended Working Group on Information and Communication Technologies, Statement by Turkey: Informal Meeting of the Open-ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security, ZD Statement, 19.02.2021, https://front.un-arm.org/wp-content/uploads/2021/02/Turkey-statement_OEWG-informal-meeting_February-2021.pdf (31.12.2024).

⁶⁰⁴ Tatbikatlar, 2014 yılında ITU ortaklığıyla uluslararası nitelikte; 2019 yılında ITU desteğiyle uluslararası nitelikte; 2021 yılında ulusal nitelikte; 2022 yılında ise bir kez ulusal bir kez de finans sektörü özelinde gerçekleştirilmiştir. Sırasıyla bkz. ITU/ITU-D, “International Cyber Shield Exercise 2014, 15 – 16 May 2014, Istanbul, Turkey”, <https://www.itu.int/en/ITU-D/Regional-Presence/Europe/Pages/International-Cyber-Shield-Exercise.aspx> (31.12.2024); ITU/ITU-D, “Cyber Shield 2019”, <https://www.itu.int/en/ITU-D/Regional-Presence/Europe/Pages/Events/2019/CyberShield/Cyber-Shield-2019.aspx> (31.12.2024); BTK, “Ulusal Siber Kalkan 2021 Tatbikatı Başladı”, 12.10.2021, <https://www.btk.gov.tr/haberler/ulusal-siber-kalkan-2021-tatbikati-basladi> (31.12.2024); BTK, “Ulusal Siber Kalkan 2022 Başladı”, 11.10.2022, <https://www.btk.gov.tr/haberler/siber-kalkan-2022-basladi> (31.12.2024); BTK, “Finans Sektörü Siber Kalkan 2022 Tatbikatı Başladı”, 20.10.2022, <https://www.btk.gov.tr/haberler/finans-sektoru-siber-kalkan-2022-tatbikati-basladi> (31.12.2024).

⁶⁰⁵ TRT Haber, “Cumhurbaşkanı Erdoğan'dan 'Siber Vatan' Mesajı”, 15.01.2021, <https://www.trthaber.com/haber/gundem/cumhurbaskani-erdogandan-siber-vatan-mesaji-547553.html> (31.12.2024).

⁶⁰⁶ T.C. Cumhurbaşkanlığı, “Türkiye’yi, Bilgi ve İletişim Teknolojilerinde Dünyanın En Önde Gelen Ülkeleri Arasına Sokacağız”, 10.02.2020, <https://www.tccb.gov.tr/haberler/410/116592/-turkiye-yi-bilgi-ve-iletisim-teknolojilerinde-dunyanin-en-onde-gelen-ulkeleri-arasina-sokacagiz-> (31.12.2024).

ancak türev aktörlerin çabalarıyla yaklaşılabilecektir. Siber uzayın uluslararası idaresinde diğer fenomenlere göre en büyük farklılık burada ortaya çıkmaktadır. Süreç öncelikle devletlerin doğrudan ilişkilerini aşmış ve uluslararası hukukta alışık olunduğu üzere gerek küresel gerek bölgesel nitelikteki uluslararası örgütlere taşınmıştır. Ancak fiili durumun bir bakıma kaçınılmaz olarak doğurduğu yönetim ve çok paydaşlılık rüzgârı ile önce uluslararası sivil toplum kuruluşlarına kritik yetkiler tanınmış, ardından çok uluslu şirketlerin hükümetlerarası girişimlere dahil olmaları sağlanmıştır.

Siber uzayda kodun yasa olması, kodu ve fiziksel altyapıyı üreten başat aktörleri süreç dışında tutmayı imkânsız kılmaktadır. Çok uluslu şirketler ya da bir devlete doğrudan angaje olmakla birlikte sınır aşan çapta faaliyet gösteren şirketler, tabii olarak karlılıklarına ya da gölgesi altında bulundukları devletin politikalarına hizmet edecek şekilde tutum ve faaliyetlerini belirlemektedir. Eldeki çalışmada uluslararası topluluk nezdinde konu ele alınırken, özellikle uluslararası hukuktaki konumları ve sayı bakımından çoklukları dikkate alındığında, şirketlerle ilgili bu tespitler yeterli görülmüş, ayrı bir başlık açılmamıştır.

Küresel ya da bölgesel olsun, siber uzayın düzenlenmesi ve yönetimi adına uluslararası çabalara ev sahipliği yapan uluslararası örgütlerin esasen siber uzaya ilişkin amaçlara özgülenmiş değil genel amaçlı örgütler olduğu görülmektedir. Bunların başında yukarıda anlatıldığı üzere BM gelmektedir. BM'nin yanı sıra AB, Avrupa Konseyi, Kuzey Atlantik Antlaşması Örgütü (NATO), Şangay İşbirliği Örgütü (ŞİÖ), BRICS, Bağımsız Devletler Topluluğu (BDT), Afrika Birliği (AfB), Güneydoğu Asya Ülkeleri Birliği (ASEAN) ve benzer başka örgütler bünyesinde düzenleyici normlar oluşturma ve iş birliğini geliştirme girişimleri gerçekleşmektedir. Dolayısıyla bu neviden örgütlere uluslararası hukuk düzenlemelerinden ve düzenleme girişimlerinden bahsederken değinmek daha faydalı olacaktır. Aşağıda doğrudan siber uzay konularına özgülenmiş başlıca uluslararası örgüt ve STK'ların siber uzay yönetimindeki rolü ele alınacaktır.

1. Uluslararası Telekomünikasyon Birliği

Kökü, 1865'te kurulmuş ve modern anlamda ilk uluslararası örgütlerden Uluslararası Telgraf Birliği'ne (*International Telegraph Union*) dayanan 1932'de mevcut

ismini almış ve 1947'den bu yana BM uzmanlık kuruluşu olarak faaliyetlerini sürdürmüştür.⁶⁰⁷ Genel yönetim mekanizmasının yanında faaliyet alanı itibariyle ITU üç sektöre sahiptir. Bunlar, radyo telekomünikasyonu için ITU-R, telekomünikasyon standartları için ITU-T ve söz konusu alanda kalkınma için ITU-D sektörleridir.

ITU için 1992 yılında Cenevre'de yeni bir Konvansiyon ve Kuruluş Yasası ihdas edilmiştir. İki de antlaşma hükmünde olan bu metinlerden Konvansiyon, ITU altındaki üç sektörün işleyişini belirlerken; Kuruluş Yasası, diğerlerinin yanı sıra, ITU'nun amaç ve yapısı ile BM ve diğer kuruluşlarla ilişkilerini düzenler ve telekomünikasyona ilişkin genel hükümler ile radyoya ilişkin özel hükümleri içerir.⁶⁰⁸

ITU'nun kuruluşundan itibaren iletişim usullerinin dünya çapındaki değişim ve gelişimi, örgütün faaliyet yelpazesinde siber uzayı daha çok ön plana taşımıştır. Tabii ki iletişimin siber uzay dışında devam eden süreçleri olduğu gibi siber uzay da tamamen iletişim ve iletişim teknolojilerinden ibaret değildir. Fakat ikisinin kesişim kümesinde bulunan ITU, kapsadığı alanda önemli rollere sahip olduğu gibi gelecek adına da yüksek bir potansiyel taşımaktadır.

ITU, öncelikle uluslararası iş birliğini geliştirecek etkinlikleri desteklemekte ve bazılarını ev sahipliği yapmaktadır. ITU-T vasıtasıyla bilhassa fiziksel altyapı için küresel standartları belirlemektedir. ITU-D vasıtasıyla devletlerin siber kapasitelerini geliştirmeleri yönünde destek programları sunarken gerek üye devletler içerisinde gerek uluslararası çapta süreç ve hizmetlerin dijitalleşmesi adına girişimlerde bulunmaktadır.⁶⁰⁹ Ulusal siber güvenlik rehberleri ve ITU-T önerilerinin etkinliğini ele alan BİT güvenliği raporları başta olmak üzere, kolektif siber güvenlik anlayışının geliştirilmesi adına çok sayıda el kitabı, rehber, indeks, rapor vb. belge yayımlamaktadır.⁶¹⁰

ITU, internet öncesi dönemde -ISO gibi diğer uluslararası kurumsal yapılarla birlikte- iletişim standartlarının belirlenmesinde merkezi roldeydi. İnternetin dağıtık

⁶⁰⁷ ITU, "Overview of ITU's History (3)", <https://www.itu.int/en/history/Pages/ITUsHistory-page-3.aspx> (31.12.2024).

⁶⁰⁸ ITU, "Constitution and Convention", <http://handle.itu.int/11.1004/020.2000/s.020> (31.12.2024).

⁶⁰⁹ Dört yılda bir toplanan Dünya Telekomünikasyon Kalkınma Konferansı (*World Telecommunication Development Conference* (WTDC)) bu minvaldeki etkinliklerin en bilinenidir. Bilgi için bkz. ITU, "World Telecommunication Development Conferences", <https://www.itu.int/en/ITU-D/Conferences/WTDC> (31.12.2024).

⁶¹⁰ ITU tarafından yayımlanan belge kategorilerine ve ilgili bütün belgelere erişim için bkz. ITU, "Publications", <https://www.itu.int/hub/pubs/> (31.12.2024).

yapısı ve özel hukuk kişileri ile ICANN gibi çoğu Amerikan menşeli aktörün norm belirleme ve idari rolleri üstlenme yönünde kurduğu teknik hakimiyet gibi nedenler, bu tür köklü kurumları zamanla merkezden çepere taşımıştır. Modern dönemde ortaya çıkan siber uzayda çok paydaşlılık düşüncesi ve mevcut yönetişimin genişletilmesi talebi ile de bir geri dönüş süreci yaşanmaktadır.⁶¹¹ Devletler egemenlikleri dolayısıyla siber uzayda kontrol sağlamak istemektedir. Ortaya çıkan rekabet, yönetişimin devletler arası platformlarda sağlanması düşüncesini ön plana çıkarmaktadır. ITU koordinasyonu ile 2003'te Cenevre ve 2005'te Tunus'ta düzenlenen Dünya Bilgi Toplumu Zirvesi (*World Summit on the Information Society* (WSIS)); kritik kaynakların yönetiminin mevcut usulüne karşı, Çin öncülüğünde Brezilya, Güney Afrika ve Hindistan gibi devletlerin de katılımıyla ilk uluslararası itirazlara sahne olmuştur.⁶¹² İtirazcı devletlerin girişimleri sonucu ITU bünyesinde 2012 Dünya Uluslararası Telekomünikasyon Konferansı (*World Conference on International Telecommunications* (WCIT-12)), 1988'de kabul edilen Uluslararası Telekomünikasyon Tüzüğü'nü (*International Telecommunication Regulations* (ITR)) güncellemek üzere toplanmıştır.⁶¹³ Zira iletişime dair o dönem yürürlükteki uluslararası düzenlemeler, siber uzay fenomeninin ortaya çıkışından önceki şartları yansıtmaktaydı. WCIT-12 girişimi, ITU'nun internetin çok paydaşlı yönetişimini domine edeceği, mimarisini değiştireceği, özgürlükçü ve açık yapısını hükümetler lehine bozacağı gibi iddialarla özellikle ABD merkezli medya organları, BİT şirketleri ve STK'lar tarafından yoğun şekilde eleştirilmiştir. ABD cephesine Avustralya, Kanada, Avrupa Birliği'nin o dönemdeki yirmi sekiz üyesi ve Japonya da dahil olmuştur.⁶¹⁴ Bu durum, kuruluşundan itibaren yüksek mutabakat oranıyla faaliyet gösteren ITU'yu birdenbire net bir kutuplaşma konusu haline getirmiştir. Nihayetinde yeni tüzük, içlerinde Çin, Rusya, Türkiye, İran, Brezilya ve Güney Afrika'nın bulunduğu 89 ülke tarafından imzalanırken; ABD, Birleşik Krallık, Almanya, Fransa, Japonya, İsrail ve Avustralya'nın

⁶¹¹ Valérie Schafer, "The ITU Facing the Emergence of the Internet, 1960s – Early 2000s", Gabriele Balbi ve Andreas Fickers (Ed.), **History of the International Telecommunication Union (ITU): Transnational Techno-diplomacy from the Telegraph to the Internet** içinde (321-343), Berlin, Boston: De Gruyter Oldenbourg, 2020, s.340.

⁶¹² Wolfgang Kleinwächter, "Beyond ICANN vs ITU?: How WSIS Tries to Enter the New Territory of Internet Governance", **International Communication Gazette**, Vol.66, Iss.3-4, (2004), s.233.

⁶¹³ ITU, "World Conference on International Telecommunications (WCIT-12)", <https://www.itu.int/en/wcit-12> (31.12.2024).

⁶¹⁴ Dwayne Winseck, "Is the International Telecommunication Union Still Relevant in 'the Internet Age?' Lessons From the 2012 World Conference on International Telecommunications (WCIT)", Gabriele Balbi ve Andreas Fickers (Ed.), **History of the International Telecommunication Union (ITU): Transnational Techno-diplomacy from the Telegraph to the Internet** içinde (321-343), Berlin, Boston: De Gruyter Oldenbourg, 2020, ss.135-136.

dahil olduđu 55 devlet tarafından imzalanmamıştır.⁶¹⁵ Sonuç itibariyle elde küresel nitelikte bir uluslararası antlaşmanın mevcudiyetinden bahsedilebilse de siber uzayda etkinliğı çok yüksek olan bloğun onayının yokluğunda, yine siber uzayın yapısı gereğı kadük kalacağı aşıkardır. Buna rağmen *Kleinwächter*’ın, ITU’nun yeni durumda üsteneceğı rolün “Endüstri Çağı diplomasisinden Bilgi Çağı diplomasisine geçiş”⁶¹⁶ olduğı yönündeki yorumu, 2004’ten bugüne isabetli bir vizyon olarak kabul edilebilir.

İnternetin açık ve özgür yapısının zarar görmesinden çekinen yazarlar, ITU’nun internet yönetişimindeki rolünün güçlenmesini endişeyle karşılamaya devam etmektedir. Nitekim 193 üyenin eşit oy hakkına sahip olduğı ve basit çoğunluk ile kararların alındığı hükümetlerarası bir yapının, siber uzayda devlet hakimiyetini sivil toplum aleyhine geliştirmesi muhtemel olacaktır.⁶¹⁷ Siber egemenlik düşüncesinin kuvvetli savunucusu olan otoriter devletlerin ITU’yu işaret eden ısrarlı tutumları ise söz konusu eleştirileri doğrular nitelikte olsa da modern egemen devletler sisteminin siber uzayı er ya da geç kendi dinamiklerine uyumlu hale getirmesi doğal bir sonuç olacaktır.

2. İnternet Tahsisli Sayılar ve İsimler Kurumu

Siber uzayda bulunan kaynaklardan bazıları (örnek: veri) teorik olarak sınırsızken bazı kaynaklar sınırlıdır. Web’de kullanılan alan adları da tabiatı itibariyle siber uzayın sınırlı ve kritik öneme sahip kaynaklarından. Dolayısıyla her sınırlı kaynak gibi kullanım esaslarının düzenlenmesi ve yönetilmesi zaruridir. Bu yetki ve sorumluluk ise halihazırda ICANN uhdesindedir. Sık sık tartışmalara konu olan ICANN’yi bugüne getiren süreç, internetin teknik gelişim serüveniyle doğrudan alakalıdır.

Henüz 1972’de ARPANET döneminde *Jon Postel*, ağa bağlı soket numaralarını kendi defterine kaydetmeye başlamıştır. Bu fonksiyona *Postel*, İnternet Tahsisli Sayılar Otoritesi (*Internet Assigned Numbers Authority* (IANA)) ismini vermiş ve işi uzun süre bizzat yürütmesi sebebiyle kendisi “*The IANA*” olarak anılmıştır.⁶¹⁸ Sonrasında IANA

⁶¹⁵ Konferansa katılan devletlerin imza durumları için bkz.: ITU, “WCIT-12 Signatories of the Final Acts”, <https://www.itu.int/osg/wcit-12/highlights/signatories.html> (31.12.2024).

⁶¹⁶ Kleinwächter, s.248.

⁶¹⁷ Vinton G. Cerf, “Keep the Internet Open”, The New York Times, 24.05.2012, <https://www.nytimes.com/2012/05/25/opinion/keep-the-internet-open.html> (31.12.2024).

⁶¹⁸ ICANN, “IANA Fonksiyonları: Giriş”, <https://www.icann.org/en/system/files/files/functions-basics-08apr14-tr.pdf> (31.12.2024).

kurumsallaşmış, *Postel* da başkanlığını yürütmeye devam etmiştir. NSFNET'in ve sonrasında Web'in ortaya çıkışı ile internetin sivilleşmesi ve ticarileşmesi, alan adlarına yönelik talep patlamasına sebep olmuştur.⁶¹⁹ NSF, fonksiyonu icra etmesi için Network Solutions şirketi ile anlaşarak "InterNIC" adıyla kayıt kurumunu işletmeye başlamış;⁶²⁰ diğer taraftan da DARPA ile anlaşmalı olarak Güney Kaliforniya Üniversitesi Bilgi Bilimleri Enstitüsü nezdinde IANA, DNS yönetim fonksiyonlarının bir kısmını yürütmeye devam etmiştir.⁶²¹ Anlaşmaların 1998'de sona erecek olmasına binaen 1997'de ABD Başkanı *Bill Clinton*, Ticaret Bakanlığı'na, "Küresel Elektronik Ticaret Çerçevesi (*Framework for Global Electronic Commerce*)" kapsamında DNS yönetiminin özelleştirmesi talimatını vermiştir.⁶²² Bakanlık, Ulusal Telekomünikasyon ve Bilgi İdaresi (*National Telecommunications and Information Administration* (NTIA)) vasıtasıyla derhal harekete geçmiş ve "İnternet İsim ve Adreslerinin Teknik Yönetimini Geliştirmek için Bir Öneri" başlığıyla "Yeşil Kitap" olarak bilinen çalışmayı başlatmıştır. Yeşil Kitap ile internet topluluğunun birçok paydaşından 430 geribildirim alınmış ve DNS yönetiminin kâr amacı gütmeyecek özel bir kuruluşa devredilmesinin isabetli olacağı kanaatine varılmıştır. Buradan elde edilen sonuç ile de NTIA bu kez "İnternet İsim ve Adreslerinin Yönetimine İlişkin Politika Beyanı" başlığıyla "Beyaz Kitap" olarak bilinen resmi raporunu yayınlamış ve böylece ICANN'nin kuruluşuna fiili zemin hazırlanmıştır.⁶²³ Kısa süre içinde Kaliforniya'da kar amacı gütmeyen kamu yararına kuruluş vasfıyla ICANN kurulmuş;⁶²⁴ ABD Ticaret Bakanlığı ile ICANN arasında yapılan mutabakat zaptına⁶²⁵ istinaden, Güney Kaliforniya Üniversitesi ile ICANN

⁶¹⁹ Mueller, 2004, s.110.

⁶²⁰ 1995'ten itibaren ".com, .org, .net, .edu ve .gov" uzantılı alan adlarının kayıt ve yenileme işlemlerinde ücret tahsil etmeye başlamış ve internet kamuoyunda tepkilerin odağı olmuştur; Mueller, 2004, s.111.

⁶²¹ Committee on Science US House of Representatives Subcommittee on Basic Research Subcommittee on Technology Hearing Charter, "The Domain Name System: Where do We Go from Here?", 31.03.1998, s.34, https://commdocs.house.gov/committees/science/hcy090140.000/hcy090140_0.HTM (31.12.2024); Bütün süreç hakkında detaylı bilgi için bkz. Mueller, 2004, s.73 vd.

⁶²² United States Department of Commerce / National Telecommunications and Information Administration, "Statement of Policy on the Management of Internet Names and Addresses", Docket Number:980212036-8146-02, 05.06.1998; <https://www.ntia.gov/federal-register-notice/statement-policy-management-internet-names-and-addresses> (31.12.2024); Belge, "Beyaz Kitap (The White Paper)" olarak bilinmektedir.

⁶²³ Ibid.

⁶²⁴ ICANN, "Articles of Incorporation of Internet Corporation for Assigned Names and Numbers", <https://www.icann.org/resources/pages/articles-2012-02-25-en> (31.12.2024).

⁶²⁵ United States Department of Commerce / National Telecommunications and Information Administration, "Memorandum of Understanding Between the U.S. Department of Commerce and the Internet Corporation for Assigned Names and Numbers", 25.11.1998, <https://www.ntia.gov/page/memorandum-understanding-between-us-department-commerce-and-internet-corporation-assigned> (31.12.2024).

arasında bir geiş anlaşması yapılmış⁶²⁶ ve DNS yönetimi ICANN sorumluluğuna gemiştir. Bu geiş, IANA’nın ICANN bünyesine süreli bir sözleşmeye baėlı şekilde entegrasyonu anlamına gelmektedir. ABD ve ICANN arasındaki hukuki baėlılık ilişkisi; yoğun tartışmalarla geen yılların ardından, IANA işlevlerinin ICANN tarafından sürdürölmesini konu edinen ve aralıklarla yenilenen anlaşmanın kesin süresinin 2016’da dolmasıyla nihayete ermiş görünmektedir.⁶²⁷

Mevcut durumda ICANN karar alma merci Yönetim Kurulu’dur. Yönetim Kurulu ise ICANN Tüzüğü’nde belirlenen çok sayıda çok paydaşlı organizasyonun tercihleriyle belirlenmektedir.⁶²⁸ Ayrıca DNS, 12 operatör tarafından işletilen, A’dan M’ye kadar harflerle isimlendirilen ve birer IP adresine sahip olan 13 mantıksal kök sunucu (*root server*) üzerinde yürümektedir. Fiziksel olarak ise dünyanın dört bir yanına dağılmış mantıksal köklere baėlı çok sayıda sunucu söz konusudur. 12 operatörün -1’i ICANN olmak üzere- 9’u ABD merkezlidir. Kalan 3 operatörün biri Hollanda, biri İsveç, biri de Japonya merkezlidir.⁶²⁹

Görölceğı üzere internet uzun yıllar doğrudan ABD hükümeti ve ABD merkezli teknokratlar tarafından idare edilmiştir. IANA işlevleri, yakın zamana kadar bazı ABD’li siyasetçilerce ABD’nin bir mülkü olarak dahi görölmuş; dolayısıyla IANA’nın ICANN yönetimine kesin devrinin usulsüz olduėu ileri sürölümüştür.⁶³⁰ WSIS görüşmeleriyle oluşan rüzgârın ve *Snowden* olaylarından sonra internet üzerinde ABD etkisine yönelik dünya kamuoyunda artan tepkilerin, baėımsız bir ICANN yapısına giden süreci hızlandırdığı düşünölabilir. Gelineen noktada ICANN ve ABD hükümeti arasındaki yetki

⁶²⁶ ICANN, “USC/ICANN Transition Agreement”, 24.12.1998, <https://www.icann.org/resources/unthemed-pages/usc-icann-transition-2012-02-25-en> (31.12.2024).

⁶²⁷ 1998’den 2016’ya kadar yaşanan gelişmeler ile ABD Ticaret Bakanlığı’nın ICANN üzerinde sürdürölüğü idari kontrol çokça eleştirilmiştir; Kieren McCarthy, “Bush Administration Annexes Internet: Extraordinary Statement”, The Register, 01.06.2005, https://www.theregister.com/2005/07/01/bush_net_policy/ (31.12.2024); Grant Gross, “New ICANN Agreement Runs Into Criticism”, PC World, 01.10.2009, <https://www.pcworld.com/article/519864/article-5164.html> (31.12.2024); Milton Mueller, “ICANN’s New MoU: Old Wine in a New Bottle”, Internet Governance, 30.09.2006, <https://www.internetgovernance.org/2006/09/30/icanns-new-mou-old-wine-in-a-new-bottle/> (31.12.2024). ABD’de cumhuriyetçilerin yoğun baskısına rağmen 2016’da IANA kalıcı olarak ICANN kontrolüne gemiştir; Klint Finley, “The Internet Finally Belongs to Everyone: ICANN might not be Perfect. But It just might be the Future”, The Wired, 03.10.2016, <https://www.wired.com/2016/10/internet-finally-belongs-everyone/> (31.12.2024).

⁶²⁸ ICANN, “Bylaws”, Section.7.2; <https://www.icann.org/resources/pages/governance/bylaws-en> (31.12.2024).

⁶²⁹ Kök sunuculara dair bilgi için bkz. Root Server Technical Operations Association, <https://root-servers.org> (31.12.2024).

⁶³⁰ Klint Finley, “The Internet Finally Belongs to Everyone: ICANN might not be Perfect. But It just might be the Future”, The Wired, 03.10.2016, <https://www.wired.com/2016/10/internet-finally-belongs-everyone/> (31.12.2024).

ilişkisi sona ermiş olsa da organizasyonun nihayetinde bir sivil toplum kuruluşu olması itibariyle merkezinin bulunduğu devlete karşı hukuken sorumlu olduğu bir gerçektir. Bu bakımdan ICANN için “çok uluslu” ve “çok paydaşlı” ifadeleri kullanılabilirken, “uluslararası” ifadesini kullanmanın mümkün olmadığı da görülecektir. Rusya ve Çin başta olmak üzere mevcut sistem muhalifi devletlerin internet yönetişimi için BM’yi işaret etmesinin gerekçeleri de bu noktalarda temellenmektedir.

Son olarak belirtilmelidir ki ICANN, internetin “sahibi” ya da “çalıştırıcısı” değildir. DNS yönetimi ve uyuşmazlık çözümü de esasen tek noktadan değil; ICANN tarafından akredite edilmiş çok sayıda kurum ve kuruluş vasıtasıyla yürütülmektedir.⁶³¹ İnternet dünyanın sayısız yerine dağılmış sunucular, kablo hatları, kablosuz vericiler ve hatta Starlink⁶³² örneğindeki gibi uydular vasıtasıyla cihazları birbirine bağlamaktadır. Bütün bu altyapı, şirketler ve devletler eliyle inşa edilip sürdürülmektedir. Protokol ve standartlar İnternet Mühendisliği Görev Gücü (*Internet Engineering Task Force* (IETF)), ISO, Elektrik ve Elektronik Mühendisleri Enstitüsü (*Institute of Electrical and Electronics Engineers* (IEEE)), Dünya Çapında Ağ Konsorsiyumu (*World Wide Web Consortium* (W3C)), İnternet Topluluğu (*Internet Society* (ISOC)), Evrensel Kod Konsorsiyumu (*Unicode Consortium*) gibi kurum ve kuruluşlar tarafından belirlenip işleyişe entegre edilmektedir. Web’in sanal/mantıksal yapısı ise geliştiricilerin katkısıyla, ölçülmesi imkânsız biçimde değişim ve gelişim göstermektedir. Yine de alan adları, tek başına bir kritik kaynak olarak siber uzay yönetişiminin birincil tartışma konularından olmaya devam edecek görünmektedir.

3. Sivil Teknik Topluluklar

Siber uzayda protokol ve standartları belirleyen, fiili iktidar sahibi bazı sivil yapılara kısaca değinmek, çok paydaşlılığın izahı açısından faydalı olacaktır. Bu yapıların

⁶³¹ Örnek olarak ülkemizde .tr uzantılı alan adlarının yönetimi BTK marifetiyle 2022 yılında kurulan TRABİS isimli sitem üzerinden yürütülmektedir. Bilgi için bkz. <https://www.trabis.gov.tr> (31.12.2024). Uyuşmazlık çözümleri ise “Yeknesak Alan Adı Uyuşmazlık Çözüm Politikası Kuralları (*Rules for Uniform Domain Name Dispute Resolution Policy* (RUDRP))” bağlamında; Dünya Fikrî Mülkiyet Örgütü (WIPO), Arap (ACDR) ve Asya (ADNDRC) Alan Adı Uyuşmazlık Çözüm Merkezleri, Kanada Uluslararası İnternet Uyuşmazlık Çözüm Merkezi, Çek Tahkim Mahkemesi İnternet Uyuşmazlıkları Tahkim Merkezi (CAC) ve Ulusal Tahkim Forumu (ADR Forum) tarafından ICANN adına sağlanmaktadır; ICANN, “List of Approved Dispute Resolution Service Providers”, <https://www.icann.org/resources/pages/providers-6d-2012-02-25-en> (31.12.2024).

⁶³² Detaylı bilgi için bkz. <https://www.starlink.com> (31.12.2024).

önde gelenleri, yukarıda zikredildiği üzere IETF, IEEE, W3C, ISOC, Unicode gibi topluluklardır. Ulusal standart kurumlarının da üye olduğu sivil bir örnek olarak ISO, faaliyet alanı siber uzaya ilişkin konulara özgü olmasa dahi bu noktada ayrıca zikredilmelidir.⁶³³ Sayısız üretici tarafından üretilen fiziksel ve mantıksal ürünlerin birbiriyle uyum içinde çalışabilmeleri, siber uzayın genişleyerek işlemeye devam etmesi demektir. Bunu da en başta protokol ve standartlar sağlamaktadır.

Standart belirleme süreci hakkında “*siyaset ve ekonominin çılgın bir karışımı*”⁶³⁴ ve “*başka yollarla siyaset*”⁶³⁵ gibi tabirler kullanılmıştır. Siber uzayda siyaset ve iktidara dair soruların cevapları da “*dağıtık, yarı formel veya refleksif koordinasyon mekanizmaları, taraflar arası özel düzenlemeler (private ordering) ve internet kaynaklarının kullanımı gibi mikro yönetim uygulamalarında*” mündemiçtir.⁶³⁶ Buradan hareketle Ten Oever, mimariyi “*bir çekişme alanı, bir güç birleşimi ve normatif bir sistemler sistemi*” olarak analiz etmiştir.⁶³⁷ Görülmektedir ki kodun yasa olması, siber uzayın düzenlenmesi bağlamında, mimariyi belirleyen aktörleri hukuku belirleyen aktörlerle fiilen yarışır hale getirmektedir. Zira protokol formundaki düzenlemeler bazen geleneksel hukuki düzenlemelerden daha etkili ve kalıcı olabilmektedir. Teknolojik altyapıya bir kez yerleşen protokol, üzerine küresel sistemlerin inşa edilmesiyle uzun yıllar işlemektedir.⁶³⁸ Hal böyleyken, kâr amacı gütmeyen sivil yapıların standart belirleyiciliği (mimarlığı), ağır işleyen devletlerarası süreçleri dışarıda tutması ve ticari aktörlerin tekelleşmesini frenlemesi açısından da işlevsel bir roldür. Devletler ise egemenlik hakları gereği bazı protokol ve standartları kendi ülkelerinde ya da

⁶³³ PDF (*Portable Document Format*) (ISO 32000-1:2008), JPEG (*Joint Photographic Experts Group*) (ISO/IEC 10918-1:1994), MPEG (*Moving Picture Experts Group*) (ISO/IEC 11172-3:1993) vb. dosya formatları; Unicode ortaklığıyla geliştirilen Evrensel Karakter Kümesi (*Universal Coded Character Set*) (ISO/IEC 10646:2020); QR Kod (*Quick-Response Code*) ve Barkod (*Barcode*) sistemleri (ISO/IEC 18004:2024) gibi çok sayıda siber uzay unsurunun standartları ISO tarafından belirlenmektedir.

⁶³⁴ Carl Shapiro ve Hai R. Varian, **Information Rules: A Strategic Guide to the Network Economy**, Boston: Harvard Business School Press, 2009, s.240.

⁶³⁵ Janet Abbate, **Inventing The Internet**, Cambridge, Massachusetts, London: The MIT Press, 1999, s.179.

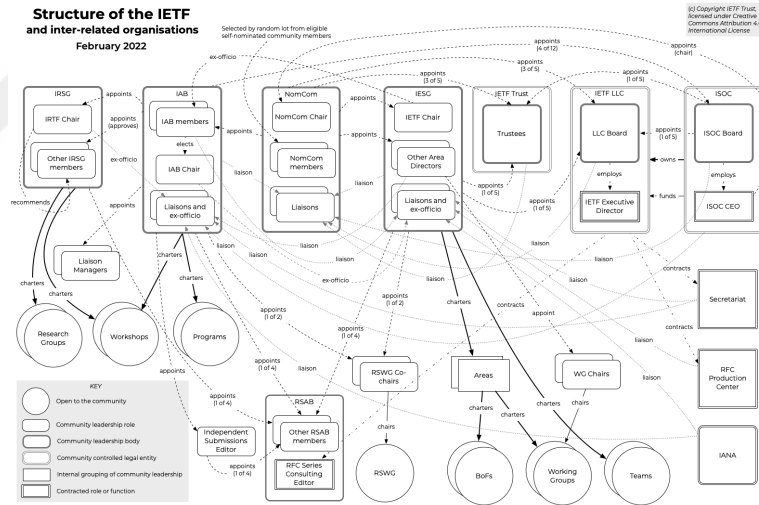
⁶³⁶ Dmitry Epstein, Christian Katzenbach ve Francesca Musiani, “Doing Internet Governance: Practices, Controversies, Infrastructures, and Institutions”, **Internet Policy Review**, Vol.5, Iss.3, (2016), s.4.

⁶³⁷ Niels Ten Oever, “‘This is not How We Imagined It’: Technological Affordances, Economic Drivers, and the Internet Architecture Imaginary”, **New Media & Society**, Vol.23, Iss.2, (2021), s.345.

⁶³⁸ Laura DeNardis, **Protocol Politics: The Globalization of Internet Governance**, Cambridge, Massachusetts: The MIT Press, 2009, s.90.

vatandaşlarının kullanımında zorunlu tutabilirler. Ayrıca bunu iradelerini birleştirmek suretiyle uluslararası örgütler marifetiyle de yapabilirler.⁶³⁹

Kâr amacı gütmeyen “mimar” toplulukların en önde geleni IETF, “interneti daha iyi çalışır kılmayı” amaçlamaktadır.⁶⁴⁰ 1986’da ABD hükümeti desteğiyle kurulan topluluk, daha sonradan 1992’de faaliyete geçen ISOC tarafından desteklenmeye başlamıştır.⁶⁴¹ Tamamen gönüllülük esasına dayalı çalışan IETF, resmi bir üyelik prosedürü olmaksızın herkesin katılımına açıktır. Yine de teoride böyle görünmekle birlikte, pratikte etkin mensupların ekseriyetinin çok uluslu şirketlerin çalışanları olduğu belirtilmiştir.⁶⁴² IETF, bünyesinde çok sayıda alt grup bulundurmakta, faaliyetleri resmîyette olmasa da doğal bir şekilde İnternet Mühendisliği Yönlendirme Grubu (*Internet Engineering Steering Group* (IESG)) tarafından idare edilmektedir.⁶⁴³ IETF’nin alt gruplar ve diğer yapılarla kurduğu karmaşık ilişki şeması aşağıdaki şekilde görülmektedir:⁶⁴⁴



Şekil.2: IETF organizasyon yapısı ve diğer ilişkili organizasyonlarla ilişkileri.

⁶³⁹ Güncel bir örnek olarak Avrupa Birliği’nin 2014/53 sayılı Radyo Ekipman Direktifi hükümlerinde, 2022/2380 sayılı Direktif ve 2023/1717 sayılı Tüzük ile değişikliğe giderek, belirli tiplerdeki elektronik aletlerin şarj cihazlarında USB-C standardının kullanımını 28 Aralık 2024’ten itibaren geçerli olacak şekilde zorunlu hale getirmesi gösterilebilir; European Commission, “One Common Charging Solution for All”, https://single-market-economy.ec.europa.eu/sectors/electrical-and-electronic-engineering-industries-eei/radio-equipment-directive-red/one-common-charging-solution-all_en (31.12.2024).

⁶⁴⁰ IETF, “A Mission Statement for the IETF”, <https://www.ietf.org/rfc/rfc3935.txt> (31.12.2024).

⁶⁴¹ Vint Cerf, “IETF and the Internet Society”, Internet Society, 18.07.1995, <https://www.internetsociety.org/internet/history-of-the-internet/ietf-internet-society/> (31.12.2024).

⁶⁴² Ten Oever, s. 346.

⁶⁴³ Lee A. Bygrave ve Terje Michaelsen, “Governors of Internet”, Lee A. Bygrave ve Jon Bing (Ed.), **Internet Governance: Infrastructure and Institutions** içinde (92-125), New York: Oxford University Press, 2009, s.99.

⁶⁴⁴ IETF, “Structure of the IETF”, https://www.ietf.org/media/documents/IETF_Structure_-_February_2022.png (31.12.2024).

En bilinen faaliyeti olarak, TCP/IP standartlarını IETF belirlemektedir. IETF'nin geliştirdiği protokol ve standartların etkilerini *Ten Oever* özetle derleyip, “davranışlarımızı şekillendirmek, kullanıcı veri akışları üzerindeki kontrol vektörlerini belirlemek, kullanıcıların bilgiye nasıl eriştiklerini ve çevrimiçi haklarını nasıl kullanabileceklerini belirlemek” şeklinde saymıştır.⁶⁴⁵

Kökleri 1884'e dayanan IEEE, dünyanın en büyük teknik profesyonel topluluğu olarak faaliyetlerini sürdürmektedir.⁶⁴⁶ Kapsamı internetle sınırlı olmayan siber uzayda, cihazlara ve bağlantı elemanlarına yönelik çok sayıda protokol ve standardın kaynağı IEEE'dir. *Ethernet*, *Bluetooth*, *Wi-Fi* gibi standartların geliştirilmeleri de IEEE sorumluluğundadır.⁶⁴⁷

Tim Berners-Lee, Web'i icat ettikten sonra 1994'te W3C'yi kurmuştur.⁶⁴⁸ W3C, protokoller ve yönergeler geliştirerek “Web'i tam potansiyeline ulaştırmayı” amaçlamaktadır.⁶⁴⁹ Web'in temelini oluşturan hiper metin konsepti Hiper Metin İşaretleme Dili (*HyperText Markup Language* (HTML)) ile kurulmuştur. W3C, HTML'nin yanı sıra 1998'de yayınlanan Genişletilebilir İşaretleme Dili (*Extensible Markup Language* (XML)) standartlarını da belirlemektedir.⁶⁵⁰ Bu dillere göre Web sayfalarına renk, yazı karakteri, boşluk vs. eklemeyi sağlayan Basamaklı Stil Şablonları (*Cascading Style Sheets* (CSS)) yine W3C'nin belirlediği standart örneklerindendir.⁶⁵¹

Sonuçta görüleceği üzere devlet, uluslararası örgüt, resmi ya da sivil yapılardan hiçbirisi siber uzay üzerinde belirgin bir tahakküm kurmuş değildir. Siber uzayı var eden bütün fiziksel ve mantıksal boyut, bahsi geçen yapıların kolektif çabasıyla oluşmuştur ve öyle işlemeye devam etmektedir. Bu durum, devletlerin dahi gerek uluslararası hukukta gerek kendi ülkelerinde regülasyon etkinliklerini sınırlamaktadır. Yine de siber uzayın kısa tarihinde gösterilen yoğun çabalar, ulusal hukuklarda olduğu gibi uluslararası

⁶⁴⁵ Ten Oever, s.345.

⁶⁴⁶ IEEE, “History of IEEE”, <https://www.ieee.org/about/ieee-history.html> (31.12.2024).

⁶⁴⁷ Bygrave ve Michaelsen, s.114.

⁶⁴⁸ Ibid., s.101.

⁶⁴⁹ W3C, “Our Mission”, <https://www.w3.org/mission/> (31.12.2024).

⁶⁵⁰ W3C, “Extensible Markup Language (XML)”, <https://www.w3.org/XML> (31.12.2024).

⁶⁵¹ W3C, “Cascading Style Sheets Home Page”, <https://www.w3.org/Style/CSS> (31.12.2024).

hukukta da bazı normatif sonuçlara ulaşılmasını sağlamıştır. Aşağıda bu düzenlemelerin önde gelenleri ele alınacaktır.

E. Uluslararası Hukuk Düzenlemeleri

Çok paydaşlı yönetim anlayışının siber uzaya hâkim olduğu modern dönemde, egemenlik hakları gereği edilgen durumda kalmamak ve siber uzayı düzenlemek isteyen devletler için uluslararası hukuk birincil vasıtaadır. Nitekim siber uzay gibi sınır aşan karmaşık bir fenomen üzerinde devlet iradesinin tecellisi, tekil girişimlere kıyasen uluslararası iş birliği yoluyla daha pratik şekilde sağlanabilecektir. Esasen küreselleşmenin sonucu olarak birçok alan için benzer durum geçerlidir. Küresel çapta yayılmış sistemler söz konusu olduğunda, devletlerin egemenlik alanlarına düşen kısımların, doğrudan ulusal girişimlerle düzenlenmesi veya yapılan düzenlemenin etkin şekilde uygulanması oldukça güçleşebilmektedir.

Siber uzayı doğrudan konu edinen uluslararası hukuk düzenlemeleri henüz yakın tarihlerde ortaya çıkmıştır ve halen üzerinde çalışılmaya devam eden birçok konu başlığı mevcuttur.⁶⁵² Hal böyle olunca genel kapsamlı düzenlemeler ilk başvuru kaynağı olacaktır. Şüphe yok ki siber uzay, uluslararası hukukun hemen hemen bütün dallarıyla uzak ya da yakın ilişki halindedir. ABD, Çin ve Rusya gibi devletlerin pratiklerinde görüleceği üzere; belli başlı konularda tartışmalar sürse de uluslararası hukukun genel hükümlerinin siber uzayda da geçerli olduğu artık uluslararası toplulukça kabul görmüş sayılmaktadır. Ayrıca siber uzaya özgü kapsamlı ve küresel bir uluslararası antlaşma olmasa dahi özellikle siber güvenlik alanında devletler arasında çok sayıda ikili yahut çok taraflı antlaşma akdedilmiştir.⁶⁵³ Bu antlaşmaların dışında, henüz taslak aşamasında olan girişimler ve model kanun çalışmaları da siber uzayın uluslararası düzenlenmesinde yol gösterici metinler olarak dikkate şayandır.⁶⁵⁴

⁶⁵² Kapsamlı uluslararası antlaşmalarla sınırlı tutmamak adına “düzenleme” ifadesi tercih edilmiştir.

⁶⁵³ 2017 yılı itibarıyla devletler arasındaki siber güvenlik antlaşmaları hakkında istatistik çalışması için bkz. Theresa Hitchens ve Nilsu Gören, “International Cybersecurity Information Sharing Agreements”, **Study Report**, Center for International & Security Studies, University of Maryland, 2017.

⁶⁵⁴ Bu tür metinlerden bazı örneklere dair bilgi için bkz. Merve Erdem ve Gürkan Özocak, “Siber Güvenliğin Sağlanmasında Uluslararası Hukukun ve Türk Hukukunun Rolü”, **Ankara Üniversitesi Hukuk Fakültesi Dergisi**, Cilt.68, Sayı.1, (2019), ss.164-166.

Aşağıda öncelikle genel kapsamlı düzenlemelerin siber uzay ile ilişkilerine kısaca değinilecek; ardından doğrudan siber uzay ile ilişkili düzenlemeler, genel özellikleri ve egemenlikle ilişkileri bağlamında ele alınacaktır.⁶⁵⁵

1. Genel Kapsamlı Uluslararası Düzenlemelerdeki Hükümler

Bu başlıkta akla ilk gelecek normlar tabii ki BM Şartı hükümleridir. Cari *jus ad bellum* sisteminin temeli olarak kuvvet kullanma yasağını düzenleyen ve siber uzayda uygulanması tartışma konusu olan m. 2/4; dolayısıyla meşru müdafaa hakkını ele alan m. 51 gibi örnekler söz konusudur. Ayrıca gerek BM Şartı’nda gerek diğer belgelerde ifade edilen, modern uluslararası hukuk sistemini belirleyen ve bazıları eldeki çalışmada Birinci Bölüm’de anlatılan ilkeler de pek tabii alakadar olduğu ölçüde siber uzay için geçerli olacaktır.

ITU Kuruluş Yasası’nın telekomünikasyona ilişkin genel hükümleri içeren 6. Bölümü, siber uzayın iletişime taalluk eden kısmına dair düzenlemeler getirmiştir.⁶⁵⁶ Buna göre üye devletler, “*halkın uluslararası kamu haberleşme hizmetleri vasıtası ile haberleşme hakkını*”⁶⁵⁷ tanımış; “*uluslararası haberleşmenin gizliliğini sağlamak için, kullanılan telekomünikasyon sistemi ile uyumlu, her türlü önlemi*”⁶⁵⁸ ve “*uluslararası telekomünikasyonun hızlı ve kesintisiz yapılabilmesini garanti etmek için gerekli olabilecek, kanal ve tesisleri en iyi teknik şartlarda, kurmak için gerekli önlemleri*”⁶⁵⁹ almayı “*Diğer Üye Devletlerin yetki alanlarındaki telekomünikasyon tesislerinin çalışmalarını bozacak, her türlü elektrikli cihaz ve tesisin çalışmasını önlemek için pratik önlemler almak gerektiğini*”⁶⁶⁰ kabul etmiştir. Ayrıca üye devletler, “*ulusal yasalarına göre, Devlet güvenliği için tehlikeli görülebilecek veya yasalarına, kamu düzenine veya ahlakına aykırı olan, herhangi bir özel telekomünikasyonu da kesme haklarını*”⁶⁶¹ da saklı tutmuşlardır. Metnin dilinin büyük çoğunlukla devletlere niteliği belirli ve kesin

⁶⁵⁵ Bu kısımda bahsi geçecek düzenlemeler hakkında farklı metodolojilerle yapılan incelemeler için bkz. Erdem ve Özocak, s.155 vd.; Piotr Milik, “International Legal Regulations in the Area of Cybersecurity”, *Cybersecurity and Law*, Vol.1, No.1, (2019), s.116 vd.; Töner Şen, s.208 vd.

⁶⁵⁶ UNTS, Vol.1825, No.31251, 1998, s.356 vd.; Eldeki çalışmada kullanılan Türkçe çeviri için bkz. R. G., 24.10.2008, Sayı.27034, Karar Sayısı.2008/14157.

⁶⁵⁷ ITU Kuruluş Yasası, m.33.

⁶⁵⁸ ITU Kuruluş Yasası, m.37/1.

⁶⁵⁹ ITU Kuruluş Yasası, m.38/1.

⁶⁶⁰ ITU Kuruluş Yasası, m.38/5.

⁶⁶¹ ITU Kuruluş Yasası, m.34/2.

yükümlülükler getirmediği görülmektedir. Ayrıca devletlerin ulusal yasaları ve kamu düzenleri adına sıklıkla genel kurallara istisnalar tanındığı da açıktır. Yine de katılım genişliği ve örgütün uluslararası saygınlığı dikkate alındığında, ITU Kuruluş Yasası'nın siber uzayda süren iletişime dair en muteber belgelerden olduğunu söylemek mümkündür.

İnsan Hakları Evrensel Beyannamesi m.19'da ifade hürriyeti konusunda belirtilen *“memleket sınırları mevzubahis olmaksızın malumat ve fikirleri her vasıta ile aramak, elde etmek veya yaymak”*⁶⁶² ve bu hükme paralel Avrupa İnsan Hakları Sözleşmesi m.10 hükmündeki *“...kamu makamlarının müdahalesi olmaksızın ve ülke sınırları gözetilmeksizin, kanaat özgürlüğünü ve haber ve görüş alma ve de verme...”*⁶⁶³ ibareleri, siber uzayın parçası olmanın temel bir insan hakkı olduğuna işaret etmektedir. Yine bu metinlerin özel hayatın korunmasına dair aynı sırasıyla m.12 ve m.8 hükümleri de siber uzayda kişilerin mahremiyet ve gizlilik haklarını genel olarak güvence altına almaktadır.

Doğrudan siber uzayla ilgili olmamakla birlikte, BİT kullanımı yoluyla ihlallerin söz konusu olabileceği çok sayıda uluslararası düzenleme de söz konusudur. Öyle ki BİT kullanımı yoluyla havacılık alanında verilen bir zarar Uluslararası Sivil Havacılık Hakkında Şikago Konvansiyonu'nun; *jus in bello* hükümlerine göre silahlı çatışmada esnasında korunan kişilere verilen fiziksel zarar Cenevre Sözleşmeleri'nin ihlali anlamına gelebilecektir. Bu örneklerin uluslararası hukukun her bir sahası için çoğaltılması mümkündür.

2. Bölgesel Uluslararası Örgütler Nezdindeki Antlaşmalar

Devletlerin aralarındaki hukuki ilişkilerinde genel olarak siber uzay yönetişimini konu edinmeleri henüz uluslararası hukuk adına lüks görünmektedir. BM bünyesinde ağır işleyen bu süreçler bir tarafa, devletler adına arz ettiği ehemmiyet üzere ivedilikle ele alınan iki konu öne çıkmaktadır: “siber güvenlik” ve “siber suçlar”. Dolayısıyla doğrudan siber uzayı konu edinen mevcut düzenlemeleri esasen bu iki grupta incelemek

⁶⁶² A/RES/217(III), ss.74-75.

⁶⁶³ AİHM, Avrupa İnsan Hakları Sözleşmesi, s.11, https://www.echr.coe.int/documents/d/echr/convention_tur (31.12.2024).

mümkündür. Gelgelelim iki grupta da küresel bir düzenleme ortaya çıkmış değildir. Zira sonuca ulaşmış çalışmaların, bölgesel örgütler nezdinde yapıldığı görülmektedir.

a. Avrupa Konseyi Sanal Ortamda İşlenen Suçlar Sözleşmesi

Siber uzayda işlenen fiillerden hangilerinin suç teşkil edeceği, bunların hangilerini hangi devletlerin tanıyacağı ve suç teşkil eden fiillere karşı devletler arasında iş birliğinin hangi esaslara dayanacağı, bilişim suçlarının temel meseleleridir. Siber suçlar, siber uzayda devletlerarası mutabakatın görece kuvvetli olduğu nadir alanlardandır. Bunu sağlayan da tabii ki söz konusu eylemlerin devletlere değil gerçek kişilere isnat ediliyor olmasıdır.⁶⁶⁴ 2001 yılında Budapeşte’de imzaya açılan ve 2004’te yürürlüğe giren “Sanal Ortamda İşlenen Suçlar Sözleşmesi (*Convention on Cybercrime*)”,⁶⁶⁵ bu meseleleri konu edinen ilk ve en önemli uluslararası antlaşma olma özelliği taşımaktadır. Sözleşmenin 2003’te imzalanan “Bilgisayar Sistemleri Aracılığıyla İşlenen Irkçı ve Yabancı Düşmanı Nitelikteki Eylemlerin Suç Sayılmasına İlişkin”⁶⁶⁶ ve 2022’de imzalanan “Gelişmiş İş Birliği ve Elektronik Delillerin İfşasına İlişkin”⁶⁶⁷ iki ek protokolü de bulunmaktadır.

Avrupa Konseyi bünyesindeki Siber Uzay Suçları Uzman Komitesi’nin (*Committee of Experts on Crime in Cyberspace (Committee “PC-CY”)*) dört yıl süren çalışmaları sonucunda hazırlanan sözleşme, Konsey üyesi olsun ya da olmasın bütün devletler için imzaya açıldığı anda 26 Avrupa Konseyi üyesi devlet dışında ABD, Kanada, Japonya ve Güney Afrika’nın da katılımıyla 30 devletçe imzalanmıştır.⁶⁶⁸ Günümüzde Avrupa Konseyi’nin 46 üyesinin tamamıyla birlikte toplam 72 devlet

⁶⁶⁴ Abid A. Adonis, “International Law on Cyber Security in the Age of Digital Sovereignty”, E-International Relations, 14.03.2020, s.2 <https://www.e-ir.info/2020/03/14/international-law-on-cyber-security-in-the-age-of-digital-sovereignty/> (31.12.2024).

⁶⁶⁵ Resmi çeviri olarak “Sanal Ortamda İşlenen Suçlar Sözleşmesi” kullanılsa da (bkz. R. G., 09.08.2014, Sayı.29083), literatürde genellikle “Siber Suç (veya Suçlar) Sözleşmesi” çevirisi ya da “Bükreş Sözleşmesi” isimlendirilmesi tercih edilmektedir. Sözleşme, eldeki çalışmada buradan itibaren “Bükreş Sözleşmesi” olarak anılacaktır. Antlaşmanın İngilizce metni için bkz. UNTS, Vol.2296, No.40916, 2006, s.167 vd.; Eldeki çalışmada esas alınan Türkçe çeviri için bkz. TBMM, **Sanal Ortamda İşlenen Suçlar Sözleşmesinin Onaylanmasının Uygun Bulunduğuna Dair Kanun Tasarısı ve Dışişleri Komisyonu Raporu**, (1/676), Yasama Dönemi.24, Yasama Yılı.3, Sıra Sayısı.380, s.11 vd.

⁶⁶⁶ Additional Protocol to the Convention on Cybercrime, Concerning the Criminalisation of Acts of a Racist and Xenophobic Nature Committed through Computer Systems, UNTS, Vol.2466, No.40916, 2006, s.209 vd.

⁶⁶⁷ Second Additional Protocol to the Convention on Cybercrime on Enhanced Co-Operation and Disclosure of Electronic Evidence, Council of Europe Treaty Series (CETS), No.224.

⁶⁶⁸ Peter Csonka, “The Council of Europe’s Convention on Cyber-Crime and Other European Initiatives”, **International Review of Penal Law**, Vol.77, (2006), s.482.

sözleşmeyi onaylamış bulunmaktadır.⁶⁶⁹ Bu yönüyle Budapeşte Sözleşmesi, bölgesel bir uluslararası örgütten çıkmış olsa da küresel nitelikli bir uluslararası antlaşmaya dönüşme yolundadır.

Budapeşte Sözleşmesi'nde bilişim suçları için genel bir sınıflandırma yapılarak, taraf devletlerin, antlaşmada sınıflandırılan suçların *“etkili, orantılı ve caydırıcı yaptırımlarla cezalandırılabilir olmasını sağlamak için gerekli olabilecek yasama tedbirlerini ve diğer tedbirleri”* almaları öngörülmüştür.⁶⁷⁰ Sözleşmede öngörülen modelin etkisi taraf devletlerle sınırlı kalmamış, 150 ülkenin ulusal siber suç mevzuatının hazırlanmasına rehberlik etmiştir.⁶⁷¹

Sözleşmenin içeriğine yönelik hüküm esaslı tartışmalar bir yana literatürde çokça eleştiri aldığı da görülmektedir. Önok, bunların bir kısmını şu şekilde dört başlıkta derlemiştir: Sözleşmenin tadili için zorlu şartların getirilmiş olması nedeniyle teknolojik değişimin hızına yetişememe riski taşıması; çekincelere tanındığı geniş imkân nedeniyle etkinlik kaybı riskini taşıması;⁶⁷² gelişmekte olan devletlerin ve STK'ların sözleşme hazırlık sürecine yeterince dahil edilmemiş olması; sözleşmenin internet servis sağlayıcılara ağır yükler yüklemesi.⁶⁷³ Lâkin eleştiriler bunlarla sınırlı değildir. Sözleşmenin bağlayıcı bir uyumsuzluk çözüm mekanizması öngörmemesi ve daha çok devlet merkezci bir yaklaşım benimsenmesi de eleştirilmiştir.⁶⁷⁴ Siber terörizmin kapsam dışı kalması da ayrı bir eleştiri konusu olmuştur.⁶⁷⁵

Sözleşmeye halihazırda taraf olmayan ve Ukrayna Savaşı nedeniyle Avrupa Konseyi üyeliğinden de çıkarılmış olan Rusya'nın ve siber müttefiki Çin'in

⁶⁶⁹ COE, “Chart of Signatures and Ratifications of Treaty 185”, <https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treaty=185> (31.12.2024).

⁶⁷⁰ Budapeşte Sözleşmesi, m.13/1.

⁶⁷¹ COE/Cybercrime Program Office (C-PROC), **The Global State of Cybercrime Legislation 2013 – 2019: A cursory Overview**, Update as at 30 June 2019 Prepared by the Cybercrime Programme Office of the Council of Europe, Version 4 July 2019 / Public, Bucharest, Romania, s.6.

⁶⁷² Gerçekten de imzacı devletlerin sözleşmeye çok sayıda çekince ile taraf oldukları görülmektedir. Çekince ve açıklayıcı beyanlar için bkz. COE, “Reservations and Declarations for Treaty No.185 – Convention on Cybercrime (ETS No. 185)”, <https://www.coe.int/en/web/conventions/full-list?module=declarations-by-treaty&numSte=185&codeNature=0> (31.12.2024).

⁶⁷³ Murat Önok, “Avrupa Konseyi Siber Suç Sözleşmesi Işığında Siber Suçlarla Mücadelede Uluslararası İşbirliği”, **Marmara Üniversitesi Hukuk Araştırmaları Dergisi – Prof. Dr. Nur Centel’e Armağan**, Cilt.19, Sayı.2, (2013), ss.145-146.

⁶⁷⁴ Adonis, s.2.

⁶⁷⁵ Ali Karagülmez, **Bilişim Suçları ve Soruşturma – Kovuşturma Evreleri**, 5. Baskı, Ankara: Seçkin Yayıncılık, 2014, s.577.

muahalefetinden de bahsedilmesi gerekir. Rusya, Avrupa Konseyi üyesi olduğu dönemde dahi, devlet egemenliği ve müdahale etmeme ilkelerini ihlal eden, güncelliğini yitirmiş bir bölgesel antlaşma olarak değerlendirdiği⁶⁷⁶ Budapeşte Sözleşmesi'ne karşı çıkmış; BM bünyesinde küresel bir uluslararası antlaşmanın imzalanması adına, benzer yaklaşımdaki devletlerle birlikte çalışmalarını sürdürmüştür. ABD ve benzer yaklaşımdaki devletlerin ise Budapeşte Sözleşmesi'ne bakışı; siber güvenliğe yönelik en büyük tehdidin devlet dışı aktörler tarafından gerçekleştirilen kötüye kullanım eylemleri olduğu varsayımından hareketle, bu eylemlerin etkin şekilde suç sayılmasını öngören sözleşmenin en iyi korumayı sağlayacağı yönünde olmuştur.⁶⁷⁷ Ayrıca bu bloğun temel kaygısı, Rusya'nın söz konusu girişimlerinin devletlere insan hakları aleyhine geniş yetkiler tanımayı amaçladığı yönündedir.⁶⁷⁸ Çok sayıda STK'nın ortak imzasıyla BM Genel Kurulu'na bu kaygıları içeren bir açık mektup da iletilmiştir.⁶⁷⁹

Siber suçların uluslararası rejimine ilişkin devlet blokları arasında süregelen çatışma, bu konuda küresel bir antlaşma ve hukuk sistemi elde edilmesine engel olmaktadır. Rusya, BM'deki yoğun girişimleriyle, Genel Kurul nezdinde de olsa amaçladığı kararların alınmasını sağlayabilmektedir. Geline nokta atılmış en net somut adım, Genel Kurul kararıyla 2020'den itibaren suç amaçlı BİT kullanımına karşı kapsamlı bir uluslararası antlaşma hazırlamak üzere açık uçlu ve geçici bir hükümetler arası uzmanlar komitesi oluşturulmasıdır.⁶⁸⁰ Mafafih büyük devlet blokları arasındaki çatlak bu büyüklükte devam ettiği sürece; Budapeşte Sözleşmesi'nin küresel niteliğinin sınırlı kalacağını, yeni bir küresel antlaşma oluşturulması adına yürütülen çalışmaların akıbetinin de bu bakımdan Budapeşte Sözleşmesi'nden çok farklı olmayacağını öngörmek pek güç olmayacaktır.

⁶⁷⁶ Joyce Hakmeh ve Allison Peters, "A New UN Cybercrime Treaty? The Way Forward for Supporters of an Open, Free, and Secure Internet", Council on Foreign Relations, 13.01.2020, <https://www.cfr.org/blog/new-un-cybercrime-treaty-way-forward-supporters-open-free-and-secure-internet> (31.12.2024).

⁶⁷⁷ Korzak, s.11.

⁶⁷⁸ Hakmeh ve Peters.

⁶⁷⁹ Open Letter to UN General Assembly: Proposed International Convention on Cybercrime Poses a Threat to Human Rights Online, https://www.apc.org/sites/default/files/Open_letter_re_UNGA_cybercrime_resolution_0.pdf (31.12.2024).

⁶⁸⁰ UN/General Assembly, Countering the Use of Information and Communications Technologies for Criminal Purposes, A/RES/74/247, 20.01.2020.

b. Şangay İşbirliği Örgütü Uluslararası Bilgi Güvenliğinin
Sağlanmasında İş Birliği Anlaşması

Yekaterinburg şehri, 15-16 Haziran 2009’da iki önemli etkinliğe ev sahipliğe yapmıştır. BRICS (Brezilya, Rusya, Hindistan, Çin, Güney Afrika) henüz BRIC iken ilk zirvesini burada gerçekleştirmiş; aynı zamanda ŞİÖ de 9. Liderler Zirvesi’ni düzenleyip çeşitli kararlara varmıştır.⁶⁸¹ ŞİÖ zirvesi sonucunda “Terörizmle Mücadele Sözleşmesi”⁶⁸² imzalanmış, “Politik Diplomatik Önlemler Hakkında Yönetmelik” ve “Bölgesel Barış, Güvenlik ve İstikrarı Tehdit Eden Gelişmelere Tepki Mekanizması” yürürlüğe konmuştur.⁶⁸³ Bunların yanında bir önemli belge de “Uluslararası Bilgi Güvenliğinin Sağlanmasında İş Birliği Anlaşması (*Agreement on Cooperation in Ensuring International Information Security*)” olmuştur.⁶⁸⁴

Yekaterinbug Anlaşması, bilgi güvenliği alanındaki temel terimler listesini içeren Ek-1 ve bu alandaki tehditlerin tip, kaynak ve özellik listesini içeren Ek-2 ile birlikte ŞİÖ üyelerince imzalanmıştır. “Anlaşma (*agreement*)” tabiri kullanılmış olsa da uluslararası hukuka göre teknik olarak “uluslararası antlaşma” statüsünde olduğu çıkarımını son hükümlerinden yapmak mümkündür.⁶⁸⁵ Fakat Terörizmle Mücadele Konvansiyonu’nun aksine BM’de tescil edilmemiştir.⁶⁸⁶ Yine aynı hükümlere göre anlaşma ŞİÖ dışından katılıma açıktır. Anlaşmada, karşısında iş birliği yapılması gereken “uluslararası bilgi güvenliği alanındaki majör tehditler” olarak kabul edilen hususlar; “bilgi silahlarının geliştirilmesi ve kullanılması, bilgi savaşının hazırlanması ve yürütülmesi”, “bilgi terörizmi”, “siber suçlar”, “bilgi uzayındaki hakim durumun diğer devletlerin menfaatlerine ve güvenliğine zarar verecek şekilde kullanılması”; “diğer devletlerin

⁶⁸¹ Guy Faulconbridge, “Developing World Leaders Show New Power at Summits”, Reuters, 16.06.2009, <https://www.reuters.com/article/idUSTRE55F02F/> (31.12.2024); China Daily, “SCO Heads of State Council Meets in Yekaterinburg”, 20.07.2009, https://www.chinadaily.com.cn/china/peacemission2009/2009-07/20/content_8449520.htm (31.12.2024); China/Ministry of Foreign Affairs, “Yekaterinburg Declaration of the Heads of the Member States of the Shanghai Cooperation Organisation”, 17.06.2009, https://www.mfa.gov.cn/mfa_eng/wjdt_665385/2649_665393/200906/t20090626_679272.html (31.12.2024).

⁶⁸² Terörizme Karşı Şangay İşbirliği Örgütü Konvansiyonu (*Convention of the Shanghai Cooperation Organization Against Terrorism*), UNTS, Vol.2815, No.49374, 2012, s.69.

⁶⁸³ China/Ministry of Foreign Affairs, “Joint Communiqué of Meeting of the Council of the Heads of the Member States of the Shanghai Cooperation Organisation”, 17.06.2009, https://www.fmprc.gov.cn/eng/wjdt_665385/2649_665393/200907/t20090710_679273.html (31.12.2024).

⁶⁸⁴ Anlaşma (buradan itibaren Yekaterinburg Anlaşması) metni ve bahsi geçen diğer metinler için bkz. <https://eng.sectsc.org/documents/?year=2009> (31.12.2024).

⁶⁸⁵ Yekaterinburg Anlaşması, m.12.

⁶⁸⁶ Yekaterinburg Anlaşması’yla aynı başlığı taşıyan Rusya ve Türkmenistan arasındaki ikili anlaşmanın ise BM’de tescil edildiği görülmektedir; UNTS, Registration No.56871, 2021.

sosyo-politik ve sosyo-ekonomik sistemlerine, manevi, ahlaki ve kültürel çevrelerine zarar verecek bilgilerin yayılması”; “doğal ve/veya insan yapımı küresel ve ulusal bilgi altyapılarının güvenli ve istikrarlı işleyişine yönelik tehditler” şeklinde sayılmıştır.⁶⁸⁷ Bu tehdit algısının Budapeşte Sözleşmesi’ndeki yaklaşımdan çok farklı olduğu aşikardır. Siber uzayın tamamen “silahsızlaşması” yönündeki talebin ilk husustaki yansımasının yanı sıra son üç hususun, siber uzaydaki cari iktidar, yönetim ve kültür yapısına yönelik eleştirileri alt metninde taşıdığını söylemek de mümkündür.

ŞİÖ’nün Yekaterinburg ile başlattığı süreç, üyesi olan ülkelerce 2011’de BM’ye sunulan ve 2015’te güncellenen taslak düzenlemelerin ve nihayetinde bugün uluslararası toplulukça destek görmekte olan “sorumlu davranış kurallarının” ortaya çıkışına kadar uzanmıştır.

c. Bağımsız Devletler Topluluğu Bilgi Teknolojileri Alanındaki Suçlarla Mücadelede İş Birliği Anlaşması

BDT bünyesinde, Budapeşte Konvansiyonu’ndan yaklaşık altı ay önce “Bilgisayar Bilgisi Alanındaki Suçlarla Mücadelede İşbirliğine İlişkin Anlaşma (*Agreement on Cooperation in Combating Crimes in the Field of Computer Information*)” imzalanmıştır. “Minsk Anlaşması” olarak anılan bu anlaşma, 2002 yılında yürürlüğe girmiş; siber suçların etkili bir şekilde tespit, ortaya çıkarılması, önlenmesi ve soruşturulması gibi hususlarda BDT üyeleri arasındaki iş birliğinin güçlendirilmesine odaklanmıştır.⁶⁸⁸ Bu bakımdan Budapeşte Sözleşmesi ile gerek dönem gerek kapsam olarak büyük paralellikler taşıdığı söylenebilecektir.

Duşanbe’de 2018’de gerçekleştirilen BDT Liderler Zirvesi sonucunda imzalanan 12 belgeden biri “Bilgi Teknolojileri Alanındaki Suçlarla Mücadelede İş Birliği Anlaşması (*Agreement on Cooperation in the Fight Against Crimes in the Field of Information Technologies*)” olmuştur.⁶⁸⁹ 2020’de yürürlüğe giren ve “Duşanbe Anlaşması” olarak anılan bu belge, m.17/2 hükmü uyarınca, yürürlüğe giriş anından

⁶⁸⁷ Yekaterinburg Anlaşması, m.2.

⁶⁸⁸ UN/General Assembly, Overview of Existing Instruments, Recommendations and Other Documents on Countering the Use of Information and Communications Technologies for Criminal Purposes, *A/AC.291/CRP.10*, 20.04.2022, s.8.

⁶⁸⁹ Kabar, “Duşanbe’deki BDT Devlet Başkanları Zirvesinde 12 Anlaşma İmzalandı”, 28.09.2018, <https://tr.kabar.kg/news/du-anbedeki-bdt-devlet-ba-kanlar-zirvesinde-12-belge-imzalandi/> (31.12.2024).

itibaren Minsk Anlaşması'nın yerine geçmiştir. Duşanbe Anlaşmasını onaylamamış ülkeler için ise, antlaşmalar hukuku hükümlerine uygun şekilde, Minsk Anlaşması geçerliliğini korumaktadır. Minsk Anlaşması'yla aynı temeli paylaşan ve biraz daha kapsamlı yapıya sahip olan Duşanbe Anlaşması'na 2022 itibariyle beş devletin taraf olduğu aktarılmıştır.⁶⁹⁰

d. Arap Devletleri Ligi Bilgi Teknolojisi Suçlarıyla Mücadele Sözleşmesi

Arap Devletleri Ligi, 2010 yılında Kahire'de “Bilgi Teknolojisi Suçlarıyla Mücadele Hakkında Arap Sözleşmesi”ni (*Arab Convention on Combating Information Technology Offences*)” imzaya açmıştır.⁶⁹¹ 2014'te yürürlüğe giren Kahire Sözleşmesi, taraf devletlerin kendi menfaatlerini ve toplumlarını bilişim suçlarına karşı korumak adına iş birliğini güçlendirmenin ve ortak bir ceza politikası benimsemenin gerekliliği inancı üzerine inşa edilmiştir.⁶⁹² Sözleşmenin önemli bir özelliği; dikkate alınacak temel hususlar arasında, giriş bölümünde “*başta İslam Hukuku (Şeriat) emirleri olmak üzere yüksek dini ve ahlaki ilkeler*” ve “*her türlü suçu reddeden Arap Milleti'nin insanlık mirası*” vurgularının yapılmış olmasıdır. Bunun dışında muadilleriyle benzer özellikler gösteren sözleşme, sadece Arap devletlerini işaret eden söylem ve yapısıyla küresel bir sözleşmeye dönüşme iddiasında değildir. Bu anlamda disipline esaslı bir yenilik katmamakla birlikte tipik bir bölgesel iş birliği sözleşmesi örneği olarak görülebilecektir.

e. Afrika Birliği Siber Güvenlik ve Kişisel Verilerin Korunması Sözleşmesi

Afrika'nın kalabalık nüfusunun dünya nüfusuna oranı gittikçe artmakta ve henüz bu nüfusun yalnızca %37'si internet kullanmaktadır.⁶⁹³ Afrika'daki büyük siber potansiyelin hayat bulabilmesi için siber uzayda istikrar sağlama çalışmalarının kayda değer bir sonucu, AfB ve BM Afrika Ekonomik Kurulu (UNECA) tarafından 2012'de

⁶⁹⁰ A/AC.291/CRP.10, ss.8-9.

⁶⁹¹ Buradan itibaren “Kahire Sözleşmesi” olarak anılacak sözleşmenin İngilizce metni için bkz. <https://www.asianlaws.org/gclid/cyberlawdb/GCC/Arab%20Convention%20on%20Combating%20Information%20Technology%20Offences.pdf> (31.12.2024).

⁶⁹² Kahire Sözleşmesi, Giriş.

⁶⁹³ ITU, “Facts and Figures 2023”, <https://www.itu.int/itu-d/reports/statistics/2023/10/10/ff23-internet-use/> (31.12.2024).

tamamlanan “Afrika'da Siber Güvenlik için Güvenilir Bir Yasal Çerçeve Oluşturulmasına İlişkin Taslak Sözleşme (*Draft Convention for the Establishment of a Credible Legal Framework for Cybersecurity in Africa*)” olmuştur. Ne var ki taslak sözleşme Ocak 2014'te AfB'de kabul için son aşamaya kadar geldiyse de gerek teknik gecikmeler gerek sivil toplumun ve akademik çevrelerin muhalefeti nedeniyle revize edilerek⁶⁹⁴ 6 ay sonra Malabo şehrinde “Siber Güvenlik ve Kişisel Verilerin Korunması Hakkında Afrika Birliği Sözleşmesi (*African Union Convention on Cyber Security and Personal Data Protection*)” adıyla kabul edilmiştir. Malabo Sözleşmesi'ni AfB'nin 55 üye devletinin henüz yalnızca 19'u imzalamış ve imzalayanlardan yalnızca 7'si onaylamış; 8 devlet de sonradan katılma yoluyla antlaşmaya dahil olmuştur.⁶⁹⁵ Böylece yürürlük için öngörülen 15 devlet tarafından onaylanma şartı ancak husule gelmiştir.⁶⁹⁶ Malabo Sözleşmesi, tıpkı Kahire Sözleşmesi gibi tipik bir bölgesel siber güvenlik antlaşması görüntüsü çizse de; taraf devletlere, siber suçlara ilişkin maddi ve usulî ceza hukuku hükümleri ihdas etme, siber güvenlik yönetişimine ve siber suçların kontrolüne yönelik hukuki ve kurumsal çerçevelerin yanı sıra ulusal siber güvenlik politikaları oluşturma gibi husularda geniş yükümlükler getirmektedir. Malabo Sözleşmesi'nin, bu yönüyle Budapeşte Sözleşmesi'nin ötesine geçtiği yorumu da yapılmıştır.⁶⁹⁷ Fakat ne kadar kapsamlı ve etkin hükümlere sahip olsa da taraf devlet sayısı itibarıyla uluslararası hukuktaki etkisi çok kısıtlı bir seviyede kalmıştır.

3. Avrupa Birliği Düzenlemeleri

AB bünyesinde, siber uzay bağlamında insan haklarından teknik standartlara birçok konuya ilişkin iç düzenlemeler bulunmaktadır. Lakin bu düzenlemeler siber uzayın gelişim sürecine göre nispeten geç bir dönemde başlamıştır. Bunun gerekçesi olarak ise klasik dönemden kalan, siber uzayın düzenlenemeyeceği yahut düzenlenmemesi

⁶⁹⁴ Taslak sözleşmeye getirilen eleştiriler, üye devletlerdeki ilgili paydaşlara kapsamlı şekilde danışılmadan hazırlandığına ve etkili bir yasal uyumlaştırma ile uluslararası iş birliğini kolaylaştıracak kritik siber güvenlik yönetim mekanizmalarından yoksun olduğuna yönelik görüşler üzerinde temellenmiştir; Uchenna Jerome Orji, “The African Union Convention on Cybersecurity: A Regional Response Towards Cyber Stability?”, **Masaryk University Journal of Law and Technology**, Vol.12, No.2, (2018), s.98.

⁶⁹⁵ Buradan itibaren “Malabo Sözleşmesi” olarak anılacak sözleşmenin metinleri ve güncel statüsü için bkz. <https://au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection> (31.12.2024).

⁶⁹⁶ Malabo Sözleşmesi, m.36.

⁶⁹⁷ Orji, s.99.

gerektiği yönündeki anlayışın etkileri gösterilmiştir.⁶⁹⁸ Ayrıca dönemin özelliği olarak, düzenleme çabalarının, internetin büyük potansiyelini gereğinden fazla kısıtlayacağı kaygısı da genel sebepler arasında görülebilir.⁶⁹⁹ Yine de zaman geçtikçe AB, siber uzayın düzenlenmesi rüzgarına kayıtsız kalmamıştır.

Esasen AB uzun yıllar siber uzay konusunda iç pazarın düzenlenmesi, tüketicinin ve kişisel verilerin korunması veya siber suçlar gibi konulara eğilmiştir. AB'nin genel yapısı gereği güvenlik meselelerinden ziyade sosyoekonomik meseleleri öncelemesi, siber uzay başlığında da gözlemlenmiştir. Fakat bu yaklaşımın sıkı sıkıya sürdürülmesi imkansızlaşmaktadır. Zira siber uzayın yapısı ve doğurduğu tehditler artık neredeyse tamamen sınırlardan bağımsız hale gelmekte ve uluslararası iş birliği olmadan etkin bir güvenlik sağlamak söz konusu olamamaktadır. Dolayısıyla AB'nin siber güvenlik enstrümanlarındaki çok parçalı yapısından uzaklaşıp kapsamlı düzenlemeler getirilmesi ihtiyacına işaret edilmiştir.⁷⁰⁰

İnternet üzerinden sürdürülen ticaretin düzenlenmesi adına 2000 yılında yürürlüğe giren Elektronik Ticaret Direktifi (*Electronic Commerce Directive*),⁷⁰¹ bu alanda hizmet veren aktörlerin yükümlülük ve sorumluluklarını, hizmet süreçlerine dair esasları konu edinmesi açısından AB bünyesindeki ilk kapsamlı düzenlemedir. İnsan haklarının ve teknik standartların harmanlandığı en bilinen AB düzenlemelerinden biri ise GDPR olmuştur.⁷⁰² 2016'da yayımlanan ve 2018'de yürürlüğe giren GDPR; hem gerçek kişilerin kişisel verilerinin korunması hakkını hem de bu verilerin AB içerisinde serbest dolaşımını güvence altına almayı amaçlamaktadır.⁷⁰³ Belirtilmelidir ki GDPR sadece dijital verilerle ilişkili değildir. Fakat dijital veriler, siber uzayın GDPR ile düzenlenen kısmını teşkil etmektedir. GDPR, kişisel veri toplayanlara bu verilerin

⁶⁹⁸ Ramses A. Wessel, "European Law and Cyberspace", Nicholas Tsagourias ve Russell Buchan (Ed.), **Research Handbook on International Law and Cyberspace** içinde (491-508), Cheltenham: Edward Elgar Publishing, 2021, s.507.

⁶⁹⁹ Joachim Zekoll, "Jurisdiction in Cyberspace", Günther Handl, Joachim Zekoll ve Peer Zumbansen (ed.), **Beyond Territoriality: Transnational Legal Authority in an Age of Globalization** içinde (341-369), Leiden: Martinus Nijhoff Publishers, 2012, s.343.

⁷⁰⁰ Wessel, s.508.

⁷⁰¹ Direktif metni için bkz. <http://data.europa.eu/eli/dir/2000/31/oj> (31.12.2024).

⁷⁰² Tüzük metni için bkz. <http://data.europa.eu/eli/reg/2016/679/oj> (31.12.2024); T.C. Dışişleri Bakanlığı'na bağlı AB Başkanlığı tarafından hazırlanan gayriresmî Türkçe çeviri için bkz. <https://www.ab.gov.tr/siteimages/resimler/Nihai-ABB-HCDB-GDPR.pdf> (31.12.2024).

⁷⁰³ GDPR, m.1.

toplanma amacını, saklanma süresini, hangi amaçlarla işleneceğini, hangi üçüncü taraflarla paylaşılacağını bildirme ve sızma/çalınma gibi durumlardan haberdar etme gibi yükümlülükler yüklemektedir. Ayrıca kişisel veriye ve veri işlemeye dair temel kavramlar tanımlanarak; veri sahiplerine kendi verilerine erişme, bunları topluca talep etme, düzelttirme ve belli şartlarda tamamen sildirme gibi haklar tanınmıştır. GDPR bir yandan Türkiye’de yürürlüğe giren KVKK örneğindeki gibi birçok ülkede kanun ihdasına model olmuş; bir yandan da BİT sektöründe yaygın bir etki oluşturarak siber uzay mimarisinde önemli değişikliklerin gerçekleşmesine yol açmıştır.

GDPR sonrası, çok kısa bir zaman dilimi içerisinde, önce 2021’de terörizmle mücadeleyle yönelik olarak Terörist İçeriğin Çevrimiçi Yayılmasının Önlenmesine ilişkin Tüzük (*Regulation on Addressing the Dissemination of Terrorist Content Online* (TERREG))⁷⁰⁴ yürürlüğe girmiştir. Sonraki yıl dijital ortamda rekabet hukukunun teşekkülü ve giderek güçlenen teknoloji şirketlerinin çevrimiçi ticari faaliyetlerinin düzenlenmesi adına Dijital Piyasalar Yasası (*Digital Markets Act* (DMA))⁷⁰⁵ ve sadece bir ay sonrasında Dijital Hizmetler Yasası (*Digital Services Act* (DSA))⁷⁰⁶ yine ismiyle müsemma olduğu üzere dijital ortamdaki hizmetlerin adil, şeffaf ve hesap verebilir şekilde gerçekleşmesini sağlama ve hem hukuka aykırı içerikle mücadele edilmesi hem ifade özgürlüğü dahil temel hakların teminat altına alınması amaçlarıyla yürürlüğe girmiştir.⁷⁰⁷

Siber güvenlik alanına gelindiğinde, AB’nin geliştirdiği en güncel ve kapsamlı düzenleme; 12 Mart 2024’te Avrupa Parlamentosu tarafından, 10 Ekim 2024’te de Bakanlar Konseyi tarafından onaylanan Siber Dayanıklılık Yasası’dır (*Cyber Resilience Act* (CRA)).⁷⁰⁸ CRA ile oyuncaklardan elektrikli ev aletlerine ve bilgisayarlara kadar bütün “dijital ögeler içeren ürünler (*products with digital element* (PDE))” için yeni teknik standartlar getirilmekte ve CE damgalı ürünlerin belirlenen asgari siber güvenlik

⁷⁰⁴ Tüzük metni için bkz. <http://data.europa.eu/eli/reg/2021/784/oj> (31.12.2024).

⁷⁰⁵ Yasa metni için bkz. <http://data.europa.eu/eli/reg/2022/1925/oj> (31.12.2024).

⁷⁰⁶ Yasa metni için bkz. <http://data.europa.eu/eli/reg/2022/2065/oj> (31.12.2024).

⁷⁰⁷ Alper Işık, *İnternet Aktörleri ve Egemenliğin Değişen Boyutları: Digital Services Act ve Türk Mevzuatı Özelinde Bir İnceleme*, İstanbul: On İki Levha Yayıncılık, 2023, s.119.

⁷⁰⁸ CRA ve yasama süreci hakkında bilgi için bkz. <https://www.european-cyber-resilience-act.com> (31.12.2024); Bakanlar Konseyi kararı ve CRA metni için bkz. <https://data.consilium.europa.eu/doc/document/PE-100-2023-REV-1/en/pdf> (31.12.2024).

şartlarını sağlamaları beklenmektedir. Söz konusu siber güvenlik standartlarını belirlemek ve mevcut durumla kıyaslamalı bir analiz yapmak amacıyla AB Siber Güvenlik Ajansı (*European Union Agency for Cybersecurity*) adıyla bilinen Avrupa Ağ ve Bilgi Güvenliği Ajansı (*European Network and Information Security Agency* (ENISA)) ve Avrupa Komisyonu’nun ortak çalışmasıyla 4 Nisan 2024’te bir haritalama çalışması yayımlanmıştır.⁷⁰⁹ Üreticilerin, ürünlerinde düzeltilememiş ve aktif olarak istismar edilen bir siber güvenlik açığı ortaya çıkması halinde 24 saat içinde ENISA’ya ve devletlerin siber olaylara müdahale birimlerine bilgilendirmede bulunmaları da CRA ile getirilen şartlardandır. Uluslararası siyaset açısından ise; metinde geçen, kilit süjelerin “yüksek riskli tedarikçilerden” temin edilen PDE’leri kullanmasının stratejik riskler taşıdığı yönündeki ifadelerin, başta Çin ve diğer otoriter ülkelerden gelen teknolojilerin kullanımını kısıtlayan yeni AB politikalarına kapı açabileceği yorumu yapılmıştır.⁷¹⁰

AB’nin son dönemde siber güvenlik alanındaki girişimleri CRA ile sınırlı kalmamıştır. Siber Güvenlik Yasası’na uygun olarak BİT ürünlerini sertifikalandırmak için 13 Ocak 2024’te Ortak Kriterler Hakkında Avrupa Siber Güvenlik Sertifikasyon Tasarısı (*European Cybersecurity Certification Scheme on Common Criteria* (EUCC))” kabul edilmiştir.⁷¹¹ Ayrıca AB kurum, kuruluş, ofis ve ajanslarında yüksek düzeyde ortak siber güvenliğe tedbirlerini belirleyen yeni bir tüzük, 7 Ocak 2024’te yürürlüğe girmiştir.⁷¹²

Son yılların en tartışmalı konularından olan yapay zekâyı da düzenleme rüzgarına dahil eden AB’de, 2021’de teklif edilen Yapay Zekâ Yasası (*Artificial Intelligence Act* (AIA)) 21 Mayıs 2024’te kabul edilerek 1 Ağustos 2024 itibariyle yürürlüğe girmiştir.⁷¹³

⁷⁰⁹ European Commission ve ENISA, “Cyber Resilience Act Requirements Standards Mapping, Joint Research Centre & ENISA Joint Analysis”, 2024, <https://www.enisa.europa.eu/publications/cyber-resilience-act-requirements-standards-mapping> (31.12.2024); ENISA, kamu ve özel sektör arasındaki iş birliğinin teşviki için uzmanlık temin etmek ve Avrupa Komisyonu ile AB üyesi devletlere daimî destek sağlamak amacıyla, Avrupa Parlamentosu ve AB Bakanlar Konseyi’nce yayımlanan (EC)460/2004 sayılı Tüzük ile kurulmuştur. Kurucu tüzük metni için bkz. <http://data.europa.eu/eli/reg/2004/460/oj> (31.12.2024); ENISA’nın cari olan güncel tüzüğü ise “Siber Güvenlik Yasası” olarak da anılan (EU)2019/881 sayılı Tüzük’tür. Tüzük metni için bkz. <http://data.europa.eu/eli/reg/2019/881/oj> (31.12.2024).

⁷¹⁰ Antoaneta Roussi, “EU Strikes Deal on Cyber Law for Internet-Connected Products”, Politico, 01.12.2023, <https://www.politico.eu/article/eu-strikes-deal-cyber-resilience-act-cra-law-internet-connected-products/> (31.12.2024).

⁷¹¹ Süreç hakkında bilgi için bkz. <https://certification.enisa.europa.eu> (31.12.2024).

⁷¹² Tüzük metni için bkz. <http://data.europa.eu/eli/reg/2023/2841/oj> (31.12.2024).

⁷¹³ Yasa metni için bkz. <http://data.europa.eu/eli/reg/2024/1689/oj> (31.12.2024); Yasa hakkındaki bilgiler, güncel gelişmeler ve analizler için bkz. <https://artificialintelligenceact.eu> (31.12.2024).

Askeri, milli güvenliğe ilişkin, bilimsel veya amatör kullanıma yönelik yapay zeka sistemlerini kapsam dışında bırakan yasa; geriye kalan bütün sektörlerdeki her tür yapay zeka sistemini, taşıdığı risklere göre tasnif ederek birtakım şartlara tabi tutmuştur. Ayrıca Avrupa Yapay Zekâ Ofisi ve Avrupa Yapay Zekâ Kurulu gibi yeni yönetim organlarının kurulmasına karar verilmiştir. Dünyadaki ilk kapsamlı yapay zekâ düzenlemesi olarak gösterilen⁷¹⁴ AIA henüz yürürlüğe girdiği için, uygulamaya nasıl yansıtılacağını ve yapay zekâ alanında ne tür etkiler doğuracağını zaman gösterecektir.

AB sosyal, ekonomik ve teknik standartlar üzerinde uzunca bir süredir etkili düzenlemeler yapmaktadır. Siber güvenlik alanındaki girişimleri ise yukarıda bahsedildiği üzere nispeten çok yakın bir dönemde başlamış ve halen devam etmektedir. Siber uzayın ve AB hukukunun dinamikleri gereği bu alanda yapılan akademik çalışmalar çok kısa sürede güncelliğini yitirebilmektedir. Dolayısıyla eldeki çalışmada yukarıdaki gelişmelere yer verilerek mevcut halin aktarımıyla iktifa edilmiş; siber uzayın uluslararası düzenlenmesinde etkin rol oynayan AB süreçlerinin gidişatına dair genel tablonun tasviri amaçlanmıştır.

4. Tallin El Kitabı

Özgül ağırlığı en yüksek askeri ittifak olan NATO'nun siber güvenlik alanındaki faal politikası şaşırtıcı değildir. 2002 yılında ilk kez siber saldırılara karşı savunma kabiliyetlerinin güçlendirilmesini gündemine alan NATO,⁷¹⁵ Rusya-Çin bloğundaki devletlerin görüşünün aksine siber uzayı kara, hava ve deniz gibi savunulması gereken bir harekât alanı olarak kabul etmiştir.⁷¹⁶ Teşkilat yapısında da en yüksek karar alma organı olan Kuzey Atlantik Konseyi (*North Atlantic Council* (NAC)) altında Siber Savunma Komitesi (*Cyber Defence Committee* (CDC)) faaliyet göstermektedir. Uzmanlar ve siber diplomatlardan oluşan CDC, NATO'nun iç siber savunmasının genel yönetimini yürütmekle birlikte bu alanda NAC'nin birincil danışma organıdır ve müttefik

⁷¹⁴ Ata Ufuk Şeker, "Avrupa Parlamentosu 'Yapay Zeka Yasası'nı onayladı", Anadolu Ajansı, 13.03.2024, <https://www.aa.com.tr/tr/dunya/avrupa-parlamentosu-yapay-zeka-yasasini-onayladi/3163480> (31.12.2024).

⁷¹⁵ NATO, "Prague Summit Declaration", 21.11.2002, https://www.nato.int/cps/en/natohq/official_texts_19552.htm (31.12.2024).

⁷¹⁶ NATO, "Warsaw Summit Communiqué", 09.07.2016, https://www.nato.int/cps/en/natohq/official_texts_133169.htm (31.12.2024).

devletlere de danışmanlık sağlamaktadır.⁷¹⁷ Müşterek Siber Savunma Mükemmeliyet Merkezi (*Cooperative Cyber Defence Centre of Excellence* (CCDCOE)) ise CDC'den farklı olarak NATO dışında kurulmuş ve kısa süre içinde NATO tarafından tam akredite edilerek askeri uluslararası örgüt statüsü tanınmıştır.⁷¹⁸

CCDCOE'nin uluslararası hukuk adına en önemli çalışması; kendi uzmanlar grubunun, uluslararası hukukçuların ve çok sayıda devletten hukuk müşavirlerinin katkılarıyla 19 yazar tarafından oluşturulan Tallin⁷¹⁹ El Kitabı'dır (*Tallinn Manual*).⁷²⁰ İlk baskısı 2013 yılında yayımlanan eserin daha sonra kapsamı genişletilerek 2017 yılında "Tallin El Kitabı 2.0" olarak anılan ikinci baskısı yayımlanmıştır. 2021 yılında da yeni bir versiyon için "Tallin El Kitabı 3.0 Projesi" başlatılmıştır.⁷²¹

Tallin El Kitabı'nın, uluslararası hukuk nezdindeki konumunun doğru anlaşılması önem arz etmektedir. İlgili metin şüphe yok ki uluslararası hukukun siber uzayda uygulanması adına en kapsamlı ve uluslararası katkılarla devlet pratikleri adına en muteber çalışmadır. Bununla birlikte bir "en iyi uygulamalar kılavuzu" değildir yahut "ilerici bir hukuk geliştirmesi" sunmamaktadır; tasarım amacı, "uygulanmakta olan hukukun nesnel bir yeniden ifadesi" olmaktır.⁷²² Ayrıca NATO dahil herhangi bir yapının hukuki pozisyonlarını veya doktrinini yansıtmaya iddiasında değildir.⁷²³ Eser bu haliyle yayımlandığı dönemde siber uzayda cari uluslararası örf ve âdet hukukun tespiti yolunda önemli bir başvuru kaynağı olarak görülmelidir.

Uluslararası hukukun cari hükümlerinin siber faaliyetler üzerindeki izdüşümü şeklinde tasarlanmış olan Tallin El Kitabı'nın eldeki çalışma adına en öne çıkan yönü; uluslararası hukukta devlet egemenliğine, yetkisine ve sorumluluk rejimine hâkim

⁷¹⁷ Steven Hill, "NATO and the International Law of Cyber Defence", Nicholas Tsagourias ve Russell Buchan (ed.), **Research Handbook on International Law and Cyberspace** içinde (509-524), Cheltenham: Edward Elgar Publishing, 2021, s.511; CCDCOE, "North Atlantic Treaty Organisation", <https://ccdcoe.org/organisations/nato/> (31.12.2024).

⁷¹⁸ CCDCOE, "About Us", <https://ccdcoe.org/about-us/> (31.12.2024).

⁷¹⁹ Türkçe literatürde eser ismi genellikle "Tallinn El Kitabı" şeklinde yer alsa da ilgili şehrin ismi dilimizde Tallin'dir; bkz. T.C. Tallin Büyükelçiliği resmî web sitesi, <https://tallin-be.mfa.gov.tr/Mission> (31.12.2024). Tallinn El Kitabı şeklinde bir kullanım, sözgelimi "London Manual" isimli bir eserin "Londra El Kitabı" yerine "London El Kitabı" şeklinde çevrilmesine benzer olacaktır.

⁷²⁰ Tallin El Kitabı, s.xii vd.

⁷²¹ CCDCOE, "The Tallinn Manual", <https://ccdcoe.org/research/tallinn-manual/> (31.12.2024).

⁷²² Tallin El Kitabı, s.3.

⁷²³ Ibid., s.5.

ilkelerin siber uzayda da geçerli olacağını belirtmesidir.⁷²⁴ Ayrıca *jus ad bellum* ve *jus in bello* açısından NATO yaklaşımına uygun hükümler barındırmaktadır. Ölçek ve etki itibarıyla siber olmayan ve kuvvet kullanımı teşkil eden fiillere kıyaslanabilir haldeki siber saldırıların, klasik anlamda silahlı kuvvet kullanımı olarak kabul edileceği belirtilmiştir.⁷²⁵ Bu tür bir saldırıya maruz kalan devletin meşru müdafaa hakkı tanınmış,⁷²⁶ karşılıklı siber eylemlerle ortaya çıkan bir silahlı çatışma durumunda da Cenevre Sözleşmeleri ile paralel hükümlerle insancıl hukuk normlarının geçerli olacağı belirtilmiştir.⁷²⁷ Silahlı saldırı seviyesine ulaşmayan siber müdahaleler, Çalışma kapsamına ikinci baskıda alınmış ve bunlara karşı genel sorumluluk rejimine uygun hükümler metinde yer almıştır. Yine de fiziksel hasar ya da yaralanmaya yol açmayan ya da siber altyapının işlevselliğini yitirmesine neden olmayan operasyonların neden ve ne zaman hedef devletin ülkesel egemenliğini ihlal edeceği sorunu uluslararası hukukta bir “gri bölge” olarak görülmeye devam etmektedir.⁷²⁸

F. Uluslararası Hukukta Siber Uzaya Hâkim İlkeler

Küresel ve kapsamlı bir uluslararası antlaşmanın yokluğunda, siber uzay için genel geçer uluslararası hukuk kural ve ilkelerinin varlığını sorgulamak, şayet mümkünse de bunları tespit etmek, ancak uluslararası topluluğun hukuki ve pratik çıktılarının iyi analiz edilmesiyle mümkün olacaktır. Mevcut bölgesel antlaşmalardan ve devletlerin ulusal düzenlemeleri ile pratiklerinden yola çıkılarak siber uzay için genel bir uluslararası teamül hukuku ve temel ilkeler tespiti yapılabilir. Devletlerin modern dönemde başlayan düzenleme dalgasıyla paralel olarak 21. yy başlarında, siber uzayda geçerli hukuk ilkelerinin tespiti adına yoğun akademik faaliyet yürütülmüştür. Antlaşmaların oluşturulmasında ve akdedilmesinde bu çalışmaların etkisi yadsınamaz. Uluslararası örf

⁷²⁴ Ibid., ss.9-167, Bölüm I: Genel Uluslararası Hukuk ve Siber Uzay.

⁷²⁵ Ibid., s.330, Kural 69.

⁷²⁶ Ibid., s.339, Kural 71.

⁷²⁷ Ibid., ss.373-400, Bölüm IV: Siber Silahlı Çatışmalar Hukuku; Söz konusu yaklaşımın uygulama esaslarına ilişkin en güncel çalışmalardan biri, UNOEWG-2 sürecinde Brezilya, Kanada, Şili, Kolombiya, Çekya, Estonya, Almanya, Hollanda, Meksika, Güney Kore, Senegal ve İsviçre tarafından ortak beyan ile sunulmuştur; UN/Open-ended Working Group on Information and Communication Technologies, Working Paper on application of international humanitarian law to the use of ICTs in situations of armed conflict submitted by Group of States, Working Papers, 01.03.2024, https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_2021/OEWG_Working_Paper_IHL_ICT_Operations.pdf (31.12.2024).

⁷²⁸ Luke Chircop, “Territorial Sovereignty in Cyberspace after Tallinn Manual 2.0”, *Melbourne Journal of International Law*, Vol.20, Iss.2, (2019), s.354.

ve âdet hukukunun tespiti ise bu hukuk kaynağının doğası gereği sürekli devam eden bir çabadır. Tallin El Kitabı örneğinde görüldüğü gibi bu çalışmalar daima güncellenmek mecburiyetindedir.

Hukuk genel ilkeleri, yeni ortaya çıkmış bir olgu hakkında hukuki kanaat geliştirirken, kıyasta kullanılabilir mevcut hukuk normlarının yanında önemli bir referanstır. Hukukun belirleyicisi olan devletler, milli menfaatlerine uygun düşecek şekilde mevcut normlarından ve genel ilkelerden hareketle pozisyon belirlemekte; böylece şayet uluslararası tutarlılık sağlanabilirse de bir örf ve âdet hukukunun oluşumuna doğru yol alınmaktadır. Söz konusu sürecin analiziyle kuralları tespit edip hüküm çıkarmak, objektif ve belirli bir usulî çerçeve bulunmadığı için uluslararası hukuk yazarları adına çetin bir mücadeledir. Nitekim *Janis* de uluslararası örf ve âdet hukuku tespitinin “*bilimsel bir metottan ziyade bir sanat*” olduğunu ileri sürer.⁷²⁹

Hukukun her alanına temas eden siber uzay için bir örf ve âdet hukuku manzumesine bu çalışmada yer vermek tabii ki mümkün ve anlamlı değildir. Ayrıca aşağıda Üçüncü Bölüm boyunca ilgili başlıklarda bu normların bazılarını yeri geldikçe değinilecektir. Bu başlıkta siber uzayın uluslararası düzenlenmesine dair temel meselelerde devletlerin mutabakat durumlarına değinilecek; literatürdeki bazı ilke seti önerilerine yer verilip, siber uzayda devlet egemenliğinin görünimleri incelenirken başvuru noktası olarak kullanılabilecek bir genel çerçeve çizilmeye çalışılacaktır.

Siber uzayda geçerli birçok kural esasen devlet dışı aktörlerin pratikleriyle gelenek haline gelmiş kurallardır. Zira Web’in ortaya çıkışının ardından internetin özelleşmesiyle, devletlerin henüz bu alanı düzenlemelere konu etmediği bir dönemde devlet dışı aktörler kendi önlemlerini almış, standartlarını belirlemiştir.⁷³⁰ Özellikle siber uzayın ticari kısmında, çevrimiçi hizmet sağlayıcıların uygulama ve standartlarında bu süreç daha belirgindir. Devlet düzenlemelerinin varlığı bu kuralların işlerliğini açıkça

⁷²⁹ Mark W. Janis, *An Introduction to International Law*, 4th Edition, New York: Aspen Publishers, 2003, s.44.

⁷³⁰ Siber uzayda işlem gizliliğinin sağlanması, günümüzdeki Taşıma Katmanı Güvenliği (*Transport Layer Security* (TLS)) protokolünün öncülü olan Güvenli Soket Katmanı (*Secure Socket Layer* (SSL)) protokol standardının benimsenmesi, güçlü şifreleme kullanımı zaruretinin standart haline gelmesi gibi bir çok gelişme, siber uzayda iş yapmak isteyen girişimlerin ve IETF gibi toplulukların inisiyatifiyle ortaya çıkmıştır; Paul Przemysław Polański, “Cyberspace: A New Branch of International Customary Law?”, *Computer Law & Security Review*, Vol.33, Iss.3, (2017), s.378.

arttırsa da -kadim ticaret hukuku *lex mercatoria* analojisine uygun şekilde- siber uzayın çoğu geleneksel kuralı, gücünü serbest piyasadan ve mimarının etkin belirleyiciliğinden almaktadır. Uluslararası hukuk disiplini dahilinde tartışılan esaslı başlıklar ise; siber uzay yönetiřimi, devletin egemenlik kaynaklı hak ve yetkileri, siber güvenlik ve kuvvet kullanma, siber suçlar, ifade ve haber alma özgürlükleri, özel hayatın gizliliğı, küresel serbest piyasa ve internet serbestliğı şeklinde sınırlayıcı olmaksızın sayılabilir.

Literatürde birtakım ilke setleri önerilmiştir. Bunlar genelde yazarlarca uluslararası topluluğun üzerinde mutabakat sağladığı varsayılan ilkeler olarak görülse de hemen hepsinin içinde tartışmalı detaylar mevcuttur.

Uerpmann-Wittzack, “Uluslararası İnternet Hukuku” ismiyle hukukun genç bir alanı olduğunu ifade ettiğı disipline geliřmekte olan beř ilkeyi incelemiřtir. Bunları; “(1) *internet özgürlüğü ilkesi*, (2) *mahremiyet ilkesi*, (3) *siber uzaya uyarlanarak tadil edilmiř bir ülkesel yargı yetkisi ilkesi*, (4) *devletlerarası iř birliğı ilkesi* ve (5) *çok paydařlı iř birliğı ilkesi*” şeklinde saymıştır.⁷³¹

Uerpmann-Wittzack’tan kısa bir zaman sonrasında, ITU Genel Sekreteri Toure’nin “siber barıř için beř ilke” olarak tespit ettikleri ise ařağıdaki gibidir:⁷³²

- “1. *Her hükümet, halkına iletiřime eriřim imkânı sağlamayı taahhüt etmelidir.*
2. *Her hükümet, halkını siber uzayda korumayı taahhüt edecektir.*
3. *Her ülke teröristleri/suçluları kendi topraklarında barındırmamayı taahhüt edecektir.*
4. *Her ülke, diğerk ülkelere yönelik siber saldırıyı ilk bařlatan taraf olmamayı taahhüt etmelidir.*
5. *Her ülke, siber uzayda barıřın sağlanması için uluslararası bir iř birliğı çerçevesinde birbiriyle ortak hareket etmeyi taahhüt etmelidir.”*

Dönemin Birleşik Krallık Dışışleri Bakanı *Hague*, 2011’de Münih Güvenlik Konferansı’nda, siber uzayın kullanımına ilişkin gelecekteki uluslararası normların

⁷³¹ Robert Uerpmann-Wittzack, “Principles of International Internet Law”, **German Law Journal**, Vo.11, Iss.11, (2010), s.1247.

⁷³² Hamadoun I. Touré, “The International Response to Cyberwar”, ITU, **The Quest for Cyber Peace** içinde (86-103), ITU, 2011, s.103.

temelini oluřturması temennisiyle Britanya'nın resmi g r ř  olarak yedi ilke ilan etmiřtir.⁷³³

“1. H k metlerin siber uzayda orantılı ve ulusal ile uluslararası hukuka uygun hareket etmesi gereklilięi;

2. Herkesin -beceri, teknoloji, g ven ve f rsat a ısından- siber uzaya eriřim kabiliyetine sahip olması gereklilięi;

3. Siber uzay kullanıcılarının dil, k lt r ve fikir  eřitlilięine hořg r  ve saygı g stermesi gereklilięi;

4. Siber uzayın yenilięe ve fikirlerin, bilginin ve ifadenin serbest akıřına a ık kalmasının saęlanması;

5. Bireysel mahremiyet haklarına saygı g sterilmesi ve fikri m lkiyete uygun koruma saęlanması gereklilięi;

6.  evrimi i faaliyet g steren su lulardan kaynaklanan tehditle m cadele etmek i in hepimizin ortak  alıřması gereklilięi;

7. Aęa, hizmetlere ve i erięe yapılan yatırımın adil bir řekilde geri d n ř n  saęlayan rekabet i bir ortamın teřvik edilmesi.”

 lke  onerilerine bir  rnek de Ryan ve Dięerleri'nin iki kategoriye ayırmak suretiyle geliřtirdikleri yaklařımdır. Siber uzaya dair uluslararası normlarla ulusal hukuk normları arasındaki iliřkinin karmařıklıęından dem vuran yazarlar; “uluslararası topluluk i indeki ulus-devletlerin sorumluluklarına ve onlardan beklentilere uygulanan normlar” ile “bir ulus i indeki siber uzay kullanıcılarının davranıřlarını kontrol etmeye y nelik ulus-devlet sorumluluklarına uygulanan normları” birbirinden ayırarak ele almıřlardır.⁷³⁴ Bu tasnifle  nerdikleri beř ilke ise ařaęıdaki gibidir:⁷³⁵

“Uluslararası Hukuk Topluluęuna İliřkin  nerilen Normlar

 lke #1: Hi bir devlet, bilgi altyapısının bařka bir devlete zarar vermek amacıyla kullanılmasına bilerek izin veremez.

⁷³³ Foreign & Commonwealth Office ve William Hague, “Security and Freedom in the Cyber Age - Seeking the Rules of the Road”, 04.02.2011, <https://www.gov.uk/government/speeches/security-and-freedom-in-the-cyber-age-seeking-the-rules-of-the-road> (31.12.2024).

⁷³⁴ Daniel J. Ryan ve Dięerleri, “International Cyberlaw: A Normative Approach”, **Georgetown Journal of International Law**, Vol.42, No.4, (2011), s.1182.

⁷³⁵ Ibid., s.1182 vd.

İlke #2: Zararlı bir siber olayın, bir devletin kontrolüne tabi bilgi altyapısı üzerinden gerçekleştirilmiş olması, o devletin bu kullanımdan haberdar olduğuna ve siber olaydan sorumlu olduğuna karine teşkil eder.

İlke #3: Muharip taraflardan birini diğerine tercih edecek hiçbir eylemde bulunmayan tarafsız bir devlet, tarafsız statüsünü kaybetmez.

İç Hukuk ve Düzenlemelere İlişkin Önerilen Normlar

İlke #4: Her devlet, kamu hukuku ve özel hukuk kanunları oluşturarak, ulusal yargı yetkisine tabi bilgi altyapısının güvenliğini ve dayanıklılığını sağlamakla yükümlüdür.

İlke #5: Bir ulus-devlet, kamu düzenine yönelik iç siber tehditlerin yanı sıra devlete yönelik dış siber tehditlere karşı da meşru müdafaa hakkına sahiptir.”

Yukarıdaki önerilerden de yansıdığı üzere, siber uzay için üzerinde genel söylem birliği olan belli başlı uluslararası hukuk ilkeleri belirginleşmektedir. Fakat en mutabık kalınan ilkelerin dahi somut çerçevesinin nasıl çizileceği ve uygulamada nasıl karşılık bulacağı büyük bir soru işaretidir. Ayrıca çoğu ilke, siber uzay özelinde ortaya çıkmış ilkeler olmaktan çok, genel uluslararası hukuk ilkelerinin siber uzayda da uygulanması düşüncesinin birer sonucu görünümündedir. Oysa DNS yönetimindeki “ilk gelen alır” ilkesi gibi genel uluslararası hukuktan bağımsız olarak siber uzayın kendi dinamiklerine göre şekillenmiş ilkeler de söz konusudur. Bunun dışında başta finans ve e-ticaret olmak üzere çevrimiçi hizmetlerin yürütülmesine dair çok sayıda ilke uluslararası hukukta norm haline gelmeye uygun niteliktedir.⁷³⁶

Siber uzayda insan haklarına yönelik hukuk ilkeleri, devletlerin derin yaklaşım farklılıkları nedeniyle uzunca bir süre daha yüzeysel nitelikte kalmaya devam edecek görünmektedir. Yaşama hakkı ve vücut bütünlüğünün korunması gibi küresel kabul görmüş ilkelerin, sözgelimi bir siber saldırı yoluyla fertlere cismani zarar verilmemesi yönünde karşılık bulması kolaylıkla sağlanabilecektir. Fakat ifade ve haber alma özgürlüğü, internet serbestliği, kişisel verilerin ve fikri mülkiyetin korunması gibi

⁷³⁶ Çevrimiçi bankacılık için zorunlu tutulacak güvenlik sertifikaları, Web sitelerinin kullanıcı hareketleri ve verileri üzerindeki hak ve yetkileri, spam içeriklere ve iletilere ilişkin kurallar gibi birçok husus, devletlerin ulusal düzenlemeleriyle veya devlet dışı aktörlerin iradeleriyle normatif değere kavuşmaktadır. Tüm bu konular siber uzayın hukuk ilkeleri olarak uluslararası topluluk nezdinde tescil edilip küresel geçerlilik kazanmaya namzettir. Bu tür ilkelerin bir kısmını içeren liste ve hakkındaki yorumlar için bkz. Polański, s.378.

başlıklara gelindiğinde, söz konusu yaklaşım farklılıkları daha kuvvetli hissedilecektir. Zira Medeni ve Siyasi Haklar Sözleşmesi'ne (*International Covenant on Civil and Political Rights*)⁷³⁷ 167 devlet taraf olmasına rağmen, uluslararası topluluk içerisinde bu hakların kavramsallaştırılmasında büyük tutarsızlıklar söz konusudur; “*siber uzayda bu tür anlaşmazlıkları çözmek, gerçek uzayda olduğundan daha kolay olmayacaktır*”.⁷³⁸

Henüz siber uzayın silahlı çatışma sahası olarak kabul edilmesi gibi kritik bir noktada dahi bloklar arası uyumsuzluk devam etmektedir. *Sic utere tuo ut alienum non laedas* kadim ilkesinin fiziksel uzaydaki uluslararası hukuk uygulamasında karşılığı artık nispeten yerleşik hale gelmişken; siber uzayda bunun sınırlarının nasıl belirleneceği netleşmiş değildir. Ayrıca bir devletin kendi ülkesinden başka bir devlete zarar verecek siber eylemleri önleme yönündeki objektif yükümlülüğünün tespiti ve uygulamaya dökülmesi güçlüğü de sürmektedir.

Devletlerin casusluğu yasaklayan iç hukuk normları vardır (casusluğun ölümle cezalandırıldığı ABD dahil) ancak casusluğu yasaklayan ya da casusluk eyleminin devlet egemenliğini ihlal ettiğini net şekilde ortaya koyan bir uluslararası hukuk normu yoktur.⁷³⁹ Fiziksel uzayda dahi barış zamanındaki casusluk faaliyetleri hakkında yerleşik bir uluslararası hukuk normu bulunmamaktayken, dramatik şekilde yaygınlaşan siber casusluk için bir uluslararası ilke geliştirilmesinin imkânı sorgulanmalıdır.

Daha özel bir başlık olarak *spam* içerik ve iletileri ele alan bir uluslararası antlaşmanın yokluğunda uluslararası örf ve âdet hukuku yegâne başvuru kaynağı olarak görülecektir. Fakat sözgelimi göndericisi belirsiz iletilerin yahut göndericisi belli olsa da istenmeyen iletilerin hukuka aykırılığıyla ilgili AB ve ABD yaklaşımları arasında dahi farklılıklar söz konusudur.⁷⁴⁰

Gri alanların ve tartışmalı hususların çokluğu, siber uzayın uluslararası düzenlenmesine ve bu husustaki ilkelerin tespitine tabii ki engel değildir. Aksine mevcut durum, gelecek adına üretken bir hukuk tespit ve geliştirme süreci vaat etmektedir. Devlet

⁷³⁷ UNTS, Vol.999, No.14668, 1976, s.172.

⁷³⁸ Ryan ve Diğerleri, s.1171.

⁷³⁹ Gary Brown ve Keira Poellet, “The Customary International Law of Cyberspace”, *Strategic Studies Quarterly*, Vol.6, No.3, (2012), s.133.

⁷⁴⁰ Polański, s.377.

egemenliğine ve yetkisine ilişkin başlıklar da bu sürecin esaslı konusu olmaya devam edecektir.



Üçüncü Bölüm

SİBER UZAY ÜZERİNDE DEVLET EGEMENLİĞİNİN GÖRÜNÜMLERİ VE SORUNLARI

I. SİBER UZAYIN BOYUT VE UNSURLARI ÜZERİNDE DEVLETİN YETKİSİ

Fiiller hukuktan ayrı, hukuk ise günümüzde devletten ayrı düşünülememektedir. Buna sebep olan süreç Birinci Bölüm’de özetlenmiştir. İç egemenlik kapsamında, devletin hukuku belirlemek ve uygulamak yönündeki meşru iktidarını ifade eden “yetki”, siber uzay ile zorunlu ve sorunlu bir ilişki içerisinde. Yabancılaşma unsuru içeren hukuk yargılamalarına ve kişiler arasındaki hukuki uyumsuzlukların çözümüne dair yetkinin çerçevesi, ceza yargısına göre daha sorunsuz ve tartışmasız görünmektedir. Fakat siber uzay ile ortaya çıkan mutlak çok uluslu iletişim yapısı ve bu yapıyı doğrudan biçimlendiren dev şirketlerin faaliyetleri; fiziksel uzaydaki ticari ya da fikri mülkiyete ilişkin uyumsuzluklar, evlenme-boşanma işlemleri veya haksız fiil yargılamaları gibi alışlageldik süreçlere göre daha karmaşık sonuçlara neden olmaktadır. Siber uzay üzerine hukuk vazedilmesi ve yabancılaşma unsuru içeren ceza yargılaması ise fiziksel uzayı düzenleyen hukuktan miras kalan problemleri yapıyı sürdürmektedir.⁷⁴¹

Yetkiyi, egemenliğe dair tartışmalardan bağımsız analiz etmek güçtür. Yine de devletin siber uzaydaki “yetki problemi” ve “siber egemenlik” konsepti ayrı başlıkların konularıdır. Şüphesiz yetki, egemenliğin bir sonucu olduğu gibi; siber egemenlik iddiası da uluslararası hukukta devletin yetkisi hakkındaki müktesebata dayanmaktadır. Ayrıca bu iki başlık, iç egemenlik – dış egemenlik ayrımının da bir tür karşılığını ifade etmektedir.⁷⁴²

Devletlerin yasama, yürütme ve yargı erklerinin izdüşümü niteliğindeki yetkilerini ülkeleri üzerinde kullanabilmeleri (yetkinin ülkeselliği (*territoriality*)),

⁷⁴¹ Siber uzayın genişlemesiyle anti-tröst, kişisel verilen korunması ve fikri mülkiyet gibi başlıklarda -Brownlie’den hatırlanacağı üzere- hukuk ve ceza yargılamaları arasındaki ayrı ayrı yer yer bulanıklaşsa da devletlerin çıkarları büyük tehdit altına girmediği sürece hukuki-cezai yetkilerin disiplinli ayrımına ilişkin yerleşik kabul tartışılmamaktadır.

⁷⁴² Siber uzayda iç egemenlik – dış egemenlik ayrımına ilişkin bir başka yorum için bkz. Tallin El Kitabı, ss.13-17.

uluslararası hukukun en kadim ve yerleşik ilkelerindendir. Ancak ülkeselliğin mutlak olmadığı ve hem yer bakımından hem kişi bakımından istisnaların söz konusu olduğu, günümüz uluslararası hukukundaki yetki doktrininde görülmüştür. Siber uzay gibi bir olgu gündeme geldiğinde ise yetkiye hâkim ilkelerle her bir unsurun ilişkisinin ayrı ayrı değerlendirilmesi gerekecektir.

Siber uzayda yetki problemi artık devlet yetkisinin siber uzaydaki mevcudiyetini değil; devletler arasında taksim ve tanzimini konu edinmektedir. Evet, siber uzay sınır aşan niteliktedir ve bilgi, sınırlar arasında serbestçe akmaktadır. Lakin siber uzayın bu özelliğinin karşı konulamaz bir doğal fenomenmiş gibi algılanması hatalı olacaktır. Zira “eğer bilgi serbestçe akıyorsa, bunun nedeni bizim buna izin vermemizdir”.⁷⁴³ Devletlerin kontrol imkanlarının gelişmesiyle şekillenen uygulamalar bunu destekler durumdadır. Şirketler de siber uzayda kendi normatif düzenlerini işletiyor gibi görünseler dahi nihayetinde devletlerin çizdiği hukuki çerçeve içerisinde çalışmaktadırlar. Devletlerin çerçeve çizme çabaları çoğu zaman şirketlerin normatif girişimlerini kovalıyor olsa da son tahlilde hukuk ve devlet yetkisi, gerçek ve etkili kurumlardır. Uygulamada da giderek bu çerçevenin belirginleştiği ve tabi olunması gereken düzenlemelerin arttığı görülmektedir. DNS yöneticisi ICANN ve belirlediği RUDRP üzerinden yürüten tahkim süreçleri, özgün özellikleriyle devlet dışı yetki alanının alametleri gibi görünseler de “*lex digitalis*” oluşumunun paradigmatik örnekleri olduklarını ileri sürmek fazla iddialı olacaktır.⁷⁴⁴

Genel teoride devletler lehine konuşmak kolay görünse de siber uzayın farklı vasıflardaki unsurları konu edilirken ve pratikte karşılaşılabilecek haller değerlendirilirken; sürecin, sözgelimi “Yunanistan’dan ateş ederek Türkiye’deki bir İngiliz vatandaşını öldüren İspanyol fail” üzerindeki yargı yetkisinin tespitinde izlenen yol kadar belirgin ve yerleşik olmadığı anlaşılmaktadır. *Kohl*’un gerçek vakalardan seçtiği sorular bu farka işaret etmektedir.⁷⁴⁵

“ABD internet kumar yasakları, Antigualı çevrimiçi kumar sağlayıcılarını kapsayabilir mi; cnnnews.com alan adına sahip bir Çin

⁷⁴³ Horatia Muir Watt, “Yahoo! Cyber-Collision of Cultures: Who Regulates?”, **Michigan Journal of International Law**, Vol.24, Iss.3, (2003), s.683.

⁷⁴⁴ Zekoll, s.369.

⁷⁴⁵ Uta Kohl, “Jurisdiction in Network Society”, Nicholas Tsagourias ve Russell Buchan (ed.), **Research Handbook on International Law and Cyberspace** içinde (69-96), Cheltenham: Edward Elgar Publishing, 2021, ss.72-73.

haber sitesinin (-ki cn, Çin ülke alan adıdır) ABD marka hukukuna uyması gerekir mi; AB veri koruma standartları Google Arama'ya uygulanabilir mi; ABD merkezli Yahoo! şirketinin Nazi hatıra koleksiyonları hakkında Fransız veya Alman yasalarına uyması gerekir mi; Hollandalı bir eczane, Almanya'da lisansı yoksa Alman müşterilere çevrimiçi olarak ilaç sunabilir mi; ya da yabancı bir korsan müzik ve film sitesi, kullanıcılarının bulunduğu devletlerin kanunlarına uymak zorunda mıdır?"

Hal böyleyken siber uzayda yetki problemini, hukuken oturmuş ve sağlıklı işleyen başlıklardan başlayarak, tartışmalı başlıklara doğru gidecek şekilde ele almanın isabetli olacağı kanaatindeyim.

A. Siber Uzayın Fiziksel Boyutu Üzerinde Devletin Yetkisi

1. Ülkesel Yetkiye Tabi Fiziksel Unsurlar

Devletin yetkisinin en köklü zemini ülkeselliğe dayanmaktadır. Siber uzayın fiziksel boyutu, çoğu zaman ülkeye doğrudan bağımlı olduğu için, devletin üç yetki türünde de tahakkümüne açıktır. Burada ortaya çıkacak hukuki problemlerin çözümü bu nedenle kolay olacaktır. Devletler, ülkelerinde bulunan elektronik iletişim altyapısı, sunucular, bilgisayarlar ve donatıları üzerinde yetki sahibidir. Taraf oldukları uluslararası antlaşmalardan doğan yükümlülükler saklı kalmak kaydıyla ülkelerinde bulunan fiziksel unsurların standartları ile satış ve kullanımına dair şartları serbestçe belirleyebilirler. Belli nitelikteki cihazların ülkeye girişini yasaklayabilir; hukuka aykırı özellikler taşıyanlara ya da hukuka aykırı şekilde kullanılanlara fiilen müdahale edebilirler. Ayrıca fiziksel unsurların kullanımıyla işlenen hukuka aykırı fiiller ya da bu unsurlara yönelik işlenen hukuka aykırı fiiller üzerinde yargı yetkisine sahip oldukları yine ülkesellik ilkesine dayanarak söylenebilir. Söz konusu yetkilerin sarahati, fiziksel varlıkların ülke ile ayrılmaz ilişkisinden kaynaklanmaktadır.

Fiziksel unsurlar, ekseriyetle devletlerin kara ve deniz ülkelerinde bulunduğu gibi bazı hallerde hava ülkelerinde seyir halinde de olabilirler. Devletler, hava ülkelerinde seyreden ve siber altyapıya sahip olan sivil hava araçları üzerinde yetki sahibidir. Dijital iletişimi dinleme ya da bozma, veri kaçırma, ulusal hukuku delege nitelikte internet içeriği sunma vb. olası hukuk ihlallerinde hava ülkesi kullanılan devlet, ilgili aracın iniş

yapmasını emredebilir. Hava aracının devlet aracı olması durumunda ise hava ülkesi kullanılacak devletten izin alınması gereklidir. Devletler, bu izin dahilinde seyreden aracın olası bir hukuk ihlalinde eylemin durdurulmasını ve gecikmeden hava ülkesinin terk edilmesini talep edebilir; bunun reddi halinde ise söz konusu hava aracına karşı gerekli ve orantılı önlemleri uygulayabilirler.⁷⁴⁶

2. Ülke Dışı Fiziksel Unsurlar

Siber uzayın fiziksel boyutunun, devletlerin ülkeleri dışında kalan kısımları da bulunmaktadır. Devletlerin karasuları dışında bulunan sualtı kabloları ve devletlerin hava ülkeleri için belirlenen sınırın üstünde bulunması hasebiyle uydular için ülkesel yetkiden söz etmek mümkün değildir.

a. Açık Deniz Sualtı Kabloları

BMDHS hükümlerine göre açık denizlerde sualtı kablo ve boru hattı döşeme serbestisi bulunmaktadır.⁷⁴⁷ Kıta sahanlığı içerisinde de kıyı devletinin faaliyetlerini engellemek kaydıyla tüm devletler için deniz altına kablo döşeme, kullanma ve bakımlarını yapma serbestisi geçerlidir. Kıyı devletinin rızası, bölge içerisinde kablo döşemek için kullanılacak güzergahın belirlenmesinde aranmaktadır.⁷⁴⁸ Karasuları ötesinde sualtı kablosu döşeme yetkisi uluslararası hukukta yerleşik bir norm olsa da bu kablolarla yönelik zarar verici eylemler için hangi devletin yargı yetkisi kullanabileceği hususunda tartışmalar mevcuttur. Kıta sahanlığında bulunan sualtı kabloları için şayet münhasır ekonomik bölge rejiminde öngörülen hakların uygulanabileceği kabul edilirse kıyı devletinin yetki sahibi olduğu söylenebilir.⁷⁴⁹ Açık denizler için ise cari deniz hukuku rejimi, ancak zarar veren -sözelimi- geminin bayrak devletinin veya failin vatandaşı olduğu devletin münhasıran yetkili olduğu sonucuna ulaştırmaktadır.⁷⁵⁰ Bu durum, devlet adına açık denizde gerçekleştirilen sabotaj eylemleri üzerinde caydırıcı bir yetki tesis

⁷⁴⁶ Kriangsak Kittichaisaree, **Public International Law of Cyberspace**, Cham: Springer, 2017, s.24.

⁷⁴⁷ BMDHS, m.87/1-c ve m.112.

⁷⁴⁸ BMDHS, m.79.

⁷⁴⁹ Jason Halog, Paul Margat ve Michael Stadermann, “Legal Considerations on the Protection of Subsea Cables in the International and National Legislative Framework”, **3rd European Workshop on Maritime Systems, Resilience and Security 2023 (MARESEC 23)**, Bremen: Institut für den Schutz maritimer Infrastrukturen, 04.10.2023, s.3.

⁷⁵⁰ BMDHS, m.92/1, m.94/1, m.113.

edilememesi nedeniyle eleştirilmektedir.⁷⁵¹ Yakın bir örnekte; 2 ve 8 Şubat 2023'te birer Çin bandıralı ticaret gemisi, Doğu Çin Denizi'ndeki kabloları koparmış ve Tayvan'a bağlı Matsu Adaları'nda düzeltilmesi oldukça maliyetli ve zaman alıcı olacak internet kesintilerine yol açmıştır. Bu eylemin kasıtlı olduğuna dair bir delil bulunmasa da Tayvanlı yetkililer olayın, Çin hükümetinin süregelen tacizlerinden biri olduğunu iddia etmişlerdir.⁷⁵² Bu tür vakalarda bayrak devleti -şayet gerçekten devlet adına bir sabotaj söz konusu ise tabii olarak kendisinden bekleneceği üzere- yetkisini etkili bir şekilde kullanmadığı takdirde, siber uzayın sağlıklı işleyişi için hayati öneme sahip sualtı kablolarının korunmasında zafiyet ortaya çıkacaktır. Henüz telgraf döneminde 1884 tarihli Denizaltı Telgraf Kablolarının Korunması için Sözleşme (*Convention for the Protection of Submarine Telegraph Cables*) için görüşmeler sürerken; 1869 yılında ABD, kablolarla karşı işlenen suçların deniz haydutluğuna eşdeğer olarak görülüp evrensel yargı yetkisine tabi kılınmasını talep etmiş fakat bu talep konferansta reddedilmiştir.⁷⁵³ Bu perspektifle BMDHS hükümlerine bakıldığında deniz haydutluğunu tarif eden m.101 hükmünü tekrar kontrol etmek gerekir. “*Özel bir geminin veya özel bir uçağın mürettebatı veya yolcuları tarafından özel amaçlarla işlenen*” ve “*herhangi bir devletin yargı yetkisi dışında bulunan, bir gemiye, uçağa, şahıslara veya mallara karşı yöneltilmiş, herhangi bir gayri hukuki şiddet ve tutuklama veya herhangi bir yağmacılık hareketi*”⁷⁵⁴ ifadeleri, yoruma ve tartışmaya açık niteliktedir. “*Herhangi bir devletin yargı yetkisi dışında bulunan... mallar*” tanımını, açık denizlerdeki sualtı kablolarını da dahil edecek şekilde yorumlamak mümkündür. Ancak özel amaç kriterinin çok istisnai ihtimaller dışında sağlanması güç olacaktır. Ayrıca bu kablolarla yönelik gerçekleşen ya da gelecekte gerçekleşmesi beklenen hukuka aykırı ve kasıtlı fiillerin, devlet dışı aktörler tarafından işlense dahi politik amaçlara dayalı ve bir devlet güdümünde olması muhtemeldir. Bu durumlarda bayrak devletinin yargı yetkisini etkin şekilde kullanması beklenemeyeceği gibi deniz haydutluğu suçu da “özel amaç” kriteri bakımından husule

⁷⁵¹ Halog, Margat ve Staderman, s.3; Amy Paik ve Jennifer Counter, “International Law Doesn’t Adequately Protect Undersea Cables: That Must Change”, Atlantic Council, 25.01.2024, <https://www.atlanticcouncil.org/content-series/hybrid-warfare-project/international-law-doesnt-adequately-protect-undersea-cables-that-must-change/> (31.12.2024).

⁷⁵² Huizhong Wu ve Johnson Lai, “Taiwan Suspects Chinese Ships Cut Islands’ Internet Cables”, Associated Press, 18.04.2023, <https://apnews.com/article/matsu-taiwan-internet-cables-cut-china-65f10f5f73a346fa788436366d7a7c70> (31.12.2024).

⁷⁵³ International Law Association, Committee on Submarine Cables and Pipelines, Submarine Cables and Pipelines under International Law, **Interim Report 2020**, s.22, para.78.

⁷⁵⁴ BMDHS, m.101/a-ii

gelmeyecektir. Fail devletin uluslararası sorumluluğuna gidilebilecek olsa da bu yolun, evrensel yargı yetkisine veya en azından objektif menfaat sahibi devletlerin yetki kullanımına göre etkililik ve caydırıcılık açısından oldukça zayıf kalacağı açıktır. Kabloların modern telekomünikasyondaki önemine binaen, pasif vatandaşlık ilkesinin istisnai şekilde mallara genişletilerek kablo sahibinin tabi olduğu devlete de yargı yetkisi tanınması yönünde dile getirilen talep,⁷⁵⁵ makul bir çözüm olarak değerlendirilebilir.

b. Siber Kapasiteli Uydular ve Uzay Araçları

1967 tarihli Ay ve Diğer Gök Cisimleri Dâhil, Uzayın Keşif ve Kullanılmasında Devletlerin Faaliyetlerini Yöneten İlkeler Hakkında Antlaşma (*Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and Other Celestial Bodies*)⁷⁵⁶ ve 1974 tarihli Dış Uzaya Fırlatılan Cisimlerin Tescili Sözleşmesi (*Convention on Registration of Objects Launched into Outer Space*)⁷⁵⁷ hükümlerine göre; Uzayın Barışçıl Amaçlarla Kullanımı Komitesi (*Committee on the Peaceful Uses of Outer Space – COPUOS*) tarafından tescil edilmiş olmak şartıyla bütün devletlerin barışçıl amaçlarla uzaya uydu vb. araçları gönderme hakkı vardır.⁷⁵⁸ Açık denizlere kablo döşenmesinde olduğu gibi serbestçe uzaya uydu gönderen devletlerin bu unsurlar üzerindeki yetkisi ülkesellik dışında şekillenmektedir. Uydular ve kullanımlarıyla gerçekleşen fiiller üzerinde, tescil sahibi fırlatan devlet için vatandaşlık ilkesine dayalı yetki tanınmıştır. Bununla birlikte, uyduların ve siber kapasiteye sahip uzay araçlarının meydana getireceği zararlardan, devlet dışı aktörler tarafından işletilseler dahi fırlatan devletin uluslararası sorumluluğu doğacaktır.⁷⁵⁹ Söz konusu unsurların zarara uğradığı durumlarda ise 1972 tarihli “Uzay Cisimlerinin Verdiği Zararlardan Dolayı Uluslararası Sorumluluk Hakkında Sözleşme (*Convention on International Liability for Damage Caused by Space Objects*)”⁷⁶⁰ ile zarara uğrayan fırlatan devlete, zarar veren fırlatan devletten tazminat talebinde bulunma hakkı tanınmıştır.⁷⁶¹ Fakat zarar

⁷⁵⁵ Paik ve Counter, International Law Doesn't...

⁷⁵⁶ Yaygın adıyla “Dış Uzay Antlaşması (*Outer Space Treaty*)”; UNTS, Vol.610, No.8843, 1970, s.205.

⁷⁵⁷ Yaygın adıyla “Kayıt Sözleşmesi (*Registration Convention*)”; UNTS, Vol.1023, No.15020, 1976, s.15.

⁷⁵⁸ Dış Uzay Antlaşması, m.1 ve m.4.; Kayıt Sözleşmesi, m.2/1.

⁷⁵⁹ Dış Uzay Antlaşması, m.6, m.7 ve m.8; Dış Uzay Antlaşması’nda fırlatan devletin sorumluluğu düzenlendikten sonra, 1976 tarihli Kayıt Sözleşmesi ile fırlatan devlete tescil yükümlülüğü getirilmiştir.

⁷⁶⁰ Yaygın adıyla “Uzay Sorumluluk Sözleşmesi (*Space Liability Convention*)”; UNTS, Vol.961, No.13810, 1975, s.187.

⁷⁶¹ Uzay Sorumluluk Sözleşmesi, m.8.

uzayda gerekleřtiđi takdirde bu sorumluluđun dođması iin, fırlatan devletin veya hareketlerinden sorumlu olduđu kiřilerin herhangi bir kusurundan kaynaklanmıř olması gerekmektedir.⁷⁶² Hkm bu ynyle uluslararası sorumluluk hukukundaki kusursuz sorumluluk yaklařımına bir istisna zelliđindedir.

Hem sualtı kablolarının hem uyduların kt niyetli faaliyetlere karřı uluslararası gvence altına alınması ihtiyaı srmektedir. Bu husus, UNOEWG-2'nin nc yıllık ilerleme raporunda da gncel olarak vurgulanmıřtır.⁷⁶³

B. Siber Uzayın Kiři Unsuru zerinde Devletin Yetkisi

Siber uzayın en nemli unsuru olan insan, fiziksel / mantıksal boyutlar ve veri ile eřitli iliřki tipleri ierisindedir. Bu tipleri ok sayıda tasnif modeliyle sınıflandırmak mmkndr. İnsanlar ferdi řekilde veya topluluklar vasıtasıyla řahsen; sivil toplum kuruluřları ve řirketler aracılıđıyla da kurumsal olarak siber uzayda varlık gsterirler. Bylece mimar, reten/tketen, hizmet veren/alan, ykleyen/indiren, veri depolayan, su iřleyen, kamu hizmeti gren gibi; bir kısmı fiziksel uzayda da birebir karřılıđı olan, bir kısmı ise siber uzaya zg olan muhtelif konumlarda bulunabilirler. Devletin yetkisine konu olma řekilleri ise bulundukları bu konuma gre belirlenir.

Devletin gerek ve tzel kiřiler ile kurduđu egemenlik iliřkisi kural olarak uyrukluk esasına dayanmaktadır. Ayrıca lkesinde bulunan veya faaliyet gsteren kiřiler iin de lkesellik esasına dayalı egemenlik hakları sz konusudur. Bu hususlardan yukarıda “Yetkiye İliřkin Ayrımlar” bařlıđında bahsedilmiřtir. Tartıřmasız kısımdan bařlamak gerekirse, gerek kiřilerin siber uzayda iřledikleri fiiller zerinde, vatandařı oldukları devletin; tzel kiřiliklerin faaliyetleri zerinde de tabi oldukları devletin dzenleme, icra ve yargı yetkisine sahip olduđu aıktır. Esasen kiřiler zerindeki yetkide temel problem, -siber uzayın uluslararasılıđa meydan okuyan btnleřik kresel yapısından kaynaklı olarak- uyrukluk iliřkisi bulunmayan kiřiler iin yetki kullanımında dođmaktadır.

⁷⁶² Uzay Sorumluluk Szleřmesi, m.3.

⁷⁶³ A/79/214, s.7, para.16.

1. Y kleyen ve İndiren Teorisi

Literat rdeki  nc   alıřmalardan birinde *Menthe*, insan ve siber uzay arasında “bilgiyi siber uzaya koymak” ve “bilgiyi siber uzaydan  ıkarmak” řeklinde iki temel etkileřim bi imi olduėunu belirtip “y kleyen ve indiren teorisi”  zerinden hareket etmiřtir.⁷⁶⁴ Bunu fiziksel uzaydaki casusluk faaliyetinde bir casusun bilgiyi bir yere bırakmasını ve ilgilisinin sonra onu oradan almasına benzeten yazar; aradaki temel farkın “ zel niyet” olduėuna dikkat  ekmiřtir. Zira internet eriřimine sunulan bir bilgiye  oėu zaman kimin nereden ulařacaėı  ng r lemez ve y kleyen, bilgiyi bu durumun farkında olarak y kler.⁷⁶⁵ Sonu ta kendiliėinden ulusařırı bir eylem ger ekleřmiř olur.

Y kleyen ve indiren teorisi kullanılarak  rnek bir sorun modeli oluřturulabilir. Devletin d zenleme yapma yetkisinin (*prescriptive jurisdiction*) sınırsız niteliėi g z  n ne alınırsa; X Devleti’nin bir i erik t r  i in y kleyen ve indirene dair ihdas etmesi muhtemel, yasaklayıcı nitelikteki hukuk normlarında,  lkeselliėe g re  aprazlanmıř d rt durumlu bir kombinasyon  ng r lebilir.⁷⁶⁶

A- İ eriėin  lke i inde y klenmesinin yasaklanması

B- İ eriėin  lke sınırları dıřında y klenmesinin yasaklanması

C- İ eriėin  lke i inde indirilmesinin yasaklanması

D- İ eriėin  lke sınırları dıřında indirilmesinin yasaklanması

D zenleme yapma yetkisinin aksine, icra yetkisinin (*enforcement jurisdiction*) ve yargı yetkisinin (*adjudicative jurisdiction*) kiřiler  zerinde kullanım imk nı her senaryoda farklı oluřacaktır. Yukarıdaki durumlar, evrensel yargı yetkisi ya da devletin hayati menfaatlerine dair koruma ilkesine dayalı yargı yetkisi doėuracak bir fiil s z konusu olmadıėı varsayımıyla deėerlendirilecektir.

⁷⁶⁴ Yazar, bu tasnifi birebir iletiřimi hari  tutarak, birden  oėa iletiřim řekli i in kullanmıřtır; *Menthe*, s.73.

⁷⁶⁵ *Ibid.*, 74.

⁷⁶⁶ D zenlemeler sayısız kural ve istisna i erebilirler. Dolayısıyla sunulacak  rnekler sınırlı sayıya tabi deėildir. D rt durum, idealize edilerek  alıřmanın amacına uygun bir analiz yapılabilmesi maksadıyla sınırlanmıřtır.

Öncelikle belirtilmelidir ki; her durumda yükleyen ya da indiren fail şayet X Devleti vatandaşı ise vatandaşlık ilkesine bağlı yargı yetkisi doğacaktır. Ülke içerisindeki aksiyonları ele alan (A) ve (C) durumları uygulanabilirlik açısından daha elverişlidir. Failler X Devleti vatandaşı olmasalar dahi fiili ülke içerisinde gerçekleştirdikleri için ülkesellik ilkesinin işletilmesi mümkün ve kolay olacaktır.

(B) durumunda, ülke dışında bulunan yabancıнын yüklediği içeriğin özelliklerine göre farklı sonuçlar doğacaktır. Zira öncelikle fiilin objektif ülkesellik ilkesine veya koruma ilkesine uygunluğunun ve evrensel yargı yetkisi kapsamına girip girmediğinin tespit edilmesi gerekecektir. Ayrıca yargı yetkisi kullanılsa dahi kararların ülke dışındaki yabancı üzerinde icra edilmesi ancak failin ülke ile maddi ilişkileri üzerinde mümkün olabilecektir.

(D) durumu ise pratikte ancak yüksek düzeyde otoriter bir devletin ülke dışındaki vatandaşları için karşılığı olabilecek bir normu ifade etmektedir. Nitekim içeriği ülke dışında indiren bir yabancı için yargı yetkisinin oluşması, henüz çocuk pornografisi gibi ciddi suç konuları için dahi pek mümkün görünmemektedir.⁷⁶⁷

Yukarıdaki modelin somut uyarlaması için “çevrimiçi kumar” örneği tercih edilebilir. X Devleti, ilgili resmi otoritesinden izin almaksızın çevrimiçi kumar hizmeti sağlayan (yükleyen) ve bu hizmeti kullanarak kumar oynayan (indiren) kişiler için cezai yaptırım öngörebilir. Yükleyen ve indiren kişiler X Devleti vatandaşı ise, bulundukları ülkeden bağımsız olarak yargı yetkisine konu olurlar. Çoğu durumda yükleyen bir şirket olacaktır ve tüzel kişilere özgü güvenlik tedbirlerine de başvurulacaktır. Yükleyen ve indirenin yabancı oldukları durumda; fiili X Devleti ülkesi içerisinde gerçekleştirdikleri

⁷⁶⁷ Budapeşte Sözleşmesi m.9/1-d hükmünde bu türden içerikleri “temin etmek (*procuring*)” suç olarak tanımlanmıştır. Sözleşme ile aynı oturumda Avrupa Konseyi Bakanlar Komitesi tarafından kabul edilen açıklayıcı raporda, temin etmek fiilinin aktif şekilde çocuk pornografisi elde etmek (örnek olarak; indirmek suretiyle) anlamına geldiği belirtilmiştir. Ayrıca Türkiye’de 5237 sayılı Türk Ceza Kanunu (TCK) m.226/3; Birleşik Krallık’ta 1978 tarihli Çocukların Korunması Yasası (*Protection of Children Act*) 1. Bölüm/m.1-c; ABD’de Çocuk Pornografisi Oluşturan ya da İçeren Materyalle İlgili Belirli Faaliyetler (*Certain Activities Relating to Material Constituting or Containing Child Pornography*) başlıklı 18 U.S. Code §2252A hükümlerinde de diğer aktif fiillerin yanı sıra erişmek veya indirmek değil ancak “bulundurma” fiilinin suç olarak tanımlandığı görülmektedir. Yargıtay da “ancak kanunilik ilkesi gereği, depolama veya bulundurma eylem ve amacı olmaksızın, salt görüntülere bakmak, seyretmek veya dinlemek suretiyle bu suçlar işlenemez” ve “...seyretmek amacıyla indirip-yükledikten sonra silinmesi ile de suç oluşmayacaktır” ifadeleriyle konuyu izah etmiştir; Yargıtay 4. Ceza Dairesi, E.2021/30178, K.2021/27676, 25.11.2021. Bu bakımdan depolamak/barındırmak yine siber uzay bağlamında bir fiil olmakla birlikte, internete dayalı yükleyen / indiren teorisinden ayrı değerlendirilmelidir.

takdirde bu kez ülkesellik ilkesi uyarınca yine yargı yetkisi doğacaktır. X Devleti'nin, ülkesi dışında çevrimiçi kumar oynayan yabancı uyruklu kişilere yaptırım öngörmesi, makuliyet sınırının dışında kalacaktır. Ülke dışındaki yabancıların çevrimiçi kumar hizmeti sunmasına gelindiğinde ise bazı ihtimalleri ayrı ayrı ele almak gerekir. Şayet sunulan hizmet ülke içerisinden erişime açıksa -ki çoğu durumda yükleyen, konuma göre erişimi sınırlandıracak bir filtreleme kullanmayacaktır- X Devleti, fiilin ülkesinde etki oluşturduğundan bahisle objektif ülkesellik ilkesine dayanarak yargı yetkisi ileri sürebilecektir. Hizmete eğer kendi ülkesinden erişilemiyorsa yetki ileri sürmek yine makuliyet sınırının dışında kalacaktır. Günümüz şartlarında X Devleti'nden beklenen, kendi ilgili resmi otoritesinden izin alınmaksızın kumar hizmeti sunan Web sitesine erişimi engellemesidir. Ancak yükleyenin bu yasadışı hizmetin X Devleti ülkesinde erişilebilir kalmasında vazgeçilmez bir menfaati varsa, bekleneceği üzere mevcut internet yönetişimi dahilinde bulacağı yollarla erişim engelini delmeye çalışacak ve ekseriyetle başarılı olacaktır. Böylece kişi üzerinde yaptırım uygulanamadığı sürece X Devleti'nin kanun ile düzenlediği amacına ulaşması zora girecektir.

Yukarıdaki analizlerden anlaşılacağı üzere -çok müstesna ihtimaller göz ardı edilirse- esas kriz, yabancı uyruklu ve ülke dışındaki yükleyen fail için geçerlidir. Nitekim devletlerin yargı yetkisi temelde ülkeselliğe ve vatandaşlık bağına dayanırken; internet, iki esastan da uzak yapıdadır. Uygulanabilir yegâne yol, objektif ülkesellik ilkesinin sağlıklı yorumlanması ve etkin işleyişinin sağlanmasıdır. Yahoo! Davası da bu durumun tam karşılığı olan bir örnektir. Yahoo! Davası'ndan 5 yıl önce, 1995'te ABD'de Minnesota Başsavcısı'nın yayınladığı muhtıra ise söz konusu soruna dair doğurduğu tartışmalarla dikkat çekicidir. *“Tüm internet kullanıcıları ve sağlayıcılarına uyarı”*⁷⁶⁸ başlığıyla Web üzerinden yayınlanan muhtırada; *“Bilginin Minnesota'da yayılacağını bilerek internet aracılığıyla bilgi aktaran Minnesota dışından kişiler, eyalet ceza ve medeni kanunlarının ihlalinde Minnesota mahkemelerinde yargı yetkisine tabidir”* ifadesi kullanılmıştır.⁷⁶⁹

⁷⁶⁸ Mohammad Osiur Rahman, Nour Mohammad ve Mohammad Mahabubur Rahman, “Towards Understanding Personal Jurisdiction in Cyberspace: An Overview of American Try-Out for Internet Cases”, **International Journal of Law and Management**, Vol.50, No.3, (2008), s.116.

⁷⁶⁹ Menthe, s.75.

Minnesota Başsavcısı'nın muhtırası hakkında -ABD'nin federal yapısından kaynaklı hukuki sorun ve tartışmalar bir yana- dönemin şartları itibarıyla *Menthe*'nin eleştirisi ve Yahoo!'nın Fransa'daki savunması aynı temele dayanmaktadır. İnternet söz konusu olduğunda herkes, yükleyeni olduğu içeriğin Minnesota'da ya da Fransa'da erişilebilir olduğunun bilincindedir. Eğer yükleyenin, yüklediği içeriğe dünyada erişilebilen her yerin hukukuna uymak zorunda olduğu kabul edilirse yükleyen için hukuken çok ağır bir sorumluluktan bahsedilmiş olacaktır. *Brierly*, bu tür bir düşünce için 1928'de görüşlerini şöyle serdetmiştir:⁷⁷⁰

“Fiilin, sanığın tabi olduğu bazı kanunlara aykırı olması, suç kavramının temelini oluşturur ve her ferdin, her zaman ve her yerde, her devletin kanunlarına tabi olduğu veya olabileceği fikri, bizihi kabul edilemez olduğu gibi, bağımsız ancak ülkesel olarak sınırlandırılan devletlerce örgütlenmiş dünya düzeniyle de çelişen anarşik bir ilkedir.”

Kişilerin birden fazla devletin hukukuna aynı anda uyma zorunluluğu, çağımızın kaçınılmaz bir gerekliliği halini almıştır. Lakin her devletin farklı menfaat ve beklentileri üzerinden ihdas ettiği normların tamamına siber uzayda uyma zorunluluğunun pratikte imkansızla yakın olduğu aşıkardır. Zira ülkesel yetki iddiasının geniş yorumlanmasıyla ortaya çıkacak durumda, yükleyenler her bir alan için en kısıtlayıcı norma sahip devletin hukukuna uymak mecburiyetinde kalacaktır. Bu konuda *Goldsmith* ve *Wu*'nun esprili bir dille yaptıkları eleştiri, *Brierly*'nin çözümlemesini destekler niteliktedir:⁷⁷¹

“Sorunu özetleyen eski bir Avrupa fıkrası var. Fıkraya göre cennette Fransız aşçılar, İngiliz hükümeti, İsviçre trenleri ve İtalyan aşıklar vardır. Cehennemde ise tam tersine Fransız hükümeti, İtalyan trenleri, İngiliz aşçılar ve İsviçreli aşıklar bulunur. İnternetin ülkesel kontrolü de hukuki cehennemin paralel bir versiyonunu vaat ediyor gibiydi: Singapur ifade özgürlüğü, Amerikan haksız fiil hukuku, Rus ticari düzenlemeleri ve Çin medeni haklarının olduğu bir dünya.”

Devletlerin egemenlik kaynaklı yetkileri vasıtasıyla siber uzayı düzenleme eğilimlerine yönelik eleştirilerde haklılık payı olmakla birlikte, devletler de tabii ki taleplerinde haksız değildir. İnternet başta olmak üzere siber uzay bünyesindeki yapıların işleyişi, devletlerin kamu düzenlerine, ekonomilerine ve hatta milli güvenliklerine yönelik birçok tehdidi bünyesinde barındırmaktadır. Günümüzde artık Minnesota

⁷⁷⁰ James Leslie Brierly, “The Lotus Case”, *Law Quarterly Review*, Vol.44, (1928), ss.161-162.

⁷⁷¹ Goldsmith ve Wu, ss.6-7.

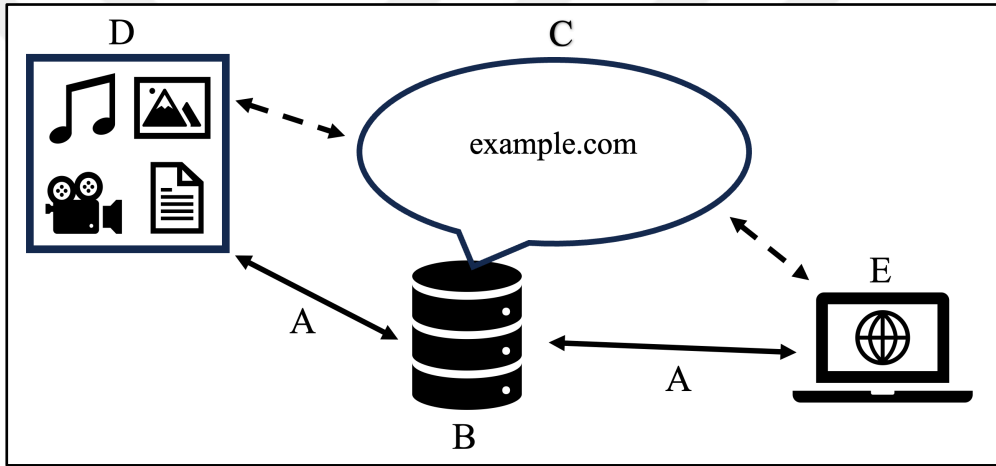
Başsavcısı'nın ve Yahoo! Davası'nın dönemi geride kalmış, teknolojinin ve hukukun gelişimi bazı pratik sorunları çözmüştür. Terminoloji de paralel olarak gelişmiş, yükleyen / indiren teorisi yine konunun özünü oluştursa da sùjeler daha detaylı tanımlamalarla çeşitlenmiştir. Uygulamada devletler, hukuka aykırı içeriğe karşı mantıksal unsurlar üzerinden erişim engeli ve içeriğin kaldırılması gibi yöntemlerle mücadele etmekte ve kısmen başarıya ulaşmaktadır. Fakat kişiler üzerindeki yetkinin tespiti ve bilhassa icrasında halen gri bölgeler ve fiili zorluklar mevcuttur.

2. İnternet Sùjelerinin Modern Tasnifi

Öncelikle belirtmek gerekir ki siber uzayın insan unsuru sadece internet aktörleri üzerinden değerlendirilmemelidir. Fiziksel boyuttaki cihaz ve altyapı elemanlarını tasarlayan, üreten, ticaretini ve kurulumunu yapan vs. bütün kişiler siber uzaya aktif katkıda bulunmaktadır. Bu kişiler üzerindeki yargı yetkisi, fiziksel uzay şartlarında işletildiği için görece sorunsuzdur. Mantıksal boyutun teşekkülünde etkinlik gösteren kişiler ise faaliyetlerinin doğası ve sonuçları itibarıyla yetki başlığındaki esas problemin konusudur. Yazılım altyapısının kurulması, dijital içeriğin üretilerek erişime açılması, bu süreçleri yürüten protokollerin işletilmesi, son kullanıcının içeriğe erişmesi ile erişime dek sanal ortamda gerçekleşen reklam, pazarlama vs. fiillerin hepsi bu kişilerce işlenmektedir. Veri analizcileri, bilim insanları, siber güvenlik uzmanları ve bilgisayar korsanları gibi aktörler de yine farklı noktalardan mantıksal boyutla ilişki içerisinde. Uluslararası antlaşmalar ve ulusal hukuk düzenlemeleri, söz konusu kişiler hakkında farklılıklar arz eden tasnif ve tanımlar öngörmüştür. Sıhhatli ve tutarlı bir değerlendirme yapılabilmesi adına, hukuken kabul görmüş bazı tanımlar üzerinden ilgili sùjelerin tespiti gerekmektedir.

İnsanın mantıksal boyutla etkileşimi, fiziksel boyut dışarıda tutularak en temelden ele alındığında; mantıksal boyutu oluşturanlar ve ondan istifade edenler şeklinde ikili bir ayrıma tabi tutulabilir. Bu tasnif, yukarıdaki yükleyen ve indiren teorisinin de temelidir. Mantıksal boyutun muhtevasına bakıldığında; Web siteleri, çoklu ortam (*multimedia*) içerikleri, programlar, protokoller gibi unsurlarla karşılaşılacaktır. Hukuk, siber uzay ile muhatap olup sorunlarıyla yüzleştikçe; hukukun incelikli yapısı gereği bu unsurların her birini ortaya çıkaranlar, sürdürenler ve kullananlar için ayrı ayrı hüküm tesis edilmesi

gerekmiştir. Akademik inceleme açısından zorluk, uluslararası ve ulusal hukuk düzenlemelerinde kullanılan terminolojinin, gelişmişliğine rağmen yeknesaklıktan uzak olmasındadır. Maalesef birçok modern alanda olduğu gibi bu alanda da kavram – terim tutarsızlıkları söz konusudur. Esasen kavramlarda muğlaklık olmasa da mahut tutarsızlık, terimlerin kavramlarla ilişkilendirilmesinde ortaya çıkmaktadır. Bu nedenle önce kavramsal bir diyagram ortaya koyarak bunun üzerinde konuşmanın isabetli olacağı kanaatindeyim. Mantıksal boyut, insan olmadan anlamsızdır ve dahi mevcudiyeti mümkün değildir. İnsanın dahliyle mantıksal boyut -diğer işlevlerinin yanı sıra- bir iletişim sürecinin de parçası haline gelmektedir. En yaygın haliyle Web üzerinden yürüten bu süreç, aşağıdaki gibi ana hatlarıyla tasvir edilebilir:



Şekil.3: İnternet üzerinden içerik erişimi için örnek diyagram

Eldeki çalışmada ilgili sùjeler, şekilde görùlen unsurlarla ilişkileri çerçevesinde, mevcut harf sırasıyla incelenecektir. Bu noktada kısaca açıklamak gerekirse: A, altyapı aracılığıyla sunulan internet erişimi hizmetini; B, üzerinde sanal yapıyı taşıyan ve erişimcilerin taleplerine karşılık veren sunucuyu; C, sunucu üzerinde çalışan Web sitesini; D, Web sitesinde yayınlanmak üzere yüklenen içeriği; E, söz konusu içeriklere erişen tarafı ifade etmektedir. Kesik çizgiler ise unsurlar arasındaki sanal ilişkiyi temsil etmektedir. Aşağıda incelenen sùjeler için seçilen adlandırma ve tanımlar, ulusal ve uluslararası hukuk düzenlemeleri ile literatürde kullanılanlar arasından genel bir derlemenin sonucudur.

a. Erişim Sağlayıcı

Siber uzayın internet ve çevrimiçi kısmı için konuşulduğunda, öncelikle bu sektörün çalışmasını sağlayan aktörler olan erişim sağlayıcılardan bahsetmek gerekecektir. Şekil.3'te "A" ile belirtilen hizmeti sağlayan bu aktörler için literatürde yerleşik tabir internet servis sağlayıcıdır (İSS) (*internet service provider* (ISP)). Fakat "servis (hizmet) sağlamak" geniş kapsamlı bir kavram olduğu için Budapeşte Sözleşmesi'nde olduğu gibi kendi içinde bir ayrıma muhtaç durumdadır.⁷⁷²

"'hizmet sağlayıcı' terimi:

(i) Hizmetlerini kullananlara bir bilgisayar sistemi aracılığıyla iletişim kurma olanağı sağlayan her türlü kamu veya özel sektör tüzel kişisi, ve

(ii) böylesi iletişim hizmeti veya bu hizmetlerin kullanıcıları adına bilgisayar verilerini işleyen veya depolayan diğer her türlü tüzel kişiyi ifade eder."

5651 sayılı Kanun ise önce "erişim" kavramını "*bir internet ortamına bağlanarak kullanım olanağı kazanılması*" olarak tanımlamış; ardından "erişim sağlayıcı" için "*kullanıcılarına internet ortamına erişim olanağı sağlayan her türlü gerçek veya tüzel kişiler*" tanımı tercih edilmiştir. Yerli literatürdeki tartışmada, bir yandan yerleşik terim olan İSS'nin aslında "internet erişim sağlayıcı" kavramına karşılık geldiği belirtilirken;⁷⁷³ diğer yandan erişim sağlayıcının salt iletici (*mere conduit*) konumundaki süreyi ifade ettiği, İSS'lerin ise farklı hizmetleri de beraberinde sunmaları hasebiyle erişim sağlayıcılardan ayrıldıkları ileri sürmüştür.⁷⁷⁴ İSS bu şekilde geniş anlamıyla ele alındığında, erişim sağlayıcının esasen bir İSS türü olarak kabul edildiği görülmektedir.⁷⁷⁵ DSA'da ise "aracılık hizmeti sağlayıcı" tabiri kullanılarak, aşağıdaki ifadelerle bundan ne kastedildiği belirtilmiştir:⁷⁷⁶

"'Aracılık hizmeti', aşağıdaki bilgi toplumu hizmetlerinden birini ifade eder:

⁷⁷² Budapeşte Sözleşmesi, m.1/c.

⁷⁷³ Müberra Güngör ve Gökhan Evren, **İnternet Sektörü ve Türkiye İncelemeleri**, Ankara: T.C. Telekomünikasyon Kurumu, 2002, s.7.

⁷⁷⁴ Tamer Soysal, "İnternet Servis Sağlayıcılarının Hukuki Sorumlulukları", **Türkiye Barolar Birliği Dergisi**, Sayı.61, (2005), s.309.

⁷⁷⁵ Örnek olarak Öztekin, İSS başlığı altında "erişim sağlayıcı", "yer sağlayıcı", "internet sitesi/uygulaması işletmecisi", "sosyal medya platformu işletmecisi", "internet yayın platform işletmecileri ve medya hizmet sağlayıcı kuruluşlar" ve "toplulu kullanım sağlayıcı" olarak 6 farklı sùje tipini ele almıştır; Alp Öztekin, **Teori ve Uygulamada Türk İnternet Hukuku**, Ankara: Seçkin Yayıncılık, 2021, s.155 vd.

⁷⁷⁶ Dijital Hizmetler Yasası, m.3/g.

(i) bir hizmet alıcısı tarafından sağlanan bilgilerin bir iletişim ağında iletilmesinden veya bir iletişim ağına erişim sağlanmasından oluşan bir ‘salt iletici (mere conduit)’ hizmeti;

(ii) bir hizmet alıcısı tarafından sağlanan bilgilerin bir iletişim ağında iletilmesinden oluşan, bu bilgilerin otomatik, ara ve geçici depolanmasını içeren ve yalnızca bilgilerin diğer alıcılara talepleri üzerine iletilmesini daha verimli hale getirmek maksadıyla gerçekleştirilen bir ‘önbelleğe alma (caching)’ hizmeti;

(iii) bir hizmet alıcısı tarafından ve onun talebiyle sağlanan bilgilerin depolanmasıyla oluşan bir ‘barındırma (hosting)’ hizmeti.”

Servis sağlama eylemini geniş yorumlamak anlam itibariyle isabetli olsa da ilgili disiplinde kullanılan dile yerleşmiş olmasından mütevellit, erişim sağlayıcılar için artık İSS adlandırması terim haline gelmiştir. Esaslı faaliyetleri internet erişimi sağlamak olan İSS’lerin tabii ki salt ileticiliğin ötesinde işlev ve hizmetlerinin de olduğu bilinmektedir. İSS’lerin bir kısmı gerekli izinler dahilinde fiziksel altyapı yatırımı yapıp bu altyapıyı çalıştırmak suretiyle kullanıcılarına internet erişimi sağlamaktadır. Bazı İSS’ler de başka İSS’lere ait fiziksel altyapıyı kullanarak erişim hizmeti vermektedir. Yine gerek yasal yükümlülükler gerek şirket politikaları doğrultusunda DSA’da belirtilen hizmetler ve hatta daha farklı sektörel faaliyetler de İSS’lerce gerçekleştirilmektedir. Bununla birlikte, sahip olduğu internet erişimini başkasının ya da başkalarının kullanımına açmak da lafzi olarak erişim sağlamak kavramına uymakla birlikte, bu hizmeti sunan kişiyi İSS ya da erişim sağlayıcı kılmamaktadır. Söz konusu fiilin faili için doğru terim “kullanım sağlayıcı” olacaktır.⁷⁷⁷

Türkiye’de 2024 ilk çeyrek verilerine göre genişbant (broadband) internet erişiminde en çok abone sayısına sahip İSS’lerin sırasıyla TTNNet, Superonline, Vodafone Net, Türksat, Türknet, D-Smart ve Millenicom olduğu açıklanmıştır.⁷⁷⁸ Ayrıca mobil internet erişiminde Turkcell, Vodafone ve TT Mobil, İSS olarak faaliyet göstermektedir.⁷⁷⁹ 5651 sayılı Kanun’da “gerçek ve tüzel kişiler” ifadesi geçse de “Telekomünikasyon Kurumu Tarafından Erişim Sağlayıcılara ve Yer Sağlayıcılara Faaliyet Belgesi Verilmesine İlişkin Usul ve Esaslar Hakkında Yönetmelik”⁷⁸⁰ m.4/1

⁷⁷⁷ Öztekin, s.160.

⁷⁷⁸ Bilgi Teknolojileri ve İletişim Kurumu, **Türkiye Elektronik Haberleşme Sektörü Üç Aylık Pazar Verileri Raporu**, 2024 Yılı 1. Çeyrek, s.47.

⁷⁷⁹ Ibid., s.62.

⁷⁸⁰ R. G., 24.10.2007, Sayı.26680; (buradan itibaren “Faaliyet Belgesi Yönetmeliği”).

hükmü uyarınca bu hizmeti ancak yetkilendirilmiş sermaye şirketleri verebilmektedir.⁷⁸¹ “Elektronik Haberleşme Sektörüne İlişkin Yetkilendirme Yönetmeliği”⁷⁸² m.5/1 hükmü ise elektronik haberleşme hizmeti sunulması ve/veya elektronik haberleşme şebekesi veya altyapısı kurulup işletilmesi için ilgili kurumca işletmecinin yetkilendirilmesi gerektiğini belirtmiş; “işletmeci” ise m.4/1-o hükmüyle “...işleten şirket” olarak tanımlanmıştır. Genel AB normlarında, ABD ve İngiltere’de ise bu hizmet için izin ve ruhsat şartları öngörülmemiştir.⁷⁸³ Ağ tarafsızlığı (*network neutrality*), veri güvenliği, kalite standartları gibi şartları sağlayan girişimler, bildirim veya kayıt usulüyle faaliyete geçebilmektedir.

İnternet küresel bir ağ olarak düşünüldüğünde, bu ağa bir ülke sınırları içinden bağlanmanın ancak ülke dışına uzanan bir hat vasıtasıyla mümkün olacağı açıktır. Zira sistem, telgraftan bu yana böyledir. Ülke dışına erişim, alışlageldik şekilde kablolar vasıtasıyla olabileceği gibi kablosuz iletişim protokolleri ve uydular aracılığı ile de gerçekleştirilebilmektedir. Herhangi bir vatandaşın kendi imkanlarıyla fiziksel altyapı oluşturup müstakil ve sınır aşırı internet bağlantısı elde etmesi, madden ve fiilen imkansızla yakın olmakla birlikte hukuken de bulundukları devletlerin düzenlemelerine göre izin, lisans, teknik şartnameler gibi çok sayıda engelin aşılmasını gerektirecektir. Dolayısıyla yetkilendirme şartı arasın ya da aramasın bütün devletler esasen ülkelerini dışarıyla bağlayan İSS’lere muhataptır. Sonuç olarak devletlerin, ilgili hizmetleri bizzat kendi kurumlarıyla sunduğu durumlar haricinde de İSS’ler üzerinde açık bir yetkisi söz konusudur. İSS’ler veri politikaları, internetin erişime açık yahut kapalı tutulacak alanları, kullanıcı kayıtlarının belli şartlarda muhafazası, erişim kalitesi gibi birçok konuda hizmet verdikleri devletin hukukuna uymakla yükümlüdür. Devletlerin İSS’lerden beklentilerinin içeriği ve cari hükümlerin yerindeliği ise başka bir çalışmanın konusudur.

⁷⁸¹ İlgili hüküm: “Türkiye Cumhuriyeti sınırları içerisinde erişim sağlayıcı olmak isteyen sermaye şirketleri ile yer sağlayıcı olarak faaliyet göstermek isteyen gerçek veya tüzel kişiler, hizmet vermeye başlamadan önce Kurum tarafından düzenlenecek faaliyet belgesini almakla yükümlüdür”.

⁷⁸² R. G., 28.05.2009, Sayı.27241.

⁷⁸³ Soysal, ss.327-328.

b. Yer Sağlayıcı

5651 sayılı Kanun'da "*hizmet ve içerikleri barındıran sistemleri sağlayan veya işleten gerçek veya tüzel kişiler*"⁷⁸⁴ şeklinde tanımlanan yer sağlayıcılar, Şekil.3'te "B" ile ifade edilen hizmeti sunmaktadır. Barındırma (*hosting*), siber uzayın en güçlü sütunlarından. Zira mantıksal boyutun sosyal etkileşime açılması bu faaliyet ile mümkün olmaktadır. Bir içeriğin iletimi, doğrudan uçtan uca (*peer to peer* (P2P)) veya tamamen dağıtık ağlar üzerinde gerçekleştiği takdirde; teorik olarak içeriği barındırıp sunan (günlük dil ile "host eden"), kendi cihazları vasıtasıyla bizzat iletişimin taraflarıdır. Ancak siber uzaydaki en yaygın iletişim modeli, tarafların sunucular üzerinden veri aktarımı gerçekleştirmesidir. Web siteleri, e-posta ve dosya transfer sistemleri, sosyal medya platformları gibi çok sayıda internet hizmeti, verilerini merkezi sunucular üzerinde barındırmakta ve kullanıcılarının erişimine sunmaktadır. DSA'da, barındırma hizmeti iletişim amaçlı olduğu takdirde sağlayıcıların "çevrimiçi platformlar" alt kategorisi içerisinde değerlendirilmesi gerektiği tespit edilerek; "*yalnızca hizmet alıcıları tarafından kendi talepleri üzerine sağlanan bilgileri depolamakla kalmayıp, aynı zamanda bu bilgileri hizmet alıcılarının talebi üzerine kamuya yayan barındırma hizmetleri sağlayıcıları*" tanımı yapılmıştır.⁷⁸⁵ Rusya'da Bilgi, Bilgi Teknolojileri ve Bilginin Korunması Hakkında Federal Yasa'da (*Federal Law On Information, Information Technologies and Protection of Information*) da benzer şekilde yer sağlayıcının (*hosting provider*) "*bilgiyi sürekli olarak internete bağlı bilgi sistemleri içinde barındırmak için berim yeteneklerini kiralayan kişi*" olarak tanımlandığı görülmektedir.⁷⁸⁶ Bu düzenlemelerden anlaşılacağı üzere esasen hizmet ve içeriklerin kullanıcıların erişimine sunulması ya da internete bağlı tutulması, yer sağlayıcı olmanın kurucu unsurudur.

Uygulamada, çevrimiçi hizmet sunan büyük şirketlerin genellikle kendilerine ait sunucuları; görece küçük Web sitelerinin ve bazı video oyunlarını çok oyunculu oynamak isteyen kullanıcı grupları gibi unsurların ise barındırma hizmeti veren yer sağlayıcı şirketlere ait sunucuları kullandıkları bilinmektedir. Türkiye'de Faaliyet Belgesi

⁷⁸⁴ 5651 sayılı Kanun, m.2/m.

⁷⁸⁵ Dijital Hizmetler Yasası, m.13.

⁷⁸⁶ Buradan itibaren "Bilgi Yasası"; The Russian Federation Federal law No. 149-FZ of 14 July 2006, m.2/18. <https://eais.rkn.gov.ru/docs.eng/149.pdf> (31.12.2024).

Yönetmeliği hükümleri uyarınca, sunucu işletmek suretiyle “*yer sağlayıcı olarak faaliyet göstermek isteyen gerçek veya tüzel kişiler*”,⁷⁸⁷ gerekli belgeleri BTK’ya ulaştırıp akabinde faaliyet belgesi almak zorundadır.⁷⁸⁸

Devletler, uyrukluk ya da ülkesellik ilkelerine dayanarak yer sağlayıcılar üzerinde yetki sahibi olabilmektedir. Genel olarak yer sağlayıcıdan hukuken beklenen, barındırdığı unsurların daimî şekilde hukuka uygunluğunu denetlemesi değil; hukuka aykırı içerikten haberdar olduğu zaman bunu kaldırmasıdır.⁷⁸⁹ Ayrıca sunucudaki trafik verilerinin belirli sürelerde ve şartlarda saklanarak gerekli durumlarda resmi makamlarla paylaşılması da istenebilmektedir.⁷⁹⁰ Ancak devletler yer sağlayıcının yabancı veya yurt dışında olması, sunucuların yurt dışında olması, yurt içinde yer sağlayıcının temsilci, ofis, malvarlığının vs. bulunmaması gibi durumlarda sonuca ulaşmakta zorlanmaktadır. Ceza yargılamalarında ise özellikle trafik verileri için adli istinabe yoluna başvurulsa da gerek ilgili devletin gerek yer sağlayıcı şirketin yaklaşımları sebebiyle ortaya çıkan sorunlarla karşılaşmaktadır.⁷⁹¹ Sonuç olarak büyüklüğüne göre karşılaşılan sorunun göz ardı edilmesi ya da İSS vasıtasıyla ilgili yer sağlayıcıya yönelik erişim engeli getirilmesi gibi seçenekler devletlerce tercih edilegelmektedir.

c. Web Sitesi İşletmecisi

Web, bir bakıma yer sağlayıcıların omuzları üzerinde yükselmektedir. Şekil.3’te “C” ile gösterilen siteler de çeşitli Web protokollerine göre, belli IP adresleri ve alan adlarına bağlı sunucular üzerinden hizmet vererek siber uzayın mantıksal boyutunun en önemli unsurunu teşkil etmektedir. Web siteleri, gerçek veya tüzel fark etmeksizin en az bir kişiye aittir ve sahip olduğu alan adı hakkı belli periyotlarla yenilenerek işletilmektedir. Web’in yapısı gereği Web sitesini işleten kişi aynı zamanda sitenin bulunduğu sunucuyu da işletebilir ve aynı zamanda sitedeki içeriği de münhasıran kendisi

⁷⁸⁷ Faaliyet Belgesi Yönetmeliği, m.4/1.

⁷⁸⁸ Faaliyet Belgesi Yönetmeliği, m.9/2 ve m.10/3.

⁷⁸⁹ 5651 sayılı Kanun, m.5; Dijital Hizmetler Yasası, m.22; Elektronik Ticaret Direktifi, m.14; ABD Dijital Binyıl Telif Hakkı Yasası (*Digital Millennium Copyright Act* (DMCA)), Çevrimiçi Materyale İlişkin Sorumluluk Sınırlamaları (*Limitations on Liability Relating to Material Online*), 17 U.S. Code, §512, <https://www.govinfo.gov/app/details/USCODE-2022-title17/USCODE-2022-title17-chap5-sec512> (31.12.2024).

⁷⁹⁰ 5651 sayılı Kanun, m.5/3.

⁷⁹¹ T.C. Adalet Bakanlığı Dış İlişkiler ve Avrupa Birliği Genel Müdürlüğü, “İnternet Ortamında İşlenen Suçlarda Uluslararası Ceza İstinabe İşlemleri”, <https://diabgm.adalet.gov.tr/Home/SayfaDetay/internet-ortaminda-islenen-suclarda-uluslararasi-ceza-istinabe-islemleri14022020041756> (31.12.2024).

belirleyebilir. Fakat bu eylemlerin kategorik olarak ayrılması, hukuki rejimin tespiti açısından isabetli olacaktır.

Öztekin, sitenin işletilmesi faaliyetini esas alarak “internet sitesi/uygulaması işletmecisi” terimini önermiş, 5651 sayılı Kanun’da bu yönde bir tanımın bulunmamasını eleştirmiştir.⁷⁹² Söz konusu kanuna 2020’de -kamuoyunda Sosyal Medya Yasası olarak bilinen- 7253 sayılı Kanun⁷⁹³ ile eklenen “sosyal ağ sağlayıcı” teriminin, “*sosyal etkileşim amacıyla kullanıcıların internet ortamında metin, görüntü, ses, konum gibi içerikleri oluşturmalarına, görüntülemelerine veya paylaşımlarına imkân sağlayan gerçek veya tüzel kişiler*” şeklinde tanımlandığı görülmektedir.⁷⁹⁴ Diğer yandan ABD’de Çocukların Çevrimiçi Mahremiyetinin Korunması Yasası (*Children's Online Privacy Protection Act*) örneğinde “işletmeci (*operator*)” terimi “*internette bulunan bir web sitesini ya da bir çevrimiçi hizmeti işleten kişi*” şeklinde tanımlanırken,⁷⁹⁵ Rusya’da Bilgi Yasası’nda “internet sitesi sahibi (*internet site owner*)” terimi tercih edilerek “*söz konusu sitede bilgi yayınlama prosedürü de dahil olmak üzere, söz konusu internet sitesini kullanma yöntemini kendi rızası ve takdiriyle belirleyen kişi*” tanımı yapılmıştır.⁷⁹⁶

Bu noktada bazı hususların çözülmesi gerekmektedir. Şekil.3’teki şablona göre yürüyen bir iletişim sürecinde, Web sitesi işletmecisini içerik sağlayıcıdan ya da yer sağlayıcıdan ayıran özellik, mantıksal boyutta sunduğu aracılık hizmetidir. Bu bakımdan “sosyal ağ sağlayıcı”, terim ve tanım itibarıyla Şekil.3’teki C segmentini tam olarak karşılamaktadır. Fakat sosyal ağ sağlayıcılar Web sitelerinin yalnızca bir kısmını oluşturmaktadır. Web üzerinde çok farklı alanlarda faaliyet gösteren ve çok çeşitli işlevlere sahip 200 milyona yakın⁷⁹⁷ aktif site bulunmaktadır. Tek kişi tarafından işletilen ve içeriği de yine yalnızca aynı kişi tarafından sağlanan siteler olduğu gibi, içeriğin editoryal süreçlerden geçerek yayınladığı siteler, kullanıcılarına sadece depolama hizmeti sunan ve işlevi depolama sunucularına erişim için arayüz sağlamaktan ibaret olan siteler, çok sınırlı bir kullanıcı grubunun kullanımına tahsis edilmiş siteler, devletlere ait resmi

⁷⁹² Öztekin, s.224.

⁷⁹³ R. G., 31.07.2020, Sayı.31202.

⁷⁹⁴ 5651 sayılı Kanun, m.2/s.

⁷⁹⁵ 15 U.S. Code, §6501, <https://www.govinfo.gov/app/details/USCODE-2022-title15/USCODE-2022-title15-chap91-sec6501> (31.12.2024).

⁷⁹⁶ Rusya Bilgi Yasası, m2/17.

⁷⁹⁷ Konu hakkında bazı istatistikler için bkz. NJ, “How Many Websites Are There in the World?”, Siteefy, 04.10.2024, <https://siteefy.com/how-many-websites-are-there> (31.12.2024).

siteler gibi örneklere sahip çok geniş bir yelpaze söz konusudur. Ayrıca tarayıcı üzerinden erişilmeksizin sözgelimi mobil uygulamalar vasıtasıyla internet üzerinden bu hizmetlerin sunulması da mümkündür.

Mevcut hukuk normları ihtiyaca binaen Web sitelerini ayırma tabi tutmak durumundadır. Öyle ki; sözgelimi bir site türü için hukuka aykırı içeriğin önlenmesi ve kaldırılması devlet adına öncelikli mesele olabileceken başka bir tür için kullanıcıların kişisel verilerinin korunması site yapısı gereği öncelikli hale gelebilecektir. Kullanıcı sayısı ve kamusal etkisinin çok yüksek olması sebebiyle sosyal ağ sağlayıcılar için özel düzenlemeler öngörülmesinin makuliyeti açık olmakla birlikte; siber uzay için süje tasnifi yapılırken Web sitesi işletmecilerini üst başlık olarak değerlendirmek kanaatimce isabetli olacaktır. Zira barındırma – işletme – içerik ilişkisi çoğu zaman bulanıklaşmaktadır. Bir sitenin sadece aracılık faaliyeti yaptığı düşünüldüğü zaman dahi site mimarisi, görsel tasarımı ve özgülendiği amaç gibi unsurlar hem işletme eylemine hem de içeriğe dair özellikler taşımaktadır. Diğer yandan çoğu büyük Web sitesi işletmecisi aynı zamanda yer sağlayıcı fonksiyonunu da beraberinde yürütmektedir. Hangi tür dijital içeriklerin hukuka aykırı olduğu, sosyal ağlarda paylaşım açılan hukuka aykırı içeriklerden kimin sorumlu olduğu, bunların kaldırılma prosedürü, editoryal süreçlerin işlediği sitelerde bu sürecin yapısına göre kusur ve sorumluluk ilişkilerinin tespiti, bir Web sitesinde hangi unsurların bulunmasının zorunlu tutulacağı, güvenlik standartlarının ve site mimarisine ilişkin esasların tespiti gibi sorunlar hukuk düzenlerinde ayrı ayrı hükümlere tabi tutulabilmektedir. Türkiye örneğinde 6563 sayılı Elektronik Ticaretin Düzenlenmesi Hakkında Kanun'da⁷⁹⁸ e-ticaret⁷⁹⁹ siteleri için aşağıdaki gibi bir ayırma gidilmiştir:

“ç) Hizmet sağlayıcı: Elektronik ticaret faaliyetinde bulunan gerçek ya da tüzel kişileri,

d) Aracı hizmet sağlayıcı: Başkalarına ait iktisadi ve ticari faaliyetlerin yapılmasına elektronik ticaret ortamını sağlayan gerçek ve tüzel kişileri,”

Günlük dile, fiziksel uzaydaki karşılığını yansıttığı “market / pazar yeri” ifadeleriyle yerleşen “hizmet sağlayıcı / aracı hizmet sağlayıcı” ayrımı, esasen içeriğin kim tarafından sağlandığıyla ilgili bir ayırmadır. Ayrıca bu dahi mutlak bir ayırım değildir.

⁷⁹⁸ R. G., 05.11.2014, Sayı.29166.

⁷⁹⁹ Kanunun m.2/1-a hükmünde elektronik ticaret, “fiziki olarak karşı karşıya gelmeksizin, elektronik ortamda gerçekleştirilen çevrim içi iktisadi ve ticari her türlü faaliyet” şeklinde tanımlanmıştır.

Pazar yeri işlevi gören aracı hizmet sağlayıcı siteler, sıklıkla kendi içeriklerine de yer vermektedir. Dolayısıyla site tasnifinde her bir site için genelleme yapılmadan somut vakaya göre süjenin sıfatı belirlenmelidir. İçeriğini kendi sağlayan hizmet sağlayıcılar için hukuki sorumluluğun kime ait olduğu belirgin olsa da aracı hizmet sağlayan site işletmecileri için kusur sorumluluğu ya da sorumsuzluk hali devlete göre değişebilmektedir.⁸⁰⁰

Devletler, sosyal ağ sağlayıcıların belli özelliklerde olanlarına birtakım yükümlülük hükümleri ihdas etmektedir. Türkiye’de 5651 sayılı Kanun’a Sosyal Medya Yasası ile eklenen hükümde “*Türkiye’den günlük erişimi bir milyondan fazla olan yurtdışı kaynaklı sosyal ağ sağlayıcı*”⁸⁰¹ şeklinde bir niteleme yapılarak, bu niteliğe sahip site işletmecilerine; en az bir kişiyi Türkiye’de temsilci olarak belirleyip ilgili kuruma bildirme,⁸⁰² hukuka aykırı içerikler hakkında başvuruda bulunan kişilere 48 saat içinde gerekçeli olarak cevap verme,⁸⁰³ kanunda belirlenen hususları ilgili kuruma 6 aylık dönemlerle raporlama⁸⁰⁴ ve Türkiye’deki kullanıcıların verilerini Türkiye’de barındırma yönünde gerekli tedbirleri alma⁸⁰⁵ yükümlülükleri getirilmiştir.

AB Hukuku’nda DSA kapsamına, içerikle ilişkisi ancak aracılık düzeyinde olan hizmet sağlayıcılar alınmıştır. Zira hukuka aykırı içeriğin yayılmasının önlenmesi söz konusu olduğunda, sorumluluğu açık olan içerik sağlayıcı yerine pasif konumu sebebiyle sorumsuzluk ileri sürebilecek aracı nitelikteki Web sitesi işletmecisi için hükümler getirilmesi isabetli olacaktır.⁸⁰⁶ DSA’da aracı hizmet sağlayıcılara tanınan yükümlülükler kademeli şekilde tasarlanmıştır. Yer sağlayıcılar için öngörülenler ve aracı hizmetlere ilişkin genel hükümler dışında Web sitesi işletmecileri “çevrimiçi platformlar ve arama motorları”, “çevrimiçi pazar yerleri”, “çok büyük çevrimiçi platformlar (*very large online*

⁸⁰⁰ Türkiye, ABD ve AB yargı kararlarına dair örnekler için bkz. Öztekin, s.229-231.

⁸⁰¹ 5651 sayılı Kanun, Ek m.4/1.

⁸⁰² 5651 sayılı Kanun, Ek m.4/1.

⁸⁰³ 5651 sayılı Kanun, Ek m.4/3.

⁸⁰⁴ 5651 sayılı Kanun, Ek m.4/4.

⁸⁰⁵ 5651 sayılı Kanun, Ek m.4/6.

⁸⁰⁶ Päivi Korpisaari, “From Delfi to Sanchez – When Can an Online Communication Platform be Responsible for Third-Party Comments?: An Analysis of the Practice of the ECtHR and some Reflections on the Digital Services Act”, **The Journal of Media Law**, Vol.14, No.2, (2022), ss.372-373.

platforms) ve çok büyük arama motorları (very large online platforms)”⁸⁰⁷ şeklinde ayrılmıştır.⁸⁰⁸

Uygulamaya gelindiğinde, devletler adına yukarıda yer sağlayıcılar konusunda belirtilen yetki esasları ve güçlükler, Web sitesi işletmecileri için de geçerlidir. Devletler, sosyal ve iktisadi gücü çok yüksek olan Web sitelerinden trafik verisi paylaşımı ve içerik kaldırılması gibi taleplerine cevap alamamakta; söz konusu şirketlerin kahir ekseriyetinin ABD’de olmasından mütevellit bu devletle başlatılan uluslararası istinabe süreçleri de sık sık sonuçsuz kalmaktadır.⁸⁰⁹ AB’de dahi mahkemeler, polis ve veri koruma ajansları bir dönem aynı sorunları yaşarken artık AB’nin ve üye devletlerin düzenlemeci ve aktif politikalara geçişiyle ses getiren yargılamalar başlamıştır.⁸¹⁰ Özellikle rekabet hukuku davalarında çok yüksek meblağlarda tazminatlara hükmedilmektedir.⁸¹¹ Bununla birlikte dev şirketlerden taleplerine olumlu karşılık bulamadıkları durumlarda devletler, kamuoyunda doğacak olumsuzluklardan kaçınmak için yaptırımlarını tedricen uygulamakta; reklam yasakları, bant daraltma ve nihayet erişim engelleme gibi yollara başvurmaktadır.⁸¹² Sonuç olarak, salt aracı hizmet sağlayıcı konumunda olan Web sitelerinin dahi hukuka uygun işleyen bir siber uzay için etkin bildirim ve denetim mekanizmaları ile filtreleme önlemleri geliştirmeleri ve egemen devletlerle işbirliği içinde olmaları önem arz etmektedir. Gelgelelim internetin mevcut yapısında, hukuka

⁸⁰⁷ “Çok büyük” sıfatı için nitelikli unsur olarak AB dahilinde ayda 45 milyondan fazla aktif hizmet alıcısı olma şartı öngörülmüştür. Dijital Hizmetler Yasası, m.33/1.

⁸⁰⁸ Söz konusu tasnif, yükümlülükler ve sorumluluk rejimine dair detaylı bilgi için bkz. Işık, s.118 vd.; İpek Çevik, “Avrupa Birliği Dijital Hizmetler Yasası’nın Değerlendirmesi”, **Yıldırım Beyazıt Hukuk Dergisi**, Sayı.2, (2023), s.395 vd.

⁸⁰⁹ Bazı örnekler ve değerlendirmeler için bkz. Öztekin, ss.251-256.

⁸¹⁰ Daniel Lambach, “The Territorialization of Cyberspace”, **International Studies Review**, Vol.22, Iss.3, (2020), s.501.

⁸¹¹ AB’de son on yılda sadece Alphabet Inc. aleyhine, işlettiği Google sitesinin faaliyetleri sebebiyle görülen davalarda hükmedilen tazminat tutarı 8,25 milyar avroya ulaşmıştır; Foo Yun Chee ve Benoit Van Overstraeten, “Google’s \$2.7 Bln EU Antitrust Fine Should be Upheld, Court Adviser Says”, Reuters, 12.01.2024, <https://www.reuters.com/technology/eu-court-should-back-googles-27-bln-eu-antitrust-fine-court-adviser-says-2024-01-11/> (31.12.2024).

⁸¹² T.C. Ulaştırma ve Altyapı Bakanı Abdülkadir Uraloğlu’nun, eski adıyla Twitter olarak bilinen sosyal medya platformu X’in Türkiye’de temsilcilik açma sürecine ilişkin beyanattı bu bakımdan ilgi çekicidir. Uraloğlu, “X’i çok kez uyardık. Belli dönemde reklam yasakları koyduk ve Twitter’ı gerek şifahi görüşmelerde gerekse yazılı olarak daha üst perdeden uyardık. Bu uyarılar nispeten süreci biraz daha hızlandırma adına katkı sağladı” ve “bu reklam yasağından sonra da net bir şekilde bant daraltma uygulamasının başlayacağını bildirdik. Bunları Cumhurbaşkanımızın ve Kabinenin bilgisi dahilinde yaptık. Onun üzerine Twitter’ın biraz daha konunun hassasiyetini anladığını düşünüyoruz ki ona yönelik de nisan ayının sonuna doğru İstanbul’da bir şirket kurdular, resmi muhabatımız haline geldiler. Hem Türkiye’de vergi ödeme noktasında hem de doğrudan yaptırımlar uygulama noktasında ciddi bir kazanım elde etmiş olduk. Sabrederek doğru metotla sonuca ulaştık” ifadelerini kullanmıştır. Sürecin bu hassasiyetle yürütülmesini ise “yasakçı zihniyet” algısı oluşturmak istenmemesiyle gerekçelendirmiştir; TRT Haber, “Sosyal Medya Platformu X, Türkiye’de Temsilcilik Açtı”, 22.05.2024, <https://www.trthaber.com/haber/gundem/sosyal-medya-platformu-x-turkiyede-temsilcilik-acti-859255.html> (31.12.2024).

aykırı içeriğin ve siber suçların önüne mutlak olarak geçmek birçok önleme rağmen en azından bugün için imkansızla yakın durumdadır. Madalyonun Web sitesi işletmecilerine ve yer sağlayıcılara bakan diğer yüzünde ise hizmet sundukları çok sayıda devletin farklılıklar arz eden hukuk sistemine intibak etmelerindeki güçlük bulunmaktadır. Bu çatışmanın doğurduğu yetki tartışmalarına aşağıda hususen değinilecektir.

d. İçerik Sağlayıcı

İnternet bağlamında içerik, Şekil.3'te “D” harfi altındaki simgelerle temsil edilmiş olsa da hukuken oldukça kapsamlı bir ifadedir. 5651 sayılı Kanun'da tercih edilen “*internet ortamı üzerinden kullanıcılara sunulan her türlü bilgi veya veri...*”⁸¹³ tanımı da bunun bir göstergesidir. İçeriğin DSA'da “yasadışı içerik (*illegal content*)” başlığında “*...herhangi bir bilgi*”;⁸¹⁴ ABD'de telekomünikasyona dair federal yasaları kodifiye eden 47 U.S. Code hükümlerinde, “bilgi içeriği sağlayıcı (*information content provider*)” başlığında “*...internet veya diğer etkileşimli bilgisayar hizmetleri aracılığıyla sağlanan bilgi...*”;⁸¹⁵ Birleşik Krallık Çevrimiçi Güvenlik Yasası (*Online Safety Act*) hükümlerinde ise “*...bir internet hizmeti aracılığıyla iletilen herhangi bir şey...*”⁸¹⁶ şeklinde tanımlandığı görülmektedir. Dolayısıyla içeriği belli türlerle sınırlı sayıya tabi tutmak mümkün değildir. Dijital ortama taşınmış her veri, hukuken “içerik” kapsamındadır. “İçerik sağlayıcı” ise internet hukuku ile ilgili bir terimdir. 5651 sayılı Kanun'un yukarıda aktarılan hükmünün tamamında “*internet ortamı üzerinden kullanıcılara sunulan her türlü bilgi veya veriyi üreten, değiştiren ve sağlayan gerçek veya tüzel kişiler*” şeklinde ifade edilen tanım da bunu göstermektedir. Bilgi ve verinin üreticisi, bu kapsamda ancak bilgi ve veri internet ortamına sunulduğu takdirde içerik sağlayıcıya dair hükümlere tabi olacaktır. Ayrıca içerik sağlayıcılık günlük dilde bir meslek olarak dahi kabul ediliyor olsa da hukuk tekniğinde bu terim, kişi için sürekli bir unvanı değil; belirli bir içerik sağlama eylemi gerçekleştirildiğinde, sağlayan kişinin o içerik için kazandığı sıfatı karşılamaktadır. Yine de bu eylemi mutlak olarak yahut kâr amacıyla gerçekleştiren kişiler için ayrı bir alt kategori tanımlanarak özel düzenlemeler getirilmesi mümkündür.

⁸¹³ 5651 sayılı Kanun, m.2/1-f.

⁸¹⁴ Dijital Hizmetler Yasası, m.3/h.

⁸¹⁵ 47 U.S. Code, §230, <https://uscode.house.gov/view.xhtml?req=granuleid:USC-prelim-title47-section230&num=0&edition=prelim> (31.12.2024).

⁸¹⁶ Online Safety Act 2023, Chapter.50, Section.236/1, <https://www.legislation.gov.uk/ukpga/2023/50> (31.12.2024).

Gerçek ve tüzel kişilerin kendilerine ait siteler üzerinden içerik yayınlaması usulünün hâkim olduğu “Web 1.0” adlandırması yapılan işleyiş, gün geçtikçe aracı hizmet sağlayıcıların Web siteleri ve uygulamaları arasında etkileşim üstünlüğü yakaladığı bir süreçte değişime uğramıştır. İçerik sağlayan kullanıcıların karşılıklı etkileşimiyle şekillenen bu işleyiş için de “Web 2.0” yakıştırması kabul görmüştür. Günümüzde ise artık adem-i merkeziyetçi (*decentralized*), dağıtık, kişiye özel ve “sosyal ağ” yapısından “semantik ağ” yapısına dönmüş bir işleyişi ifade eden “Web 3.0” için bir geçiş sürecinde olduğu belirtilmektedir.⁸¹⁷ Ayrıca gelinen noktada içerikler artık botlar vasıtasıyla otomatikleştirilmiş sürçlerle üretilip internet erişimine açılabilir. Bu tür içeriklerin kişilere isnat edilmesi konusu, öğretideki tartışmalar ışığında aşağıda ayrı bir başlık altında değerlendirilecektir.

Yükleyen ve indiren teorisindeki yükleyene karşılık gelen içerik sağlayıcıların sorumluluğu için hukukta kabul görmüş genel ilke, 5651 sayılı Kanun’daki “*içerik sağlayıcı, internet ortamında kullanıma sunduğu her türlü içerikten sorumludur*”⁸¹⁸ hükmünde vücut bulmuştur. Bu ilke esasen hukuktaki en temel “süje – fiil – sorumluluk” ilişkisinin ifadesidir. Devletler, cari sorumluluk hukuku rejimlerine göre içerik sağlayıcıların hukuki ve cezai sorumluluklarına ilişkin özgün düzenlemeler yapabilirler.

Hukuka aykırı içerikler için uygulamadaki esas sorunlar ise kimlik gizleme yöntemleri kullanan içerik sağlayıcıların tespiti ve yabancı uyruklu içerik sağlayıcılar üzerinde yetki icrasıdır. Diğer taraftan -yer sağlayıcılar ve Web sitesi işletmecilerinde de olduğu gibi- internet erişimine içerik sunan bir içerik sağlayıcının, eylemlerinin ülkelerinde içeriğe erişilebilen bütün devletlerin hukukuna uygunluğunu denetlemesinde güçlük ve hatta imkânsızlık söz konusudur. Bu sorunların çözümü için uluslararası iş birliği zorunlu olduğu gibi bütün internet sükelerinin belli ölçüde katkıda bulunması da gereklidir. Misal X Devleti, aracı hizmeti veren yabancı bir Web sitesindeki isimsiz hesaptan yapılan hukuka aykırı paylaşımın failini tespit etmek için öncelikle Web sitesi işletmecisine başvurarak, paylaşım yapan kişinin IP adresini ve hesap bilgilerini talep etmelidir. Söz konusu kayıtlar Web sitesi işletmecisine hizmet veren bir yer sağlayıcısının

⁸¹⁷ Web için kabul edilen bu versiyon yapıları ve konu hakkında bilgi için bkz. Hatipoğlu Aydın, ss.19-26.

⁸¹⁸ 5651 sayılı Kanun, m.4/1.

sunucusunda olabileceği gibi doğrudan işletmeciyeye ait sunucularda da tutulabilir. Web sitesi işletmecisi bu talebi reddettiği takdirde X Devleti için ilgili işletmecinin tabi olduğu devletten talepte bulunmak, elindeki istihbarat verilerini değerlendirmek ve açık kaynak araştırması yapmaktan başka hukuki yol kalmamaktadır. Web sitesi işletmecisi talebe olumlu karşılık verdiğinde ise X Devleti’nde hizmet veren İSS aracılığıyla IP adresi üzerinden kullanıcının kimlik bilgilerine erişilebilecektir.⁸¹⁹ Ayrıca Web sitesi işletmecisi talebe karşılık verse dahi içerik sağlayıcının sanal özel ağ (*virtual private network* (VPN)) veya vekil (*proxy*) sunucu kullanmak suretiyle IP adresini ilgili Web sitesine ulaşana dek manipüle ederek kimliğini gizlemesi mümkündür. Bu tür durumlarda fail şayet bir VPN yahut vekil sunucu hizmet sağlayıcısından faydalandıysa bu hizmet sağlayıcıya başvurularak ilgili trafik verileri talep edilebilir. Böylece tekrar bir talep-cevap süreci oluşacaktır. TOR (*The Onion Router*) gibi ağ yapıları üzerinden gerçekleştirilen erişimlerde ise kullanıcı ve sunucu arasında çok sayıda düğüm (*node*) bulunduğundan, ileri teknolojik yeterliliğe sahip olmayan devletlerin kullanıcıya erişmesi imkansıza yakın hale gelmektedir.⁸²⁰ Failin alışveriş merkezi, otel, internet kafe, okul, belediye gibi toplu internet kullanımı sağlayan yerlerden istifade etmiş olması durumunda “toplu kullanım sağlayıcı” olarak kabul edilen bu yerlerin, failin tespiti için uygun önlemleri (güvenlik kamerası, erişimlerin kütük (*log*) kayıtlarının tutulması, kimlik doğrulama yöntemleri vb.) almış olma yükümlülükleri söz konusudur.⁸²¹ Bazı durumlarda ise Web siteleri, kullanıcıların IP adreslerinin yanı sıra Web tarayıcısı (*browser*) vasıtasıyla cihazlara ilişkin elde ettiği donanım ve yazılım bilgilerini kullanarak, bağlantı sağlayan cihazların parmak izini (*device fingerprint*) oluşturabilir. Bu şekilde oluşturulan cihaz parmak izi üzerinden de haliyle kullanıcı bilgilerine erişilebilmektedir.⁸²² Çocuk istismarı gibi ciddi

⁸¹⁹ Türkiye’de yaygın olduğu üzere abonelerine IPv4 sistemiyle IP adresi sunan İSS’ler, abone sayısı ellerindeki adres sayısının çok üzerinde olduğu için dinamik IP usulünü uygulamaktadır. Bu durumda kullanıcıya tahsis edilen IPv4 tabanlı adresler zaman içinde değişkenlik göstermektedir. Ayrıca ağ adres değişimi (*network address translation*) yönteminin İSS’ler tarafından kullanılan türü olan taşıyıcı sınıf (*carrier-grade*) NAT (CGNAT) ile bir IP adresi birden fazla kullanıcıya tahsis edilerek hizmet sunulmaktadır. Bu durumda kimlik tespiti için sadece IP adres bilgisi yeterli olmayacak, beraberinde kullanıcının port bilgileri ve erişim anına dair zaman damgası da gerekecektir. İSS’ler bunları kayıt altında tuttuğu için failin kimliğini ilgili otoriteye bildirebilmektedir. CGNAT sistemi işleyişi hakkında bilgi için bkz. IETF, “Common Requirements for Carrier-Grade NATs (CGNs)”, RFC 6888, 2013, <https://datatracker.ietf.org/doc/html/rfc6888> (31.12.2024).

⁸²⁰ TOR ağının işleyişine dair bkz. Merve Varol Arısoy ve Ecir Uğur Küçüksille, “TOR Gizli Servis Tarayıcılarının Performans Karşılaştırması”, *Bilecik Şeyh Edebali Üniversitesi Fen Bilimleri Dergisi*, Cilt.6, Sayı.2, (2019), ss.149-151.

⁸²¹ 5651 sayılı Kanun, m.7; İnternet Toplu Kullanım Sağlayıcıları Hakkında Yönetmelik, m.4, m.5 ve m.9, R. G., 11.04.2017, Sayı.30035.

⁸²² Peter Eckersley, “How Unique Is Your Web Browser?”, Mikhail J. Atallah ve Nicholas J. Hopper (Ed.), *Privacy Enhancing Technologies* içinde (1-18), Berlin, Heidelberg, New York: Springer, 2010, ss.1-5.

vakalarda ise bazı Web siteleri, bu süreçlerle hiç gerek bırakmadan proaktif hareket ederek failin bulunduğu devlete ihbarda bulunabilmektedir. Görüldüğü üzere zaman zaman karmaşık bir hal alabilen fail tespit süreci çok kez sonuçsuz kalabildiği gibi, tespit edilen failin yabancı ya da yurt dışında olması durumunda da uluslararası hukukta süregelen yetki tespit ve icra sorunlarıyla karşı karşıya kalınmaktadır.

e. Kullanıcı

Şekil.3'te "E" ile belirtilen konumdaki "kullanıcı" için ayrı bir tanımlayıcı hüküm içermese de 5651 sayılı Kanun'da erişim sağlayıcı için yapılan tanımdaki *"kullanıcılarına internet ortamına erişim olanağı sağlayan..."* ifadesi, dolaylı olarak kullanıcıyı da tanımlamaktadır. Kullanıcı, internete "erişen" kişidir. 5809 sayılı Elektronik Haberleşme Kanunu'nda⁸²³ ise doğrudan *"aboneliği olup olmamasına bakılmaksızın elektronik haberleşme hizmetlerinden yararlanan gerçek veya tüzel kişi"* şeklinde tanımlanmıştır.⁸²⁴ Yukarıda bahsedildiği üzere uygulamada kullanıcılar, İSS'ler aracılığıyla internete erişebilmektedir. Bu erişim de bir abonelik sözleşmesine dayalı olarak gerçekleşmektedir. Fakat toplu kullanım sağlayıcılardan yararlanılması veya bir şekilde kaçak erişim sağlanması gibi ihtimallerden anlaşılabileceği üzere kullanıcının abone vasfını taşıma şartı bulunmamaktadır.

Kullanıcının kurucu eyleminin "internet'e erişmek" olduğu söylenebilir. Hukukun kullanıcıya dair ilgi alanına giren kısmında ise bir içeriğe "erişilmesi", içeriğin "indirilmesi" ve "depolanması" gibi eylemler bulunmaktadır. Devletler, bu eylemleri ayrı ayrı hukuki sonuçlara tabi tutabilir. Örnek olarak TCK m.226'da düzenlenen müstehcenlik suçunun tespitinde Yargıtay içtihadı aşağıdaki gibi şekillenmiştir:⁸²⁵

"Aynı şekilde, müstehcen görüntülerin, internet ortamından ya da başka bir yolla (örneğin başka bir şahıstan temin edilen video dosyasının flash bellek aracılığıyla bilgisayara atılması), seyretmek amacıyla indirip-yükledikten sonra silinmesi ile de suç oluşmayacaktır. Zira silinen bu verilerin ancak özel yazılımlar aracılığıyla geri getirilmesi mümkün olup yine depolama veya bulundurma kastı yoktur. Ancak, failde önceden depolama veya bulundurma iradesinin bulunup bulunmadığı kastının ortaya çıkarılması açısından, görüntülerin temin edildikten sonra ne kadar süre tutulduğu, görüntülerin sayısı, silinen veriler için ayrı bir

⁸²³ R. G., 10.11.2008, Sayı.27050.

⁸²⁴ Elektronik Haberleşme Kanunu, m.3/1-cc.

⁸²⁵ Yargıtay 18. Ceza Dairesi, E.2018/5669, K.2019/10900, 19.06.2019.

tasnifleme yapıp yapılmadığı (örneğin özel isimler verilen klasörlerde tutma gibi), daha profesyonel kullanıcılar açısından, silinen verileri geri getirip tekrar tekrar kullanmak amacıyla sistemde özel bir yazılım bulundurulup bulundurulmadığı gibi hususların teknik olarak incelenip araştırılması gereklidir.”

İçerikte herhangi bir değişikliğe sebep olmaksızın -ki bu durumda içerik sağlayıcı kategorisine girilecektir- “erişmek” fiilinin hukuka aykırı olduğu istisnai durumların örnekleri, Budapeşte Sözleşmesi’nde düzenlenen “yasadışı erişim”⁸²⁶ ve “yasadışı araya girme”⁸²⁷ fiilleridir. Sözleşme hükümlerinin TCK’daki yansıması, “bilgi sistemine girme” suçu olmuştur. Eylemin faili de “bir bilgi sisteminin bütününe veya bir kısmına, hukuka aykırı olarak giren veya orada kalmaya devam eden kimse” olarak düzenlenmiştir.⁸²⁸ Ayrıca “bir bilgi sisteminin kendi içinde veya bilgi sistemleri arasında gerçekleşen veri nakillerini, sisteme girmeksizin teknik araçlarla hukuka aykırı olarak izleyen kişi” için de yaptırım öngörülmüştür.⁸²⁹

Erişmek fiilinin, içeriğin hukuka aykırı niteliği dolayısıyla suç teşkil ettiği ulusal hukuk düzenlemelerine de rastlanabilmektedir. Birleşik Krallık’ta “terör eylemi gerçekleştiren veya hazırlayan bir kişi için yararlı olabilecek türden bilgileri” içeren “belge ve kayda internet üzerinden erişilmesi” suç olarak düzenlenmiştir. Bu suçla itham edilen kişinin, fiili için makul bir mazereti olduğunu kanıtlaması gerekmektedir.⁸³⁰ Avustralya’da çocuk istismarı içeren materyallere erişmek için bir hizmet kullanmak suç olarak düzenlenmiştir.⁸³¹ Türkiye’de de benzer nitelikteki fiillerin, “ısrar”⁸³² gibi unsurlar eklenerek hukuki belirlilik ve öngörülebilirlik ilkelerine uygun şekilde düzenlenmesinin isabetli olacağı kanaatindeyim.

Bu noktaya kadar anlaşılabileceği üzere Web’de kullanıcı sıfatının taşınmasında dikkat edilecek husus, Web’in mevcut durumunda doğrudan değişiklik yapılmamasıdır. Web’de bulunan herhangi bir içeriğe bağlantı sağlandığı anda erişim gerçekleşir.

⁸²⁶ Budapeşte Sözleşmesi, m.2.

⁸²⁷ Budapeşte Sözleşmesi, m.3.

⁸²⁸ TCK, m.243/1.

⁸²⁹ TCK, m.243/4.

⁸³⁰ Terrorism Act 2000, Chapter.11, Section.58/1, <https://www.legislation.gov.uk/ukpga/2000/11/section/58> (31.12.2024).

⁸³¹ Criminal Code Act 1995, Section.474.22, https://www5.austlii.edu.au/au/legis/cth/consol_act/cca1995115/sch1.html (31.12.2024).

⁸³² TCK m.123/A’da düzenlenen “ısrarlı takip” suçundaki ısrar unsuru, bu bağlamda uygun bir örnektir.

Sonrasında içeriğin türüne göre erişimin sürdürülmesi, içerikteki değişikliklerin takip edilmesi, kayıt altında alınması ve indirilmesine dek kullanıcı eylemleri çeşitlenir. İndirme eylemiyle birlikte, kullanıcı çevrimdışı duruma geçse dahi içeriği fiziksel olarak elinde bulunduruyor olacağı için, indirilmiş içeriklerin fiziksel belleklerde depolanması ve dağıtımı gibi eylemler, bir internet süjesini ifade eden haliyle “kullanıcı” eylemi sayılmayacaktır.

Devletlerin kullanıcılar üzerindeki yetki tespiti ve icrası temelde uyruklu ve ülkesellik esasına göre gerçekleşmektedir. Ayrıca bilgisayar korsanlığı gibi yetkisiz erişim kaynaklı hukuka aykırı eylemlerin milli güvenliği tehdit edecek boyutlara ulaştığı durumlarda devletler koruma ilkesine dayanarak fail üzerinde yetki ileri sürebilecektir. Failin kimlik tespitine ve yetkinin icrasına dair sorun ve süreçler ise yukarıda içerik sağlayıcı başlığında bahsedilenlerle ortaktır.

3. Ülke Dışındaki Yabancı Süjeler Üzerinde Yetki Tespiti ve İcrasına İlişkin Teorik Zemin

Siber uzayın süjelerine sağladığı imkânlarla egemen devletler sisteminin yüzleşmesi, yukarıda *Brierly* ile *Goldsmith* ve *Wu*’dan aktarılan sorunların kaynağıdır. Egemen devlet, egemenlik alanına giren bütün olguların kendi normlarına uygun olmasını isteyecek ve bunu sağlamak için gerekli önlemleri alacaktır. Egemenlik alanının tespiti için ise yer, kişi ve konu bakımından bir kapsam çerçevesi çizilmelidir. Kişi bakımından kapsamın gri bölgesinin temel unsuru, başta yukarıda tanımlanan internet süjeleri olmak üzere siber uzayda eylemde bulunan bütün süjelerin ülke dışında bulunan yabancı uyruklu olanlarıdır. Yabancıların eylemleri ilgili devletin ülkesinde gerçekleştiği takdirde gri bölgeden çıkılmaktadır. Fakat ülke dışındaki yabancıların eylemleri, bu bağlam dahilinde uluslararası hukuktaki teorik tartışmanın esas konusunu teşkil etmektedir. Böyle durumlarda yetki kullanımı için vaka ile devlet arasında gerçek bir bağlantının varlığı aranacaktır.

a. Pasif Vatandaşlık İlkesi

Ülke dışındaki yabancıların eylemlerinden bahsedildiğinde, devletin vatandaşına yönelik bir zararın meydana gelmesi, yetki tespitinin nispeten kolay olduğu bir durum

olarak görülebilir. Failin kimliğinin tespitindeki ve ele geçirilmek suretiyle fiilen yargılanmasındaki zorluklar uygulamada sürüyor olsa da doğrudan bir vatandaşın hukuki menfaatine zarar verildiğinin tespiti genellikle sarıh bir süreç ile gerçekleşir. Bu ilkenin uygulanmasındaki uluslararası kabul, diğer devletin egemenliğinin ve hukuk düzeninin haksız şekilde ihlal edilmemesine ve hakkında yetki ileri sürülen eylemin hukuka aykırılığının yabancı fail tarafından bilinmesinin makul ölçüde beklenebilir olmasına bağlıdır.⁸³³ Haliyle bu makuliyet ölçüsü de süjenin türüne ve niteliklerine bağlı olarak değişecektir. Sözelimi X Devleti'ndeki bir X Devleti vatandaşının Y Devleti'ndeki Y Devleti vatandaşına hitaben sağladığı bir sosyal medya içeriğinde, fail tarafından öngörülmesini beklemenin makul olmayacağı şekilde Y Devleti hukukuna göre vatandaşın hukuki menfaatine zarar verdiği kabul edilen bir ifade bulunabilir. Diğer yandan, dünya çapında hizmet veren bir sosyal medya platformunun işletmecisi olan çokuluslu bir şirket söz konusu olduğunda ise hizmet verdiği devletlerin hukukuna uygun davranma noktasındaki beklentinin makuliyet sınırları çok daha geniş değerlendirilecektir. Süje tipinin yanı sıra, ileri sürülen hukuka aykırılığın dayandırıldığı ulusal hukuk normunun niteliğine ilişkin bir örnek olarak; bir devletin, vatandaşlarının fotoğraflarının yurtdışındaki yabancılar tarafından sosyal medyada paylaşılmasını yasaklayan bir düzenleme getirerek pasif vatandaşlık ilkesine dayanmasının haklı görülemeyeceği, Tallin El Kitabı'nda belirtilmiştir. Zira bunun hem mantıksız hem diğer devletin ifade özgürlüğüne dair iç politikasına haksız bir müdahale olduğu kanaati iletilmiştir.⁸³⁴

b. Objektif Ülkesellik İlkesi ve Etki Doktrinleri

Devletlerin, ülkeleri dışında gerçekleşen eylemler hakkında pasif vatandaşlık ilkesinden bağımsız olarak yetki ileri sürebilmesi, bu eylemlerden bir şekilde etkilenmeleri durumunda mümkün olacaktır. Eylemin koruma ilkesine başvurulabilir derecede milli menfaatlere zarar verici olması veya evrensellik ilkesi kapsamına giren bir suç teşkil etmesi gibi oldukça istisnai haller dışında, yetki için temel dayanak yine ülkesellikte bulunacaktır. Ancak bu noktada sadece eylemin gerçekleştiği ülke değil, sınır aşan sonucun gerçekleştiği ülke için de objektif ülkesellik ilkesinden bahsedilecektir.

⁸³³ Tallin El Kitabı, s.65.

⁸³⁴ Ibid, s.61.

Siber uzayın dış uzay, açık denizler veya Antarktika gibi devlet egemenliğine istisna teşkil ettiği kabulü üzerinden; yetkinin ülkesel değil, milliyete bağlı olarak kişisel zemin üzerinde tesis edilebileceğini ileri süren uluslararası alanlar teorisi,⁸³⁵ günümüzde geçerliliğini yitirmiş görünmektedir. Siber uzayın tamamı üzerinde herhangi bir devletin egemenliğinden pek tabii bahsedilemiyor olsa da ülkesellik, siber uzayda yetki kullanımının en temel ilkelerinden biri haline gelmiştir.

Siber uzay bağlamındaki eylemler, bilhassa internet vasıtasıyla ve Web üzerinden gerçekleşenler, genellikle dünyadaki neredeyse bütün ülkelerde sonuç doğurmaktadır. Söz konusu sonuç, erişilebilirliktir. Yahoo! Davası'nda görüldüğü gibi, bir içeriğin ülke içinde sadece erişilebilir olması dahi devletlerce müdahale edilmesi gereken bir durum olarak görülebilmektedir. Benzer nitelikteki Perrin Davası'nda; Birleşik Krallık mahkemesinin, Fransa vatandaşı olan Stephane Laurent Perrin'i, ABD merkezli bir Web sitesi işletmecisi şirket tarafından işletilen siteye sağladığı müstehcen içerik sebebiyle cezaya çarptırmasına gerekçe olarak, içeriğe Londra'daki bir polis karakolundan erişilmiş olması gösterilmiştir.⁸³⁶ Bu bakımdan, içerik sağlayıcılara ve kullanıcılara yönelik ceza yargılamalarında olduğu kadar Web sitesi işletmecilerine ve yer sağlayıcılara yönelik hukuki girişimlerde de objektif ülkeselliğe dayalı devlet yetkisinin sınırları tartışmalara konu olmuştur. Nitekim Web'de sınır tanımayan bir içerik üzerinde bütün devletlerin aynı oranda ilgisi söz konusu olabilecektir. Objektif ülkesellik ise özgün bir ilgi gerektirmektedir.⁸³⁷

Bir devlete ait siber altyapıya yahut devlet ülkesindeki özel sunuculara yönelik saldırılar gibi hukuka aykırı eylemler söz konusu olduğunda, yargı yetkisi için objektif ülkesellik ilkesine dayanılabileceği açıktır. Fakat sanal ortamda gerçekleşen içerik sağlama gibi eylemler için erişilebilirlik dışındaki somut sonuçların yokluğu hatta erişilebilirlik söz konusu olmasa dahi ülkede olumsuz etki doğurabilecek fiiller için siber imkânların genişlemesi gibi sebepler; konu hakkındaki literatürü, objektif ülkesellik ilkesi üzerinde yükselen “etki doktrini” esaslarına başvurmaya yöneltmiştir. Yargıya ilk

⁸³⁵ Menthe, s.83.

⁸³⁶ Perrin v. The United Kingdom, **Decision**, European Court of Human Rights, No.5446/03, 18.10.2005.

⁸³⁷ Menthe, s.80.

yansıması ABD’de 1945 tarihli Alcoa Davası’nda⁸³⁸ görülen doktrin, bu davaya benzer şekilde rekabet hukukuna ilişkin 1949 tarihli Akkor Lamba (*Incandescent Lamp*) Patent Davası⁸³⁹ ile 1958 tarihli İsviçreli Saatçiler (*Swiss Watchmakers*) Davası⁸⁴⁰ gibi dava kararlarında tartışmalara da sebep olarak uygulanmaya devam etmiştir. Bu kararlarda, fiil ABD ülkesi dışındaki yabancılar tarafından işleniyor olsa da ABD’deki ticareti etkilediği için fiilin etkisinin ülke içinde meydana geldiği ve dolayısıyla ABD mahkemelerinin failler üzerinde yargı yetkisine sahip olduğu kabul edilmiştir.⁸⁴¹ Zira ABD perspektifinden bu yaklaşım, esasen ülkesel yargı yetkisinin bir örneğidir.⁸⁴²

Devam eden yıllarda Atlantik’in diğer yakasındaki Avrupa Toplulukları Adalet Divanı’nda görülen Kâğıt Hamuru (*Wood Pulp*) Davası’nda; topluluk dışındaki ülkelerde bulunan şirketlerin kartel oluşturan faaliyetlerinden ötürü, Avrupa Ekonomik Topluluğu’nu kuran Roma Antlaşması m.35 hükmüne göre Komisyon tarafından cezalandırılmaları hukuka uygun görülmüştür.⁸⁴³ Gelgelelim o vakte kadar etki doktrinine dayanarak Avrupalı şirketlere karşı geniş yetki kullanan ABD’ye duyulan tepki sebebiyle, kararda bu doktrinin tanınması konusunda çekimser davranılmıştır.⁸⁴⁴ Bunun yerine, kartel oluşturma fiilinin dışında, kartel sonucunda ortaya çıkan fiyat politikasının Topluluk üyesi devletlerin ülkelerinde uygulanması (*implementation*), hukuka aykırılık ve yargı yetkisi için kurucu unsur olarak kabul edilmiştir. Böylece esasen uluslararası hukukta yerleşik nitelikteki ülkesellik ilkesine dayanıldığı ileri sürülmüştür. *Lange* ve *Sandage* da bu düşünceyi, yetki için bir çeşit “ülke benzeri (*quasi-territorial*)” zemin kurgulamak olarak değerlendirecektir.⁸⁴⁵ Objektif ülkesellik ilkesi ile etki doktrini

⁸³⁸ United States v. Aluminum Company of America, U.S. Court of Appeals for the Second Circuit, 148 F.2d 416, 12.03.1945.

⁸³⁹ United States v. General Electric Company, U.S. District Court for the District of New Jersey, 82 F. Supp. 753, 04.04.1949.

⁸⁴⁰ United States v. Watchmakers of Switzerland Information Center, U.S. District Court for the Southern District of New York, 25 F.R.D. 203, 3 Fed. R. Serv. 2d 648, 02.03.1960.

⁸⁴¹ Ağah Kürşat Karauz ve Halil Alperen Işık, “Rekabet Kurallarının Yer Bakımından Uygulanması”, **Yıldırım Beyazıt Hukuk Dergisi**, Sayı.1, (2016), ss.293-294; Najeeb Samie, “The Doctrine of "Effects" and the Extraterritorial Application of Antitrust Laws”, **University of Miami Inter-American Law Review**, Vol.14, Iss.1, (1982), s.27 vd.

⁸⁴² Don Wallace Jr., “Extraterritorial Jurisdiction”, **Law and Policy in International Business**, Vol.15, No.4, (1983), s.1102.

⁸⁴³ Evan Breibart, “The Wood Pulp Case: The Application of European Economic Community Competition Law to Foreign Based Undertakings”, **Georgia Journal of International and Comparative Law**, Vol.19, No.1, (1989), s.165.

⁸⁴⁴ Muhammad Rifky Wicaksono ve Diğerleri, “Implementing the Extraterritoriality Principle to Strengthen Competition Law Enforcement in Indonesia in the Aec Era: A Comparative Study”, **Indonesia Law Review**, Vol.9, No.1, (2019), s.39.

⁸⁴⁵ Dieter G.F Lange ve John Byron Sandage, “The Wood Pulp Decision and Its Implications for the Scope of EC Competition Law”, **Common Market Law Review**, Vol.26, Iss.2, (1989), s.157.

arasında konumlandığı söylenebilecek bu yaklaşımın, uygulanma unsurunun yokluğunda dahi ortaya çıkabilecek olumsuz etkilerin bertaraf edilmesi için etki doktrininin devletlere sunduğu imkanları kısıtlamış görünmektedir.⁸⁴⁶

Etki doktrinin doğuşundan yıllar sonra, 2017’de AB Adalet Divanı (ABAD), Intel Davası’nda⁸⁴⁷ önemli bir karara imza atmıştır. Dava, ABD merkezli çip üreticisi Intel ile bu çiplerin kullanımına müsait bilgisayar donanımlarının Çin merkezli üreticisi Lenovo şirketleri arasındaki anlaşmaların, Intel’in rakibi konumunda olan yine ABD merkezli AMD şirketini işlemci pazarında engellemek amacıyla gerçekleştiği; bu şekilde de piyasadaki hâkim konumun kötüye kullanıldığı iddiasıyla AB Komisyonu tarafından Intel şirketine yaptırım uygulanmasını konu edinmiştir. İlgili şirketler AB dışındadır. Ayrıca AB dışında üretilen ve satılan çipler, AB dışında üretilen bilgisayarlara monte edilecektir. Bu durumda velev ki rekabete aykırılık olsa dahi AB makamlarının yetki ileri sürebilmesi için “uygulanma” unsurunun ötesinde bir gerekçe bulunmalıdır. Sadece etki oluşmasına bağlı yargı yetkisini kabul etmek ise devletlere diğer devletlerin egemenlik haklarını ihlal edecek derecede geniş bir alan açmaktadır. Bu noktada ABAD, AB’de oluşacak etkinin “öngörülebilir, doğrudan ve esaslı” olması şartını aramış, bunu da “nitelikli etki (*qualified effect*) olarak tanımlamıştır.⁸⁴⁸ Divan’a göre işlemler tamamen AB dışında gerçekleşse bile AB pazarında oluşturacağı haksız rekabet etkisi; öngörülebilir, doğrudan ve esaslı niteliktedir. Etki değerlendirmesi yapılırken de fiillerin unsurlarının ayrı ayrı değerlendirilmesi yerine, holistik bir yaklaşımla, davranışın bütün olarak ele alınması gerektiği ifade edilmiştir.⁸⁴⁹ Sonuç olarak; ülke dışındaki yabancıların fiilleri, doğrudan bir stratejik planın parçası olarak gerçekleştiği takdirde, bu stratejinin ülke içinde etki doğurmaya yönelik olması, devletin failler üzerinde yetki ileri sürmesine haklı bir gerekçe sağlayacaktır.

Intel Davası’nın sonuçlandığı senenin başında 2.0 versiyonu yayımlanan Tallin El Kitabı’nda, devletlerin ülkelerinde “esaslı etki” doğuran siber aktiviteler için “ülkesel

⁸⁴⁶ Wicaksono ve Diğerleri, ss.40-41.

⁸⁴⁷ Intel Corp. v European Commission, Judgment of the Court (Grand Chamber), Case C-413/14 P., 06.09.2017, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:62014CJ0413> (31.12.2024).

⁸⁴⁸ Intel Corp. v European Commission, para.18.

⁸⁴⁹ Intel Corp. v European Commission, para.50 ve para.56.

yetki” öngörölmüştür.⁸⁵⁰ Devamında, aşırı yetki oluşmaması adına birtakım kriterler aranıyor olsa da etki doktrininin uluslararası örf ve âdet hukukunu yansıttığının söylenebileceği de ileri sürölmüştür.⁸⁵¹ Ayrıca bu dayanağın, ölkedışı yetki doğuran koruma ilkesinden veya objektif ve subjektif ölkesellik ilkelerinden ayrı düşünölmesi gerektiği belirtilmiştir.⁸⁵² Tallin El Kitabı’nda etki doktrinine başvurulabilmesi için aranacak kriterler şu şekilde sayılmıştır: Devlet adına “açık ve uluslararası kabul edilebilir bir menfaatin” varlığı; düzenlenecek etkinin yeterince “doğrudan” ve “amaçlanmış veya öngörülebilir” olması; oluşan etkinin devletin ölkedışında yetki kullanmasını haklı çıkaracak ölçüde “esaslı” olması ve yetki kullanımının diğer devletler ile yabancı uyrukluların menfaatlerini gereksiz yere ihlal etmemesi.⁸⁵³

Yukarıdaki gelişmelerden anlaşılacağı üzere “etki doktrini” zaman içinde en azından belli kriterler aranacak şekilde geliştirilmiş ve “nitelikli etki doktrini” haline dönüşmüştür. Mevcut durumda, varlığı ileri sürölen etkinin “öngörülebilir, doğrudan ve esaslı” nitelikte olup olmadığı her somut olay için ayrı değerlendirilmelidir. Sözgelimi bir Web sitesinin faaliyetlerinden bahsedildiğinde, sitede sunulan dil seçenekleri arasında bir devletin resmi dilinin bulunması, ilgili devletin TLD uzantısıyla hizmet vermesi, sitenin amacı, içerik politikası, hedef kitlesi, trafik hacmi gibi çok sayıda faktör bu etki değerlendirmesi kapsamında ele alınmalıdır. Böylece bir içeriğin bir ölkede sadece erişilebilir olmasının, içerik sağlayıcı üzerinde ilgili devlete yargı yetkisi tanınması adına yeterli olmayacağı artık kabul görmüştür. Fakat doktrinin uygulanmasında yoruma açık kısımların fazlalığının, devletlerin yetkilerini geniş şekilde ileri sürmelerine imkân sağlayacağı da bir gerçektir.

c. Seçici Uyum Doktrini ve Mevcut Sisteme Yönelik Eleştiriler

Uluslararası hukukta cari yetki sistemine yönelik dikkate değer eleştirel teorilerden biri olan, *Svantesson*’a ait seçici uyum doktrininden bahsetmekte fayda olduğu kanaatindeyim. Devletin yetkisine dair geleneksel tasnifi reddederek herhangi bir yetki iddiasının makullüğü ve meşruluğunun, başka bir devletin egemenliğine müdahale

⁸⁵⁰ Tallin El Kitabı, s.55.

⁸⁵¹ Ibid., ss.57-58.

⁸⁵² Ibid., s.59.

⁸⁵³ Ibid., s.58.

etme derecesine göre değerlendirilebileceğini görüşü üzerinden hareket eden yazar, mevcut yetki türlerinin yanında “soruşturma yetkisi” ve “iyileştirici (*remedial*) yetki” kavramlarını önermiştir.⁸⁵⁴ Yazarın bu girişiminin genel sebebi, mevcut yetki sistematığının siber uzayın gerçekleriyle uyumlu olmadığını düşünmesidir.⁸⁵⁵ Zira siber uzayda ülkesellik için dayanak bulmak her zaman için çok kolaydır ve fiziksel uzaydaki ülke sınırları belirgin şekilde muhatabını “dur işareti” ile uyarırken siber uzayda bu şekilde bir ülkeselleşme düşünölemeyecektir.⁸⁵⁶

Svantesson’un ileri sürdüğü bir ayrım da “havlama yetkisi (*bark jurisdiction*)” ve “ısıрма yetkisi (*bite jurisdiction*)” şeklindedir. Bazı yetki iddialarının pratikte gerçekleşme imkânı olmadığı bilinmesine rağmen ileri sürölüyor olmasını havlamaya benzeten yazar; iddia edilen hukuki doğruya dair bir pozisyon göstermesi ve muhataplarına aktif müdahale edemese dahi onları yönlendirici etkisinin olması gibi özellikleri sebebiyle havlama yetkisinin de hukuken muteber ve faydalı olduğunu kabul etmiştir.⁸⁵⁷ Bu yaklaşımın kodlarına, yazarın da atıfta bulunduğı *Hart*’ın düşüncesinde rastlanmaktadır. *Hart*, hukukun temel amacının insan davranışına yönelik kılavuzlar ve eleştiri standartları getirmek olduğunu; hukuka tabi söljelerin davranışlarının buna uygun gerçekleşmediğı durumları düzenleyen ikincil kuralların işlevinin de ancak ikincil olduğunu ve bu sebeple hukukun hedef ve amacının “cebir kullanımı” olarak kabulünün yanlış olacağını savunmuştur.⁸⁵⁸

Hukuk felsefesinin başlıca tartışmalarından olan hedef ve amaç konusunda *Svantesson*’un savunduğı pozisyon, ileri süreceğı seçici yetki doktrinine düşünsel zemin sağlamak amaçlıdır. Yazar, internet aracıları (*internet intermediaries*) olarak tanımladığı ve yer yer İSS üst kümesi altında “aracı hizmet sağlayıcı” olarak da anıldığı görölen Web sitesi işletmecileri için ayrıcalıklı bir statü öngörmüştür. Mutlak ifade özgürlüğü terk edildiğı anda aracılar için altından kalkılması güç denetim ve sansür yükümlölükleri doğacağına dikkat çeken yazar, internetin yapısı itibariyle aracılarn radyo/televizyon

⁸⁵⁴ Svantesson, s.6.

⁸⁵⁵ Ibid., ss.3-5.

⁸⁵⁶ Ibid., s.225.

⁸⁵⁷ Ibid., ss.133-134.

⁸⁵⁸ Herbert Lionel Adolphus Hart, *The Concept of Law*, Third Edition, Oxford: Oxford University Press, 2012, s. 249.

yayıncılarından ve gazetelerden çok farklı bir konumda olduğunu ileri sürmüştür.⁸⁵⁹ Siber uzay hukuk teorisinin bitmeyen özgürlükçü – düzenlemeci tartışmasındaki temel sorunu da “çoğu insan, internet araçlarının kendi ülkelerinin kanunlarına uymasını beklerken; muhtemelen internet araçlarının dünyadaki diğer tüm ülkelerin kanunlarına uymasını istemeyecektir” sözleriyle özetlemiştir.⁸⁶⁰ Burada kastedilenin, Goldsmith ve Wu’nun aktardığı Avrupa fikrasındakiyle aynı olduğu görülebilmektedir.

Küresel çapta faaliyet gösteren bir internet aracısının, erişilebilir olduğu bütün ülkelerin hukuk kurallarını bilmesi ve bu kurallara uyması gerçekten de ağır bir yükür. Hatta böyle bir külfetin üstesinden yalnızca çok büyük girişimlerin gelebileceğı düşünülürse, kolayca küresel erişime sahip olunabilen Web ortamındaki küçük şirketler için haksız rekabet oluşacağı da görülebilecektir.⁸⁶¹ Aşırı düzenleme çağında internet araçlarının korunması gerektiğı iddiasıyla Svantesson’un önerdiği çözüm; küresel çapta faaliyet gösteren araçların, hangi devlette sürekli, sistematik ve esaslı şekilde -fiziksel ya da sanal fark etmeksizin- varlık göstermek istiyorsa o devletin hukukuna uymayı seçtiğinin kabul edilmesidir.⁸⁶² Ayrıca yetki ileri süreceğ devletın de konu ile esaslı bağlantısının (*substantial connection*) olması, yetki kullanımında meşru menfaatinin (*legitimate interest*) bulunması ve diğer sşjelerle menfaat dengesinin gözetilmesi (*interest balancing*) şartlarını sağlaması gereklidir.⁸⁶³

Svantesson, teklifinin provokatif ve tartışmaya açık olduğunun farkındadır. Nitekim araçların erişilebilir oldukları ve hizmet verdikleri fakat “sürekli, sistematik ve esaslı” varlık gösterme amacı taşımadıkları ülkelerin kanunlarına uyup uymama konusunda belirleyecekleri politikaları ve bunun sonuçları üzerine kesin bir duruş gösterememiştir. Yine de siber özgürlükçü yazarların uluslararası hukukun mevcut yetki sistemine yönelik eleştirilerinde haklı oldukları birçok nokta olduğunun kabul edilmesi

⁸⁵⁹ Svantesson, ss.215-216.

⁸⁶⁰ Ibid., s.216.

⁸⁶¹ Ibid., s.217.

⁸⁶² Ibid., s.220.

⁸⁶³ Ibid., s.61.

gerektiği kanaatindeyim. İstisnacıların son kuvvetli isyancısı sayılabilecek *Post, Kohl*'dan yukarıda aktarılan sorulara benzer bir dizi soru sıralamıştır.⁸⁶⁴

“Ponzi şemaları dolandırıcılık mıdır, yoksa sadece ‘oyunun bir parçası’ mıdır? Tacirler iflas edebilir mi? Nasıl? Burada kumara izin veriliyor mu? Bir mülkü satışa sunduğumda bildiğim kusurlarını açıklamam gerekir mi? Nazi hatıra ürünlerini satabilir miyim? Çıplak insanların resimlerini göstermek? Ünlülerin resimleri? Başka birinin elbisesinin tasarımını veya başka birinin binasının özelliklerini kopyalayabilir miyim?”

Devlet egemenliği çok keskin şekilde ele alındığında, siber uzayda eylemde bulunacak kişiler her bir ülke için bu tür sorulara daima cevap aramak durumunda kalabilirler. Diğer taraftan devletler de ülke dışındaki yabancılar üzerinde yetki icra etmekte genellikle zorlanacağı için ya kanunlarının birtakım ihlallerine göz yumacak ya da bütün dünyaya yayılmış internet sükeleriyle amansız bir kovalamacaya girişecektir. Zira uluslararası hukukun -siber uzaydan bağımsız olarak- mevcut halinde, faili elinde bulundurmayan ve faile ait taşınmaz, banka hesabı vb. unsurlara da hâkim olmayan bir devletin iade ve istinabe talep etmekten; talebine olumsuz karşılık aldığı anda ise failin bir şekilde “ağına düşmesini” beklemekten başka çaresi yoktur. *Post*, bu durumu çekiçle köstebek vurma oyununa benzetmiştir.⁸⁶⁵ Eleştirileri oldukça kuvvetli olsa da nihayetinde gelen çözüm önerisi, yazarın kendisinin de “çılıncı” görüldüğünü kabul ettiği fakat öyle olduğunu düşünmediği, kendi kendini yöneten topluluklara (*self-governing communities*) alan açılarak internet topluluklarının kendi hukukunu kendi üretmesi olmuştur.⁸⁶⁶

Modern devletler sisteminde devletlerin egemen olma vasfı korunduğu müddetçe yetki icrasında çıkmazların yaşanması, gri bölgelerin oluşması, köstebek vurma oyunun sürmesi kaçınılmazdır. Ortaya çıkan sorunlar, bir vakıa olan “egemen devletler” sisteminden kaynaklanan sorunlardır. Sistemin mevcut yapısı içerisinde kalarak bulunabilen en güncel çözümün de nitelikli etki doktrini olduğu görülmektedir. Eleştirel çözüm önerileri ise genellikle devlet egemenliğinin kabulü üzerinden üretilseler dahi devletlerin egemenlikleri gereği kabul etmelerine imkân olmayan türdendir. Yetki

⁸⁶⁴ David G. Post, “Governing Cyberspace: Law”, *Santa Clara High Technology Law Journal*, Vol.24, Iss.4, (2008), s.911.

⁸⁶⁵ Ibid.

⁸⁶⁶ Ibid., s.912.

hakkında mevcut belirsiz çerçevenin, uluslararası hukukun gelecekteki gidişatında daha somut esaslarla belirginleşeceği; bunun da ancak uluslararası iş birliği ile mümkün olabileceği; aksi halde siber uzayda fragmantasyon yaşanarak devletlerin tek tek yahut kamplar halinde dijital kapıları birbirine büyük ölçüde kapatması gibi bir ihtimalin de varlığını devam ettirdiği kanaatindeyim. Öyle ki egemen vasıfları gereği devletler, aşikâr sorunlara ortak çözüm arayışından sonuç alamadıklarında çoğu zaman saldırganlaşmak veya içe kapanmak gibi eğilimlere yönelebilmektedir.

4. Otonom Araçların Eylemlerinde ve Yapay Zekâ Sistemleri Tarafından Üretilen İçeriklerde İsnat Sorunu

Otonom araçlar ve yapay zekâ, son yıllarda sosyal hayatta büyük ses getirdiği gibi birçok disiplinle beraber hukukun da en popüler çalışma konularından biri haline gelmiştir. Teknolojinin gelişim sürecinde önce tamamen fiziksel ve kimyasal mekanizmaların çalıştırılmasıyla işleyen makineler, daha sonra elektronik işlemcilerin desteğiyle mantıksal süreçleri fiziksel eylemlere dönüştürmeye başlamıştır. Berim işlevli donanımların ve çalıştırdıkları yazılımların kapasitesinin artması ile gerek mantıksal sonuçların gerek bu sonuçların dönüştürüldüğü fiziksel eylemlerin öngörülebilirliği azalmıştır. Önceleri kural tabanlı gerçekleşen işlemler, insanın bilişsel fonksiyonlarını taklit etmeyi amaçlayan yapay zekâ algoritmalarının gelişimi sonucunda çok daha sofistike bir hal almıştır. Bu sebeple yapay zekâyâ düşünme, analiz etme, seçenekleri ve riskleri değerlendirme, karar verme, konuşma ve tasarım yapma gibi özellikler atfedilmektedir. Konu hakkındaki en güncel düzenleme olan AIA'da yapılan tanım da bu doğrultudadır:⁸⁶⁷

“‘YZ sistemi’, çeşitli otonomi seviyelerinde çalışmak üzere tasarlanmış ve konuşlandırıldıktan sonra uyarlanabilirlik gösteren; aldığı girdiden, açık veya örtük hedefler için, fiziksel veya sanal ortamları etkileyebilecek tahminler, içerik, tavsiyeler veya kararlar gibi çıktıların nasıl üretilceğinin çıkarımını yapan makine tabanlı bir sistem anlamına gelir.”

⁸⁶⁷ Yapay Zekâ Yasası, m.3/1.

UNESCO bünyesindeki Yapay Zekâ Etiği Hakkında Genişletilmiş Çalışma Grubu tarafından 2019’da sunulan çalışmada ise tanım yapmaktan kaçınılarak AIA’daki ile benzer doğrultuda bir çerçeve çizilmiştir.⁸⁶⁸

“YZ’nin tek bir tanımı olmamakla birlikte tartışmalar; algılama, öğrenme, muhakeme, problem çözme, dil etkileşimi ve hatta yaratıcı işler üretme gibi özellikler de dahil olmak üzere insan zekâsının belirli işlevlerini taklit edebilen makinelerle odaklanma eğilimindedir.”

“Otonom araç” kavramı ise literatürde sıklıkla taşıtlar için kullanılmaktadır. Türkiye’de yürürlükte olan Motorlu Araçlar ve Römorkları ile Bunlar İçin Tasarlanan Aksam, Sistem ve Ayrı Teknik Ünitelerin Genel Güvenliği ve Korunmasız Karayolu Kullanıcılarının ve Yolcuların Korunması ile İlgili Tip Onayı Yönetmeliği’ndeki tanım da bu duruma örnektir.⁸⁶⁹

“Otonom araç: Sürücünün devamlı kontrolü olmadan, ancak sürücü müdahalesinin yine de beklendiği veya gerekli olduğu, belirli bir süre için otonom olarak hareket etmek üzere tasarlanmış ve imal edilmiş motorlu aracı,”

Bu anlamdaki kullanımların, düzenlenmesi amaçlanan konuya göre sınırlandırılmış tanımları yansıttığı açıktır. Oysa en genel şekilde otonom aracın; “belirli bir operasyonel bağlamda, doğrudan gerçek kişi müdahalesi olmadan, önceden tanımlanmamış senaryolarda dahi üretim amacına belli düzeylerde uygun hareket etme kabiliyetine sahip her tür araç” olarak tanımlanması mümkündür. Bu kabiliyet için de sensörler, işlemciler, çevre elemanları gibi donanımlar, geniş veri tabanları ve verileri işleyen yapay zekâ yazılımları kullanılmaktadır. Taşıt, silah, insansız hava aracı, ev aleti vs. formlarda görülebilen ilgili araçlar aynı zamanda “robot” kategorisindedir.⁸⁷⁰

Çalışma prensipleri, türleri, modelleri, kabiliyetleri, etkinlik sahaları vs. çok geniş çeşit yelpazesine sahip olan söz konusu unsurlara dair detaylar, başlı başına kapsamlı bir literatürün konusudur. Eldeki çalışmanın bu bölümü için esas ehemmiyet arz eden nokta ise bu unsurların eylemlerini ifade eden sanal ve fiziksel çıktıların hangi süjeye isnat edileceğidir. Yapay zekâ sistemlerinin ve otonom araçların özellikleri insanlar için o

⁸⁶⁸ UNESCO/Executive Board, “Preliminary Study on the Technical and Legal Aspects Relating to the Desirability of a Standard-Setting Instrument on the Ethics of Artificial Intelligence”, **206 EX/42**, 21.03.2019, s.1.

⁸⁶⁹ R. G., 14.05.2020, Sayı.31127, m.3/1-t.

⁸⁷⁰ Raci Çetin Yüksekbaş, **Otonom Araçların Haksız Fiil Sorumluluğu**, Ankara: Seçkin Yayıncılık, 2024, s.41.

kadar etkileyicidir ki sıklıkla antropomorfizme konu edilmektedir. Nitekim insanların teknolojiyle teması arttıkça ve kontrol edilebilirlik ile öngörülebilirlik düştükçe antropomorfizme başvurma oranının arttığını gösteren çalışmalar literatürde mevcuttur.⁸⁷¹ Algılama, öğrenme, muhakeme etme, karar verme, eyleme geçme gibi kabiliyetler cansız varlıklara atfedildiğinde, otonom aracın gerçekleştirdiği hareketin failinin yine bizzat otonom araç olduğunun kabulü de mümkün olacaktır. Benzer şekilde bir yapay zekâ sisteminin çıktısı olan metin veya medya içeriğinin “sağlayıcısının” da bizzat yapay zekâ olduğu söylenebilecektir. Antropomorfizmin son noktasında ise söz konusu unsurların irade sahibi olduğu dile getirilecektir.⁸⁷² Hayvanların statüsü için dahi tartışmaların sürdüğü⁸⁷³ modern hukuk literatürü göz önüne alınıp, meseleye realist cepheden bakıldığında ise; otonom araçlar ile yapay zekâ sistemlerinin cansız varlık olduklarından bahisle birer eşya ve araç niteliğinde oldukları, nihayetinde de onlara irade ve fiil isnadında bulunulamayacağı savunulabilecektir. Fakat “otonomi” söz konusu olduğunda ortaya çıkan sonuç ile hukukun mevcut kişileri arasındaki mesafe açıldığı için fiillerin kişilere isnat edilmesinde güçlük doğacaktır. Yine de insanlığın kontrol dışı hareket kabiliyetine sahip varlıklarla ilk kez karşılaşmış olmadığı kesindir. Misal sahipli hayvanlar, kıyasa uygun bir seçenek olarak değerlendirilebilir. Ayrıca köleleri insanların malvarlığına eşya (*res*) sıfatıyla dahil edip, malvarlığı içerisindeki diğer unsurlardan da kişi (*persona*) vasfıyla ayrı bir konuma koyan Roma Hukuku’nda dahi bu sorunun izleri görülebilmüş; yapay zekâ ile işleyen makinelerin hukuki statüsü için Roma’daki köle hukuku ile kıyasa başvurulması da mümkün olmuştur.⁸⁷⁴ Fakat bilinen tarihte, insan yapısı olup kontrol dışı hareket edebilen cansız varlıklarla sadece modern dönemde karşılaşıldığı gerçeğini ve sorunun bu bakımdan özgün niteliğini de kabul etmek gerekir.

Yukarıda arz edilenler ışığında, sonuç olarak; siber uzayda hukuk inşa edilirken realizm ve metaforik yaklaşım arasında nerede konumlanmak gerektiği sorunundaki belirsizliğin, şimdilik bu konuda da geçerli olduğu kanaatindeyim. Gelgelelim hukukun

⁸⁷¹ Adam Waytz ve Diğerleri, “Making Sense by Making Sentient: Effectance Motivation Increases Anthropomorphism”, *Journal of Personality and Social Psychology*, Vol.99, No.3, (2010), ss.423-425.

⁸⁷² Christophe Leroux ve Roberto Labruto (Ed.), *Suggestion for a Green Paper on Legal Issues in Robotics*, The European Robotics Coordination Action, Grant Agreement Number: 248552, 2012, s.12.

⁸⁷³ Konu hakkında inceleme için bkz. Cengiz Koçhisarlıoğlu ve Özlem Söğütü Erişgin, “Hayvanların Hukuki Konumu”, *Yaşar Üniversitesi E-Dergisi*, Cilt.8, Sayı.Özel, (2013), s.1691 vd.

⁸⁷⁴ Özgür Taşdemir, Ümit Vefa Özbay ve Burhanettin Onur Kireçtepe, “Robotların Hukuki ve Cezai Sorumluluğu Üzerine Bir Deneme”, *Ankara Üniversitesi Hukuk Fakültesi Dergisi*, Cilt.69, Sayı.2, (2020), ss.808-809.

ilgilendiği asıl hususun, sözgelimi “içerik sağlayıcı” sıfatına kimin/neyin sahip olacağından ziyade hukuka aykırılık durumunda kimin “sorumlu” sıfatını alacağı sorusu olduğu da bir gerçektir.⁸⁷⁵ Hukuk literatüründe de söz konusu mesele genellikle ve tabii olarak “sorumluluk” başlığı altında ele alınmıştır. Üzerinde yoğun akademik çalışmaların yürütüldüğü bu bahsin detaylarına, kapsam sınırlarını muhafaza etmek adına eldeki çalışmada girilmeyecektir. Hukuka aykırılıktan doğan sorumluluk ancak gerçek veya tüzel kişiler içindir. Devletlerin ilgili hususta tercih edecekleri hukuki rejime göre, sorumluluk isnat edilecek kişiler değişebilecektir.⁸⁷⁶ Devletler, ulusal hukuklarında bu tür düzenlemeleri yapma yetkisine sahiptir. Uluslararası hukuk normları da devletlerin pozisyonlarına bağlı olarak zamanla şekillenecektir. Ulusal düzenlemelerin icrasına dair esas ve süreçler için de bu bölümde yukarıda bahsedilen ilgili mekanizmalar aynen geçerli olacaktır.

C. Siber Uzayın Mantıksal Boyutu ve Veri Unsuru Üzerinde Devletin Yetkisi

Ülke ve vatandaşlık bağı, siber uzayın fiziksel boyutu ve kişi unsuru üzerindeki devlet yetkisi adına tüm tartışmalara rağmen kuvvetli dayanak noktaları oluştursa da mantıksal boyut ve veri unsuru için bu zemin daha gevşek yapıdadır. Fiziksel varlıklar ile gerçek ve tüzel kişilerin, devletle fiziksel uzaydaki ilişkileri asırlardır sürmektedir. Siber uzayı yeni ve farklı kılan, dolayısıyla devlet egemenliği hakkında yeni sorular doğuran esas cephe ise klasik tanımlardaki sanal gerçekliğin kaynağı olan mantıksal boyut ve dijital formdaki veridir. Buna binaen eldeki çalışmada aynı başlık altında işlenmelerinin sebebi olan ortak yönleri, fiziksel formda bulunmaksızın kodlardan ve mantıksal örgülerden müteşekkil fakat donanım ve arayüzler vasıtasıyla somut olarak algılanabilir ve anlamlandırılabilir olmalarıdır. Hal böyleyken devlet yetkisinin tespit ve icrası da mantıksal boyut ve verinin, kişiler ve ülkelerle ilişkilendirilmesi yoluyla

⁸⁷⁵ Öztekin, s.353.

⁸⁷⁶ Unsurların türüne göre son kullanıcı konumundaki tüketiciler, sistemleri üreten üreticiler, Web üzerindeki içerikler söz konusu olduğunda Web sitesi işletmecileri veya yer sağlayıcılar, otonom silah sistemleri için devletler gibi süjelere kusur sorumluluğu veya kusursuz sorumluluk esaslarına göre sorumluluk yüklenebilecektir. Türk hukuk doktrininde konu hakkında ileri sürülen görüşlerden bazı örnekler için bkz. Ibid., ss.354-355.

sağlanabilecektir. Temel ilişki noktalarının belirlenmesi ve hukuka konu edilmesi ile en azından bir çerçeve çizilmesi mümkün olacaktır.

Siber uzayda fiziksel ve mantıksal boyut arasındaki etkileşimin en kök noktasında, belli standarttaki elektrik akımının varlığı ve yokluğu (dijital sinyal) üzerinden işleyen ikili (*binary*) sistem bulunmaktadır. Günlük hayatta kullanılan onluk sisteme benzer şekilde ikili sistem ile bütün sayıların temsil edilmesi mümkündür. Daha sonrasında harfler, renkler, ses frekansları gibi unsurlar, belirlenen standartlar çerçevesinde sayılarla temsil edilir. Sonuçta, dijital (sayısal) ifadesinin kullanım sebebi olarak; mantıksal boyuttaki her bir “şey”, temelde sayıdan ibarettir. Bu çok temel mekanizmaya burada değinilmesindeki amaç, siber uzayın bir boyutu olan mantıksal boyutun ve bir unsuru olan dijital verinin, kökünde “birler ve sıfırlardan” oluştuğunu hatırlatmaktır. Lakin insan, temas ettiği olguları, algıladığı biçimde değerlendirir ve kategorize eder. Sözelimi ekran vasıtasıyla resim olarak gözlemlenen şeyin esasen bir sayı bütünü olması, hukuk gibi sosyal bilim dallarında dikkate alınmaz. Günümüzde bilgi teknolojileri alanında dahi çalışmacıların çok büyük çoğunluğu söz konusu sayılarla ilgilenmemektedir. Disiplin, birikerek ilerlemiş, sayıların organizasyonunu sağlayan standart, protokol ve programlar uygulamada yerleştikçe sayı seviyesinden büyük oranda soyutlanmış, gelişmeler de yerleşik sistemler üzerinden sürdürülmüştür.

Ham ya da işlenmiş, yapısal ya da yapısal olmayan dijital formdaki veri üzerinde yapılacak bütün işlemler, mantıksal boyutta olgunlaşmış sistemler marifetiyle gerçekleşmektedir. Geniş bir kapsam ve tanım skalası barındıran veri ile bilgi kavramlarının Birinci Bölüm’de açıklanan siber uzaya münhasır çerçevesi göz önüne alındığında; dijital formdaki verinin hukuka konu edilmesinin, formundan bağımsız şekilde insan tarafından anlamlandırılmasıyla kazandığı hususiyetlere bağlı olduğu görülecektir.⁸⁷⁷ Bunun yanı sıra verinin formundan ileri gelen girilmesi, depolanması, işlenmesi, dağıtılması gibi süreçler de devletlerin yetki alanına girmektedir. Mantıksal boyutun esas işlev ve ehemmiyetiyse bu noktada belirlemektedir. Nihayet veri, eşleştiği

⁸⁷⁷ Verinin böylece ortaya çıkan en önemli ayırt edici özelliği ise zuhur potansiyelini taşıdığı bilgi itibarıyla fiziksel uzayda daima bir izdüşüme sahip olmasıdır. Sık kullanılan basit bir örnek olarak; esasen fiziksel uzaydaki veri veya bilginin siber uzaya aktarılmasını ifade eden “veri girişi” tabiri dahi verinin insan eliyle fiziksel boyut ve mantıksal boyut arasındaki geçişkenliğinin bir göstergesidir.

süjeler ve ortaya çıktığı, üretildiği ya da depolama donanımları vasıtasıyla fiziken bulunduğu yerler üzerinden devletle ilişkilendirilebilmektedir. Mantıksal boyutun izafesi ise kullanılan dijital araçların üreticileri, sahipleri, kullanıcıları ve işletilen süreçlerin failleri ile sonuç doğurduğu ülkeler üzerinden gerçekleşmektedir. Devlet yetkisinden bahsedilebilecek belli başlı ilişkilendirme sahaları, aşağıda bu düsturla incelenecektir.

1. Fikri Mülkiyet

Arka planında tartışmalı bir felsefi müktesebata sahip olan fikri mülkiyet, hukukun en özgül alanlarından biridir. Siber uzayın yapı itibarıyla vadettikleri, klasik dönemin siber özgürlükçüleri arasında, fikri mülkiyetin siber uzayda ortadan kalkabileceği düşüncesini kuvvetlendirmiştir. Ancak zaman, devlet düzenlemeleri lehine işlemiş; fikri mülkiyet, siber uzayda hukukun başat sahalarından biri olmuştur. Bilgisayar programları, yazılımlar,⁸⁷⁸ alan adları, video oyunları,⁸⁷⁹ dijital tasarımlar gibi unsurlar, fikri mülkiyet hakları üzerinden gerçek ve tüzel kişilerle eşleşmektedir. Kurulan hukuki ilişki de doğal olarak devletin yetki konusu haline gelmektedir. Sibere uzaya özgü unsurlar dışında film, müzik, video, kitap gibi fiziksel uzay unsurlarının dijital haldeki dosyaları da internetin sağladığı imkanlar ile fikri mülkiyet ihlallerine konu olabilmektedir.

Lessig, fikri mülkiyet tartışmasını merkeze alarak; Web'in doğuşundan sonraki on yıl içerisinde internet devriminin, fikri mülkiyetin neredeyse hiç olmadığı bir sistem ile gerçekleştiğini fakat geline nokta hukukun yoğun müdahalesiyle ihdas edilen korumaların, siber uzayın doğasına aykırı olduğunu ve siber uzayı öldürdüğünü

⁸⁷⁸ Bilgisayar programı ve yazılımın anlamdaş olduğu iddialarının mevcudiyetine karşın yazılımın daha geniş kapsamlı bir terimi ifade etmesine ve hukuki korumanın buna göre değişiklik göstereceğine dair tespitler için bkz. Sırma Korkut Emrağ, “Bilgisayar Programlarının Fikri Mülkiyet Hukuku Kapsamında Korunması”, (Yüksek Lisans Tezi, İstanbul Bilgi Üniversitesi, Lisansüstü Programlar Enstitüsü, 2024), s.9-12.

⁸⁷⁹ Dijital formdaki oyun programlarının, donanımlarla görüntüye dönüştürülmesi suretiyle çok çeşitli platformlar üzerinden, farklı etkileşim biçimleriyle oynanabilmesi; ortak özellikleri olan “video” ismiyle anılmalarına sebep olmuştur. Çalıştıkları platformlara göre bilgisayar oyunu (*computer/pc game*), konsol oyunu (*console game*), mobil oyun (*mobile game*), sanal gerçeklik oyunu (*virtual reality game*) gibi alt dallara ayrılan video oyunları, ticari ve sosyal hayatın doğurduğu geleneklerden kaynaklı farklılıklara sahip olsa da hukuken tek çatı altında değerlendirilebilirler. Bilgisayar programlarından farklı olarak, kod yapısı haricinde oyunun görsel sunumu içerisinde algılanan karakter, tasarım vs. unsurlar da fikri mülkiyet koruması altındadır; Emin Çelik, “Mobil Oyunların Fikri Mülkiyet Hukukunda Korunması”, *Anadolu Üniversitesi Hukuk Fakültesi Dergisi*, Cilt.9, Sayı.1, (2023), s.148.

savunmuştur.⁸⁸⁰ Yazara göre internet büyüyüp gelişerek var olmaya devam edecektir. Fakat başta yazılım olmak üzere ürünlerin üretimi, artan telif korumaları sebebiyle yine güçlü şirketlerin ve kurumsal yapıların münhasır alanında kalma riski altındadır. Zira açık kaynak kullananların ve bağımsız üreticilerin mevcut şartlarda oluşacak hukuki ve mali yükü karşılamaları oldukça güç olacaktır. Bu da internet öncesi dünyaya dönüş demektir.⁸⁸¹ Sonuçta ise *Thomas Jefferson*'un "paylaşmakla tükenmeyeceği" gerekçesiyle fikri, mülkiyete konu etmeme idealinin gerçekleşmesine dair ümitler yeniden ortadan kalkacaktır.⁸⁸²

Lessig, Post, Stallman,⁸⁸³ *Doctorow*,⁸⁸⁴ *Elbakyan*⁸⁸⁵ gibi yazar ve aktivistlerin; EFF, FSF,⁸⁸⁶ Creative Commons,⁸⁸⁷ The Pirate Bay,⁸⁸⁸ gibi çok sayıda topluluk ve Web platformu ile çeşitli ülkelerde faaliyet gösteren siyasi korsan partilerin⁸⁸⁹ çabalarına

⁸⁸⁰ Lessig, 2000, ss.342-347; *Lessig*'e göre siber uzay, fikri mülkiyetin reddi öncül kabul edilerek doğmuştur. Hırsızların hapse atıldığı fiziksel uzayın aksine siber uzay, fikrin ve yaratıcılığın korunup saklanmak yerine dağıtılmasıyla refah üretilen bir yerdir. *Post* da bu noktaya işaret edip siber uzayda herhangi bir fikri mülkiyet koruması yokken ortaya çıkan ürünleri örnek vererek; kolektif yaratıcılığın harekete geçmesi için telif haklarından doğan teşviklere ihtiyaç gerekseydi internetin bugün çorak bir araziden ibaret kalacağını ileri sürmüştür; *Post*, 2009, ss.203-204.

⁸⁸¹ *Ibid.*, s.346.

⁸⁸² *Ibid.*, s.347; ayrıca yukarıda bkz. dipnot.469.

⁸⁸³ 1985'te Özgür Yazılım Vakfı'nı (*Free Software Foundation* (FSF)) kuran Richard Stallman'ın konu hakkındaki görüşlerini içeren eser için bkz. Joshua Gay (ed.), **Free Software, Free Society: Selected Essays of Richard M. Stallman**, Boston: GNU Press, 2002.

⁸⁸⁴ Bir dönem EFF Avrupa Direktörlüğü de yapan, Birleşik Krallık Açık Haklar Grubu (*UK Open Rights Group*) kurucularından bilimkurgu yazarı *Cory Doctorow*, mevcut telif sisteminin gereğinden fazla koruma sağladığı görüşünü ileri sürdükten sonra yaklaşımını "Eğer bu telif hakkı vizyonu ve daha fazla insanın yaratabildiği, daha fazla kitleye hizmet verilebildiği, cihazlarımızın dürüst hizmetkarlarımız olduğu ve bize ihanet etmediği, ağılarımızın sansür ve gözetim için tasarlanmadığı bir dünya arasında seçim yapmak durumundaysak, ben ikincisini seçiyorum. Umarım siz de öyle yaparsınız" sözleriyle özetlemiştir; *Cory Doctorow, Information Doesn't Want to Be Free: Laws for the Internet Age*, San Francisco: McSweeney's, 2015, s.154.

⁸⁸⁵ Bilimde devrim yapma çabasında olduğunu ifade eden, bilginin özel mülkiyete konu olamayacağı iddiasıyla akademik yayınların serbest dolaşımını savunan *Alexandra Elbakyan*, bu amaçla Sci-Hub isimli Web sitesini kurmuştur; *Alexandra Elbakyan ve Aras Bozkurt, "A Critical Conversation with Alexandra Elbakyan: Is she the Pirate Queen, Robin Hood, a Scholarly Activist, or a Butterfly Flapping its Wings?"*, **Asian Journal of Distance Education**, Vol.16, Iss.1, (2021), ss.112-113.

⁸⁸⁶ Free Software Foundation, "About", <https://www.fsf.org/about> (31.12.2024).

⁸⁸⁷ Creative Commons, "Who We are", <https://creativecommons.org/mission/> (31.12.2024).

⁸⁸⁸ The Pirate Bay topluluğu, mevcut fikri mülkiyet rejimlerine karşı politik hareketin merkezi olarak görülmüştür; *Jessica Lucia Beyer, Expect Us: Online Communities and Political Mobilization*, New York: Oxford University Press, 2014, s.65. Bir P2P dosya paylaşım protokolü olan Torrent'in dünyadaki en popüler izleyicilerinden birini kuran topluluğun söz konusu Web sitesi için bkz. <https://thepiratebay.org> (31.12.2024); Türkiye'de faaliyet gösteren İSS'lerden TTNet, söz konusu Web sitesine erişim engeline ilişkin mahkeme kararı olmamasına rağmen DNS hizmetinde kara liste uygulamak suretiyle erişim taleplerine yanıt vermemektedir.

⁸⁸⁹ İlk örneği The Pirate Bay kurucularının ülkesi İsveç'te görülen fikri mülkiyet karşıtı siyasi partiler, özellikle Avrupa'da yaygınlaşmıştır; Mehmet Tayyib Gül, "Siyasal Yaşamda Yeni Bir Oluşum: Korsan Parti ve İsveç Korsan Partisi Örneği", **Anadolu Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi**, Cilt.24, Sayı.4, (2023), ss.532-533.

rağmen;⁸⁹⁰ siber uzayda fikri mülkiyet hukuku ve denetim enstrümanları gün geçtikçe gelişmiş, ihlallerle mücadele kuvvetlenmiştir.

Siber uzayın erken dönemindeki hukuki tartışmaların fikri mülkiyet üzerinden başlaması, menşe ülkenin ABD olduğu düşünülürse pek şaşırtıcı değildir. 1989’da Apple şirketinin Hewlett-Packard ve Microsoft şirketlerine karşı agresif şekilde telif davaları açma yönünde yürüttüğü politikasını protesto etmek amacıyla, kendisine “*NuPrometheus League*” adını veren kişi veya kişilerce Apple şirketine ait Macintosh kaynak kodlarının bir kısmı dışarı sızdırılıp dağıtılmıştır.⁸⁹¹ Bir dönem ürettiği bilgisayarların kullanımını yaygınlaştırmak adına yazılımların disketlerle paylaşılmasını teşvik eden Apple, bu kez yaşanan olaya karşı yasal yollara başvuracağını ve çalınan kodları edinen veya dağıtan kişilerin de federal yasalara göre suçlu sayılması gerektiğini ileri sürmüştür.⁸⁹² Bilgisayar programlarının hukuk nezdinde donanımdan ayrı şekilde ele alınması; 1969’da ABD Adalet Bakanlığı’nın IBM şirketi aleyhine rekabet hukukuna aykırılık iddiasıyla mahkemeye başvurması ve yargı sürecinin ancak 1982’de IBM ile ABD arasında imzalanan anlaşma ile nihayete ermesinin önemli sonuçlarından biridir.⁸⁹³ Yazılım ve donanım arasındaki sıkı ilişkinin rekabet hukukundaki modern örneği ise 2018’de AB Komisyonu’nun Google ve dolayısıyla ana şirket Alphabet’e, Android işletim sistemi bulunduran cihaz üreticilerine uyguladığı yazılım bazlı kısıtlamalar sebebiyle 4,34 milyar avro tutarında para cezası vermesidir.⁸⁹⁴

Devletler, ulusal hukuk düzenlemelerindeki fikri mülkiyet hükümlerini siber uzaya genişletmişlerdir. ABD’de 1998’de kabul edilen Dijital Binyıl Telif Hakkı Yasası (*Digital Millennium Copyright Act (DMCA)*), bu alandaki en meşhur ulusal düzenlemedir. Bu yasa ile WIPO antlaşmalarındaki hükümler ABD hukukunda yürür hale getirilmiş; kullanıcı eylemlerinden kaynaklı fikri mülkiyet ihlallerinde hizmet

⁸⁹⁰ Siber uzayda mevcut fikri mülkiyet rejimine karşı fikri ve sosyal sürece dair inceleme için bkz. Hatipoğlu Aydın, ss.282-290.

⁸⁹¹ Branscomb, 1991, s.155; Bruce Sterling, *The Hacker Crackdown: Law and Disorder on the Electronic Frontier*, New York, Toronto: Bantam Books, 1992, s.232.

⁸⁹² Branscomb, 1991, s.155.

⁸⁹³ Onur Şahin, *Telif Hakları Bakımından Bilgisayar Programları: Araişlerlik Serbestisi ile Özgür ve Açık Kaynak Kodlu Programlar*, On İki Levha Yayıncılık, 2021, s.46; U.S. Justice Department vs International Business Machines Corporation, US Court of Appeals for the Second Circuit, 687 F.2d 591, 13.08.1982.

⁸⁹⁴ European Commission, “Antitrust: Commission fines Google €4.34 Billion for Illegal Practices Regarding Android Mobile Devices to Strengthen Dominance of Google's Search Engine”, 18.07.2018. https://ec.europa.eu/commission/presscorner/detail/en/IP_18_4581 (31.12.2024).

sağlayıcıların sorumlulukları belli koşullarla sınırlandırılmış; programlar, sinema filmleri, ses kayıtları gibi dijital eserlerin türlerine göre fikri mülkiyet rejimleri tesis edilmiştir.⁸⁹⁵ Türkiye’de ise fikri mülkiyet rejimini dijital ortama tahsisen düzenleyen bir kanun bulunmamaktadır. Genel fikri mülkiyet rejimini düzenleyen 5846 sayılı Fikir ve Sanat Eserleri Kanunu (FSEK),⁸⁹⁶ siber uzaya kıyasen uygulanmaktadır. Ayrıca 4110 sayılı “5846 Sayılı Fikir ve Sanat Eserleri Kanununun Bazı Maddelerinin Değiştirilmesine İlişkin Kanun”⁸⁹⁷ ile “bilgisayar programları” FSEK kapsamına dahil edilmiştir. Böylece bilgisayar programlarının hazırlık tasarımı, kontrol akışı (*control flow*), kaynak kodu (*source code*) ve nesne kodu (*object code*) fikri mülkiyet bakımından koruma altına alınmıştır. Programların kullandığı algoritmalar ve genel kullanıcı arayüzleri ise kapsam dışında bırakılmıştır.⁸⁹⁸ Zira algoritmalar, özünde matematiksel yöntemlerdir. Kullanıcı arayüzlerinde ise belirli tasarım ve işlevler için koruma öngörülebilse de yapı elemanları olan menü düzeni, düğme tasarımı gibi unsurlar için kural olarak fikri mülkiyetten bahsedilemeyecektir. Türk hukukunda bilgisayar programları için telif koruması söz konusuysa 5769 sayılı Sınai Mülkiyet Kanunu hükmüne göre patente uygun görülmemiştir. Ancak kanunda öngörülen şartları taşıyan ve teknik yönü olan “yazılımların” patent korumasından yararlanabileceği belirtilmiştir.⁸⁹⁹

Uluslararası hukukta fikri mülkiyet oldukça köklü bir düzenleme alanıdır. 1886 tarihli Edebiyat ve Sanat Eserlerinin Korunmasına İlişkin Bern Sözleşmesi (*Berne Convention for the Protection of Literary and Artistic Works*), yıllar içinde geçirdiği değişikliklerle günümüzde dahi yürürlüğünü sürdürmektedir.⁹⁰⁰ Bern Sözleşmesi’nde, siber uzayın doğuşundan sonraki süreçte bu konuda bir değişiklik yapılmadığından doğrudan dijital unsurlara ilişkin hükümler bulunmasa da mevcut hükümler kıyasen uygulanabilmektedir. Dünya Ticaret Örgütü (DTÖ) kurucu anlaşmasına ek olarak 1994’te imzalanan ve TRIPS adıyla anılan Fikri Mülkiyet Haklarının Ticaretle İlişkili Yönleri

⁸⁹⁵ 17 U.S. Code, §512; yasa metni için bkz. <https://www.copyright.gov/legislation/dmca.pdf> (31.12.2024).

⁸⁹⁶ R. G., 13.12.1951, Sayı.7981.

⁸⁹⁷ R. G., 12.06.1995, Sayı.22311.

⁸⁹⁸ Canan Küçükali, “Bilgisayar Programlarının Fikri Mülkiyet Kapsamında Korunması”, *İstanbul Ticaret Üniversitesi Sosyal Bilimler Dergisi*, Cilt.19, Sayı.37, Covid19-Özel Ek, (2020), s.105.

⁸⁹⁹ Cahit Suluk, Rauf Karasu ve Temel Nal, *Fikri Mülkiyet Hukuku*, Ankara: Seçkin Yayıncılık, 2017, s.239.

⁹⁰⁰ İmzalandığı günden bu yana muhtelif zamanlarda revizyona uğrayan sözleşmenin 1979’daki düzenleme ile oluşmuş son halinin İngilizce metni için bkz. <https://www.wipo.int/wipolex/en/text/283693> (31.12.2024).

Hakkı Anlaşma'da (*Agreement on Trade-Related Aspects of Intellectual Property Rights*)⁹⁰¹ Bern Sözleşmesi'ne atıfta bulunularak, “Bilgisayar programları ister kaynak ister nesne kodu olsun, Bern Sözleşmesi kapsamında edebi eser olarak korunacaktır” hükmü getirilmiştir.⁹⁰² Devamında “veri tabanı (*database*)” kavramı da “veri derlemesi (*compilations of data*)” tabiriyle yer bulmuştur. Hükme göre “seçimi veya tanzimi fikri yaratış teşkil eden” veri veya diğer materyallerin derlemeleri telif koruması altındadır. Söz konusu koruma, derlenen veri veya materyalle ilgili değil; derlemenin bizzat kendisiyle ilgilidir.⁹⁰³ 1995'te DTÖ ile WIPO arasında bir iş birliği anlaşması imzalanmış,⁹⁰⁴ sonrasında 1996'da imzalanan WIPO Telif Antlaşması (*WIPO Copyright Treaty*)⁹⁰⁵ ile bilgisayar programları ve veri tabanları TRIPS hükmüne paralel şekilde telif koruması altına alınmıştır.⁹⁰⁶

Uluslararası iş birliği ve hukuk düzenlemeleri sayesinde fikri mülkiyet koruması sınır aşıcı özellik kazanmıştır. Devletler, bu alanda yabancılık unsuru içeren uyuşmazlıklara Milletlerarası Özel Hukuk ilkelerine göre çözüm bulmaktadır.⁹⁰⁷ Ayrıca alan adı uyuşmazlıklarının çözümünün RUDRP'ye göre ICANN adına gerçekleştirildiği WIPO Tahkimi, bir uluslararası uyuşmazlık çözümü enstrümanı olarak öne çıkmaktadır.⁹⁰⁸

2. İnternet Üzerinde Yetki İcrası

Devletler, internetin fiziksel altyapısı ve internette eylemde bulunan süjeler üzerinde olduğu gibi, internetin mantıksal yapısı üzerinde de yetki sahibidir. Özellikle Web mimarisinin sonucu olarak; devletlerin mantıksal boyuta ve verilere müdahalesi, yabancı veya ülke dışındaki kişiler üzerinde yetki tespit ve icrasına göre çoğu kez daha

⁹⁰¹ Anlaşma hakkında genel bilgiler ve İngilizce metne erişim için bkz. https://www.wto.org/english/docs_e/legal_e/27-trips_01_e.htm (31.12.2024).

⁹⁰² TRIPS, m.10/1.

⁹⁰³ TRIPS, m.10/2.

⁹⁰⁴ Anlaşmanın İngilizce metni için bkz. https://www.wto.org/english/tratop_e/trips_e/towip_e.htm (31.12.2024).

⁹⁰⁵ Antlaşmanın İngilizce metni için bkz. <https://www.wipo.int/wipolex/en/text/295166> (31.12.2024).

⁹⁰⁶ Söz konusu koruma, “ifade şekli ve biçimi ne olursa olsun” kaydıyla vurgulanmıştır; WIPO Telif Sözleşmesi, m.4.

⁹⁰⁷ Abdurrahman Hamza Tüzgen, “Tasarımlara İlişkin Yabancılık Unsuru Taşıyan Uyuşmazlıklarda Uygulanacak Hukuk”, *Ticaret ve Fikri Mülkiyet Hukuku Dergisi*, Cilt.9, Sayı.2, (2023), s.310; Cansu Kaya Ülken, “Yabancılık Unsuru İçeren Fikri Haklara İlişkin Uyuşmazlıklarda İlk Sahipliğin Tespiti Sorunu”, Canan Küçükali (Ed.), *Fikri Mülkiyet Hukukunda Güncel Gelişmeler Uluslararası Sempozyumu Tam Metin Bildiri Kitabı*, Balıkesir, 23-24 Haziran 2023, İstanbul: Filiz Kitabevi, 2023, ss.104-106.

⁹⁰⁸ Bkz. dipnot.631.

rahat şekilde gerekleřmektedir. İnternet ierięine devlet mdahalesi, resm kurumlar vasıtasıyla doęrudan icra edilebileceęi gibi bařta İSS'ler olmak zere hizmet saęlayıcılar aracılığıyla da meydana gelebilmektedir.

Muhtelif amalarla belli kullanıcılar arasında kapalı devre iletiřim olanaęı saęlayan intranet sistemleri dahi lke veya uyrukluđ iliřkisi kurulabildięi takdirde devlet yetkisine tabidir. Bu sistemlerin szgelimi bir soruřturma kapsamında gizli řekilde takibe alınması yahut aıktan ve cebren mdahale etmek suretiyle eriřim saęlanması gibi uygulamalar, hukuken ngrlmř řartlar karřılandığında devletler iin mmkndr. İnternette ise Tor Aęı gibi alternatif aęların yahut IP zerinden Ses İletimi (*Voice over Internet Protocol* (VoIP)), Dosya Aktarım Protokol (*File Transfer Protocol* (FTP)), İnternet Aktarmalı Sohbet (*Internet Relay Chat* (IRC)) gibi P2P protokollerin kullanımında da benzer durum geerlidir. Web ise hiper metin ve hiper link yapısı, kamusallařması ve İSS'ler ile site iřletmecilerinin tahakkmnde olması ile farklılařmaktadır. Ortaya ıktıęı zamanlardaki adem-i merkeziyeti yapısı ile zgrlk ve devletlerden baęımsızlık rzgarına sebep olan Web, gnmzde ana hatlarıyla olduka kontrol edilebilir hale getirilmiřtir. Devletler iin sjeler ve fiilleri zerindeki yetki icrasının yanında Web ierikleri zerindeki icra imkanları da geliřmiřtir. Genellikle İSS'ler ile yer ve hizmet saęlayıcıları muhatap alan devletler, Web ieriklerine yapılacak mdahaleleri bu muhatapları vasıtasıyla gerekleřtirmektedir. Sz konusu ierikler iin; gzetleme ve denetleme, kaldırma, filtreleme ve eriřim engelleme gibi yntemlere bařvurulabilmektedir.

a. Gzetim ve Denetim

Devletlerin, lkelerinde meydana gelen olaylar ve kiřilerin eylemleri zerinde gzetim ve denetim yetkisine sahip olması, devlet olmanın doęal bir sonucudur. Lakin bu yetkinin sınırlarına dair tartıřmalar muhtemeldir ki devlet mefhumu var olduęu srece devam edecektir. Mamafih kamu dzeni ve milli gvenlik gibi kaygılar ile insan hak ve zgrlkleri arasındaki dengeyi saęlamak, hukukun etin bir vazifesidir. Devletlerin ulusal hukuk dzenlemelerinin ve mer'i uygulamalarının bu bakımdan yerindelięi meselesi, anayasa ve insan hakları baęlamındaki farklı alıřmaların konusudur. Modern egemen devletler sistemine dayalı uluslararası hukukun konu hakkındaki esas meselesi

ise; yetki doktrinleriyle tesis ve icra sınırları belirlenen devletlerin, sınır aşan ve bütünü üstünde egemenlik iddiası mümkün olmayan internet üzerindeki gözetim ve denetim normları ve uygulamaları ile oluşan vakıanın tespiti. Zira devletleri bundan meneden yahut açıkça sınırları belirleyen bir uluslararası hukuk kaynağının yokluğunda, devlet normları ve uygulamaları rehber niteliğinde kabul edilecektir.

İnternet bağlamında “gözetim (*surveillance*)”⁹⁰⁹ eylemi, en sade tanımla kullanıcılar ile sunucular arasındaki trafiğin ve içeriğin takibini ifade etmektedir. Web’in geçirdiği evrim ve kullanıcıların internet ortamına sağladığı içeriğin ulaştığı çeşitlilik ve büyüklük, gözetimi sosyal ve siyasal açıdan çok kapsamlı ve etkili bir araç haline getirmiştir. İnternet gözetimi teknoloji temelli bir eylem olduğu için en başta teknoloji sahiplerinin fiilen elinde bulundurduğu bir imkandır. Dolayısıyla akla ilk olarak şirketler gelmektedir. İnternet hizmetlerini doğrudan kullanıcıyla buluşturan şirketler, hizmetlerin kullanımıyla ortaya çıkan veri yığınına karşı hâkim pozisyonundadır. Devletlerin de hem doğrudan teknoloji kullanımı marifetiyle hem şirketler üzerindeki yetkisini kullanmak suretiyle gözetim icra etmesi mümkündür. Hem şirketler hem devletler tarafından yürütülen gözetim açık veya örtülü, hukuki veya hukuka aykırı olabilir. Şirketler için öncelik genellikle reklam isabeti, kullanıcı alışkanlıklarının tespiti, pazar hakimiyeti, verilerden maddi menfaat sağlanması gibi ekonomik/ticari motivasyonlardır. Devletler ise kamu düzeninin ve milli güvenliğin temini başlığı altında; siber güvenlik, terörle mücadele, suç önleme ve tespit, kitlelerin siyaseten kontrolü veya baskı altına alınması, mali denetim, hak ve özgürlüklerin muhafazası, dezavantajlı grupların korunması gibi amaçlar taşıyabilir. Ayrıca çocuk istismarı gibi kamu vicdanında büyük tahribata sebep olan suçlara karşı uluslararası örgütler, STK’lar ve gönüllüler tarafından düzenli izleme, raporlama ve bildirim faaliyetleri yürütülmektedir.⁹¹⁰

⁹⁰⁹ Literatürde BİT kullanımı yoluyla gözetim izleme için “veri gözetimi/verizleme (*dataveillance*)”, dijital/elektronik gözetim, elektronik panoptikon gibi kullanımlar tercih edilmektedir; Christian Fuchs ve Diğerleri, “Introduction: Internet and Surveillance”, Christian Fuchs ve Diğerleri (Ed.), **Internet and Surveillance: The Challenges of Web 2.0 and Social Media** içinde (1-28), New York, London: Routledge, 2012, s.1.

⁹¹⁰ Uluslararası Kriminal Polis Teşkilatı (*The International Criminal Police Organization* (INTERPOL)) bünyesindeki Çocukların Cinsel İstismarı Uluslararası Veri Tabanı (*International Child Sexual Exploitation* (ICSE) *Database*), Uluslararası İnternet İhbar Merkezleri Birliği (*International Association of Internet Hotlines* (INHOPE)), İnternet İzleme Vakfı (*Internet Watch Foundation* (IWF)), gibi kurumlar örnek olarak gösterilebilir. Haklarında detaylı bilgi için sırasıyla bkz. <https://www.interpol.int/Crimes/Crimes-against-children/International-Child-Sexual-Exploitation-database> (31.12.2024), <https://www.inhope.org> (31.12.2024), <https://www.iwf.org.uk/about-us/> (31.12.2024).

Uluslararası hukukta internet gözetimine dair sınırlar insan hakları sözleşmelerinden başlamaktadır. İnsan Hakları Evrensel Beyannamesi,⁹¹¹ Medeni ve Siyasi Haklar Sözleşmesi,⁹¹² Avrupa İnsan Hakları Sözleşmesi (AİHS)⁹¹³ gibi metinlerde özel hayatın ve haberleşmenin mahremiyeti vurgulanmıştır. Siber uzay özelinde ise BM Genel Kurulu, 2014 tarihli Dijital Çağda Mahremiyet Hakkı başlıklı kararıyla devletlere şu çağrılarda bulunmuştur:⁹¹⁴

“(a) Dijital iletişim bağlamı da dahil olmak üzere mahremiyet hakkına saygı gösterilmesi ve onun korunması;

(b) İlgili ulusal mevzuatın uluslararası insan hakları hukuku kapsamındaki yükümlülüklerine uygunluğunu temin etmek de dahil olmak üzere, bu hakların ihlallerine son vermek ve bu tür ihlalleri önleyecek şartları sağlamak için tedbirler almak;

(c) Uluslararası insan hakları hukuku kapsamındaki tüm yükümlülüklerinin tam ve etkili bir şekilde uygulanmasını sağlayarak mahremiyet hakkını idame ettirmek amacıyla; kitlesel gözetim, dinleme ve toplama dahil olmak üzere iletişimlerin gözetimi, dinlenmesi ve kişisel verilerin toplanmasıyla ilgili usullerini, uygulamalarını ve mevzuatlarını gözden geçirmek;

(d) İletişimlerin devletçe gözetimi, dinlenmesi ve kişisel verilerin toplanması için uygun ölçüde şeffaflığı ve hesap verilebilirliği sağlayabilecek bağımsız, etkili yerel denetim mekanizmaları kurmak veya mevcut olanları sürdürmek”

İnsan hak ve özgürlüklerine dair sınırlar, yukarıda bahsedildiği üzere uluslararası hukukun temelini oluşturan egemenlik haklarına karşı çizilmiştir. Diğer taraftan fiziksel uzayda olduğu gibi siber uzay için de devletlerin egemen eşitliği ve iç işlerine karışmama ilkeleri küresel kabul görmüş durumdadır. Bu bakımdan devletin internet üzerindeki iç egemenliğine tekabül eden yetkisinin ilk basamağı gözetim ve denetim olacaktır.

⁹¹¹ İnsan Hakları Evrensel Beyannamesi, m.12: “Hiç kimse özel hayatı, ailesi, meskeni veya yazışması hususlarında keyfi karışmalara, şeref ve şöhretine karşı tecavüzlere maruz bırakılamaz. Herkesin bu karışma ve tecavüzlere karşı kanun ile korunmaya hakkı vardır.”

⁹¹² Medeni ve Siyasi Haklar Sözleşmesi, m.17: “Hiç kimsenin özel hayatına, ailesine, evine ya da haberleşmesine keyfi ya da yasadışı olarak müdahale edilemez; hiç kimsenin şeref ve itibarına yasal olmayan tecavüzlerde bulunulamaz.”

⁹¹³ Resmi adıyla; İnsan Haklarının ve Temel Özgürlüklerin Korunması Sözleşmesi (Convention for the Protection of Human Rights and Fundamental Freedoms), UNTS, Vol.213, No.2889, 1955, s.221; m.8: “1. Herkes özel ve aile hayatına, konutuna ve yazışmasına saygı gösterilmesi hakkına sahiptir.

2. Bu hakkın kullanılmasına bir kamu makamının müdahalesi, ancak müdahalenin yasayla öngörülmüş ve demokratik bir toplumda ulusal güvenlik, kamu güvenliği, ülkenin ekonomik refahı, düzenin korunması, suç işlenmesinin önlenmesi, sağlığın veya ahlakın veya başkalarının hak ve özgürlüklerinin korunması için gerekli bir tedbir olması durumunda söz konusu olabilir.”

⁹¹⁴ UN/General Assembly, The Right to Privacy in the Digital Age, A/RES/68/167, 21.01.2014, ss.2-3.

Siber uzayda etkin gözetim politikaları izleyen Çin, Siber Güvenlik Yasası⁹¹⁵ hükümleriyle vatandaşlarına güvenli ve yaygın şekilde ağ erişimi sunmayı taahhüt etmiş; ağları kullanan vatandaşların da rejime ve sosyoekonomik düzene tehdit teşkil edecek davranışlarda bulunmalarını yasaklamıştır.⁹¹⁶ Siber uzayda hukuka uygunluğun denetimi ve tehditlere karşı güvenliğin sağlanması için de bir “siber güvenlik izleme, erken uyarı ve bilgi iletişim sistemi” kurulmasına hükmedilmiştir.⁹¹⁷ Çin ayrıca her devletin sınırları içerisindeki veri akışını tamamen kontrol etme yetkisi olduğunu kabul etmektedir.⁹¹⁸

ABD’nin 11 Eylül sonrasındaki güvenlikçi politikalarının sembollerinden olan ABD Yurtseverlik Yasası’nın (*USA PATRIOT Act*)⁹¹⁹ 215. Bölüm hükümleri ile devlete internet üzerinde geniş bir gözetim yetkisi tanınmıştır.⁹²⁰ Yasanın süresi 2015’te dolduğunda ise bu kez ABD Özgürlük Yasası (*USA FREEDOM Act*)⁹²¹ adında yeni bir yasa ile reforma gidilmiştir. Aradaki süreçte 1978 tarihli Yabancı İstihbarat Gözetimi Yasası’nda (*Foreign Intelligence Surveillance Act (FISA)*) reform yapılmış ve 2008 tarihli FISA Değişiklikleri (*FISA Amendments*)⁹²² kabul edilmiştir. Sonuçta ABD hukukunda internet gözetimine dair hukuki dayanak, Yurtseverlik Yasası ile getirilen normların Özgürlük Yasası ile tadil edilmiş hali ve FISA normları tarafından tamamlanan kısımlardan müteşekkildir.⁹²³ FISA hükümleriyle ABD hükümetine, ABD dışındaki kişilerin internet hareketlerinin dahi milli güvenlik gerekçesiyle gözetimi için yetki tanınmıştır. Gelgelelim bu yetkinin NSA tarafından ABD ülkesindeki ABD vatandaşlarının bilgileri için de kullanılmak suretiyle istismar edildiği, işeyişi gizlilik esasına göre yürüten FISA Mahkemesi’nin konu hakkındaki beyanının kamuya

⁹¹⁵ Yasanın İngilizce çevirileri için bkz. <https://digichina.stanford.edu/work/translation-cybersecurity-law-of-the-peoples-republic-of-china-effective-june-1-2017/> (31.12.2024); <https://www.chinajusticeobserver.com/law/x/cybersecurity-law-of-china-20161107> (31.12.2024).

⁹¹⁶ Çin Siber Güvenlik Yasası, m.12.

⁹¹⁷ Çin Siber Güvenlik Yasası, m.51.

⁹¹⁸ Cemre Çise Kadioğlu Kumtepe, “Siber Uzayda Kuvvet Kullanma Yasağı ve Yasağın İstisnalarının Geçerliliğinin Tallinn Rehberi Kapsamında Değerlendirilmesi”, *The Turkish Yearbook of International Relations*, Vol.53, (2022), s.26.

⁹¹⁹ Yasanın resmi ve tam adı: “*Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001*”.

⁹²⁰ American Civil Liberties Union, “Surveillance Under the USA/PATRIOT Act”, <https://www.aclu.org/documents/surveillance-under-usapatriot-act> (31.12.2024).

⁹²¹ Yurtseverlik yasasına benzer şekilde yasanın resmi ve tam isimden anlamlı bir kısaltma çıkarılmıştır: “*Uniting and Strengthening America by Fulfilling Rights and Ensuring Effective Discipline Over Monitoring Act of 2015*”;

⁹²² 129 Stat. 268 – Public Law No.114-23, 06.02.2015.

⁹²³ 215. Bölüm özelinde düzenlemeler arasındaki ilişkiye dair resmi bilgilendirme için bkz. United States House of Representatives/Judiciary Committee, “USA Freedom Act”, <https://judiciary.house.gov/usa-freedom-act> (31.12.2024).

açılmasıyla ortaya çıkmıştır.⁹²⁴ Bu gelişme, PRISM vakasının baş aktörü *Snowden* tarafından ileri sürülen iddialarla paralellik içermektedir.⁹²⁵

SORM kısaltmasıyla bilinen “Operasyonel Soruşturma Faaliyetleri Sistemi”, Rusya’da başta Federal Güvenlik Sevisi (FSB) olmak üzere ilgili devlet kurumlarınca ağ gözetiminin etkili bir enstrümanı olarak kullanılmaktadır.⁹²⁶ SORM, 1995 tarihli Operasyonel Arama Faaliyetleri Federal Yasası’na⁹²⁷ dayanmaktadır. Yasanın kapsamı yıllar içinde genişletilmiştir. Diğer taraftan 2016’da kabul edilen ve Yarovaya Yasaları adıyla bilinen düzenlemelerle hizmet sağlayıcıların veri ve metaveri saklama yükümlülüklerinde süre uzatımına gidilmiş, mesajlaşma uygulamalarında şifreli arka kapılar bulundurulması zorunlu tutulmuştur.⁹²⁸

Türkiye’de genel internet denetimi BTK tarafından yürütülmektedir.⁹²⁹ Ayrıca Milli İstihbarat Teşkilatı’na (MİT), 2014’te kabul edilen değişiklikle “*Dış istihbarat, millî savunma, terörle mücadele ve uluslararası suçlar ile siber güvenlik konularında her türlü teknik istihbarat ve insan istihbaratı usul, araç ve sistemlerini kullanmak suretiyle bilgi, belge, haber ve veri toplamak, kaydetmek, analiz etmek ve üretilen istihbaratı gerekli kuruluşlara ulaştırmak*” yetkisi verilmiştir.⁹³⁰ Ayrıca hemen her ülkede benzerleri olduğu üzere BTK ve USOM, siber uzaydaki hukuka aykırılıklara yönelik çevrimiçi ihbar hizmeti sunmaktadır.⁹³¹

⁹²⁴ Greg Nojeim, “FISA Court Opinion Outlines FBI Abuse of Key Intelligence Surveillance Authority”, Center for Democracy & Technology, 04.09.2020, <https://cdt.org/insights/fisa-court-opinion-outlines-fbi-abuse-of-key-intelligence-surveillance-authority/> (31.12.2024); ABD Ulusal İstihbarat Direktörlüğü Ofisi’nin (*Office of the Director of National Intelligence* (ODNI)) verdiği yetkiyle kamuya açılan FISA Mahkemesi beyan ve emir için bkz. https://www.intelligence.gov/assets/documents/702%20Documents/declassified/2019_702_Cert_FISC_Opinion_06Dec19_OCR.pdf (31.12.2024).

⁹²⁵ Katie Randers, “Fact-checking John Oliver's Interview with Edward Snowden about NSA Surveillance”, Politifact, 09.04.2015, <https://www.politifact.com/factchecks/2015/apr/09/edward-snowden/fact-checking-john-olivers-interview-edward-snowden/> (31.12.2024).

⁹²⁶ Andrei Soldatov ve Irina Borogan, “Russia's Surveillance State”, **World Policy Journal**, Vol.30, No.3, (2013), s.25; Nathalie Maréchal, “Networked Authoritarianism and the Geopolitics of Information: Understanding Russian Internet Policy”, **Media and Communication**, Vol.5, No.1, (2017), s.33.

⁹²⁷ Federal law No. 144-FZ of 12 August 1995, m.8; Kanun metninin İngilizce çevirisi için bkz. https://www.wto.org/english/thewto_e/acc_e/rus_e/wtaccrus58_leg_373.pdf (31.12.2024).

⁹²⁸ Maréchal, s.34.

⁹²⁹ BTK, “Denetleme”, 15.12.2017, <https://www.btk.gov.tr/denetleme> (31.12.2024).

⁹³⁰ 6532 sayılı Devlet İstihbarat Hizmetleri ve Millî İstihbarat Teşkilatı Kanununda Değişiklik Yapılmasına Dair Kanun, m.1; R. G., 26.04.2014, Sayı.28983.

⁹³¹ Hizmetlere erişim için sırasıyla bkz. BTK, “İnternet İhbar Başvurusu”, <https://www.turkiye.gov.tr/btk-internet-ihbar-basvurusu> (31.12.2024), USOM, “İhbar”, <https://www.usom.gov.tr/ihbar> (31.12.2024).

İnternetin devletlerin gözetiminde olması, günümüzde bir sır olarak görülmemektedir. Devletler, hukuk düzenlemeleri ve teknik kapasiteleri ölçüsünde veri toplama ve değerlendirme süreçlerini yürütmektedir. Çoğu durumda ise bunun için hizmet sağlayıcılardan bilgi talep edilmektedir. Çocuk istismarı ve uyuşturucu ticareti gibi vakalarda hizmet sağlayıcılar ilgili devlet makamlarına kendiliğinden bilgi verebilirken, bilhassa ölüm veya ciddi yaralamaya ilişkin tehlike durumlarında acil bilgi taleplerine de karşılık verilebilmektedir.⁹³² Şifreli iletişim ise gözetim meselenin çekirdeğini oluşturan hususlardandır. Özel hayatın ve iletişimin mahremiyeti gereği şifreli iletişim kural olarak serbest olsa dahi içeriğine asla erişilemeyecek şekilde şifrelenmiş iletişim araçlarına karşı devletlerin -en azından- mesafeli olması doğaldır. Hizmet sağlayıcılara en sık talep ileten devletlerden Hindistan'da 2000 tarihli Bilgi Teknolojisi Yasası (*The Information Technology Act*)⁹³³ ile devletin güvenliği, kamu düzeni, yabancı devletlerle dostane ilişkilerin sürmesi ve suçun önlenmesi gibi gerekçelere dayalı talep durumunda şifreli iletişim içeriğinin devlete bildirilmesi zorunlu kılınmıştır. Bu durumlarda şifre çözümünden imtina edilmesi ise hapis cezasına tabi tutulmuştur.⁹³⁴ ABD'de Kolluk Kuvvetleri için İletişim Yardımı Yasası (*Communications Assistance for Law Enforcement Act (CALEA)*),⁹³⁵ Rusya'da Yarovaya Yasaları benzer yetkiler öngörmektedir. Çin'e gelindiğinde Siber Güvenlik Yasası, Kriptografi Yasası⁹³⁶ ve Kamu Güvenlik Kurumları Tarafından İnternet Güvenliği Gözetim ve Denetimine İlişkin Yönetmelik⁹³⁷ gibi düzenlemelerle dijital ve şifreli iletişimin sıkı gözetim altına alındığı görülmektedir. Uçtan uca şifreleme hizmeti sunan mesajlaşma uygulamalarda ise ne hizmet sağlayıcının ne devletin mesaj içeriklerine erişim imkânı bulunmaktadır.⁹³⁸ Devletlerin bilgi paylaşımına dair zorlayıcı hükümlerini bu alana genişletmeleri ve caydırıcı yaptırımlar öngörmeleri halinde söz konusu hizmet

⁹³² En yaygın kullanılan sosyal medya platformlarından X ve Instagram örneklerinde, işletmecilerin devletlerle bilgi paylaşımına dair belirledikleri esaslar için sırasıyla bkz. X, "Hukuki Talep SSS", <https://help.x.com/tr/rules-and-policies/x-legal-faqs> (31.12.2024), Instagram, "Kolluk Kuvvetlerine Yönelik Bilgiler", <https://help.instagram.com/494561080557017> (31.12.2024).

⁹³³ Yasa metnine ve 2008 tarihli değişikliklere erişim için bkz. <https://eprocure.gov.in/cppp/rulesandprocs> (31.12.2024).

⁹³⁴ Hindistan Bilgi Teknolojisi Yasası, m.69.

⁹³⁵ Yasaya dair genel bilgi ve metne erişim için bkz. <https://www.govinfo.gov/app/details/COMPS-937/> (31.12.2024).

⁹³⁶ Yasanın İngilizce çevirisi için bkz. Todd Kuhns, Cryptography Law of the People's Republic of China, <https://appinchina.co/government-documents/cryptography-law-of-the-peoples-republic-of-china/> (31.12.2024).

⁹³⁷ Yönetmeliğin İngilizce çevirisi için bkz. <https://digichina.stanford.edu/work/regulations-on-internet-security-supervision-and-inspection-by-public-security-bodies/> (31.12.2024).

⁹³⁸ Söz konusu durum, hizmet sağlayıcıların sistemlerini vaat ettikleri şekilde işlettikleri ve gizli bir arka kapı kullanmadıkları varsayımında geçerlidir.

sağlayıcılar ya şifreleme prosedürlerini esneterek veri çıkışı için kapı açmak ya da ilgili devletin ülkesindeki faaliyetlerine son vermek durumunda kalacaktır.⁹³⁹

b. İçerik Kaldırma

İnternet üzerinde husule gelen hukuka aykırılıkların türüne göre fail, fiil ve durum hakkındaki önlemler değişkenlik gösterir. Devlet, kişiler üzerindeki yetkisini kullanmak suretiyle suç veya haksız fiil failine ulusal hukukunu uygulayabilmektedir. Benzer durum, eşya üzerindeki ülkesel yetki kullanımında da geçerlidir. İnternetteki mantıksal unsurlar söz konusu olduğunda ise ulusal hukukun icrasını “doğrudan” gerçekleştirmek çoğu devlet için mümkün değildir.

Bir içeriğin internet aracılığıyla erişilebilir olmasının hukuka aykırılığı durumunda, bir taraftan hukuka aykırılığa sebep olan fail hakkında yetki tespit ve icrası gündeme gelirken diğer taraftan hukuka aykırı durumun sona erdirilmesi için ilgili içeriğin “erişilemez” hale getirilmesi gerekmektedir. İnternetin yapısı itibariyle bir içeriğin erişilemez hale gelmesinin birincil yolu, içeriğin bulunduğu sunucudan “kaldırılmasıdır”. Bu sonucun sağlanması ise öncelikle fiili imkanlara bağlıdır. Kaldırma eylemini gerçekleştirebilecek sükeler, kullanılan platforma göre değişebilir. Web için konuşulduğunda, bazı sitelerinin mimarisinin içerik sağlayan kişiye sonradan içeriği kaldırma imkânı tanımaması mümkündür. Kişilerin kendi cihazlarını sunucu olarak kullandığı adem-i merkezîyetçi dosya paylaşım platformlarında ise içerik ancak bu kişiler tarafından kaldırılabilir. İçerik kaldırmanın uygulamada en sık gerçekleştiği alanlar olan sosyal medya platformları ve depolama hizmetlerinde ise hem hizmet hem içerik sağlayıcılar içeriği kaldırma imkânına sahiptir. Her durumda, devletler, ülkelerindeki sunuculara fiziksel olarak ve ülke dışındaki sunuculara BİT kullanımı yoluyla cebren erişerek müdahale etmek fiili imkânına sahiptir. Fakat devletin, ülkesi dışındaki sunucuya cebren yetkisiz erişimi, -sunucu devlet dışı aktöre ait olsa dahi- sunucuyu ülkesinde bulunduran devletin egemenliğini ihlal edecek nitelikte bir siber faaliyet olarak kabul görebilir. Sunucunun uzayda yahut açık denizdeki bir platformda olması gibi durumlarda

⁹³⁹ Böyle bir gelişmenin Türkiye’de gerçekleşmesinin önüne geçilmesi yönünde sivil toplum kuruluşları, şirketler ve topluluklardan oluşan bir grup tarafından bir çağrı metni yayınlanmıştır; “Türkiye: Uçtan uca şifreleme korunmalı”, 20.04.2023, <https://www.article19.org/tr/resources/turkey-protect-end-to-end-encrypted-services/> (31.12.2024).

dahi yer sağlayıcının uyrukluk ile bağılı olduğu devlet, diplomatik koruma müessesesine dayanarak fail devletin sorumluluğunu ileri sürebilecektir.⁹⁴⁰

Uygulamada devletler genellikle içeriğin kaldırılması için hizmet sağlayıcılara başvurma yolunu izlemektedir. Belli başlı sorunların da doğrudan devlet müdahalesine gerek olmadan öncelikle internet sükjeleri arasında çözümlüne imkân tanınmıştır. Bilhassa fikri mülkiyet gibi hak ihlallerinin yargıya aksetmeden sona erdirilmesi adına DMCA ile hukuk alanına giren “uyar ve kaldır (*notice and takedown*)” prosedürü, hukuka aykırı içerik karşısında aracı hizmet sağlayıcıların sorumluluklarını sınırlamakla birlikte içeriğin kaldırılması için kullanıcı, devlet ve hizmet sağlayıcı arasında bir iş birliği zemini kurmuştur.⁹⁴¹ Bu sayede aracı hizmet sağlayıcı, platformundaki tüm içerikleri anbean izleme ve olası hukuka aykırılıkta doğrudan sorumlu tutulma gibi ağır külfetlerden kurtulmuştur. Bir içerik nedeniyle haklarının ihlal edildiğini düşünen kişi, aracı hizmet sağlayıcıya bildirimde bulunur. Böylece hem aracı hizmet sağlayıcı hukuka aykırılıktan haberdar edilmiş olur hem içeriğin kaldırılması pratik, hızlı ve verimli bir süreç sonucunda sağlanır. Aracı hizmet sağlayıcılar, içeriğin hukuka veya kendi politikalarına aykırı olduğuna kanaat getirirse, içerik sağlayıcıyı bilgilendirip içeriği kaldırmasını isteyebilir, konu hakkındaki savunmasını talep edebilir yahut doğrudan içeriği kaldırabilir. Bildirime rağmen içerik kaldırılmazsa bu kez başta yargı olmak üzere devlet organlarına başvurulur. Gelgelelim bu mekanizma zaman zaman, teoride umulduğu gibi sağlıklı işlememektedir. Bildirim sonucunda hizmet sağlayıcılar içeriği meşru bularak platformlarında tutmaya devam edebilmekte yahut aslında hukuka uygun olan bir içeriği meşru bulmayarak kaldırabilmektedir. Dolayısıyla literatürde uyar ve kaldır prosedürü keyfilik temelli olması nedeniyle eleştirilmiştir.⁹⁴²

⁹⁴⁰ UAD, Barcelona Traction Davası’nda şirketlerin uyrukluğunda olduğu devletin diplomatik koruma hakkının mevcudiyetini kabul etmiştir; Sümeyra Sena Kurt, “Uluslararası Hukukta Diplomatik Koruma”, **Anadolu Üniversitesi Hukuk Fakültesi Dergisi**, Cilt.6, Sayı.2, (2020), s.488.

⁹⁴¹ Domingos Soares Farinho ve Ricardo Resende Campos, “Models of Legal Liability for Social Networks: Between Germany and Portugal”, Carlos Blanco de Moraes, Gilmar Ferreira Mendes ve Thomas Vesting (Ed.), **The Rule of Law in Cyberspace** içinde (331-348), Cham: Springer, 2022, s.334.

⁹⁴² Jennifer M. Urban ve Laura Quilter, “Efficient Process or Chilling Effects - Takedown Notices under Section 512 of the Digital Millennium Copyright Act”, **Santa Clara High Technology Law Journal**, Vol.22, Iss.4, (2006), s.623; Aleksandra Kuczerawy, “From ‘Notice and Takedown’ to ‘Notice and Stay Down’: Risks and Safeguards for Freedom of Expression”, Giancarlo Frosio (Ed.), **Oxford Handbook of Online Intermediary Liability** içinde (525-543), Oxford: Oxford University Press, 2020, s.532; Korpisaari, ss.373-374.

İçerik kaldırılması sürecine devletlerin dahli, ilgili kurumlarının internet s jelerine talimatta bulunması ya da bir mahkeme kararının icrası yoluyla ger ekle ebilir. T rkiye  rneğinde, s z konusu i lem i in 5651 Sayılı Kanun metninde “i eriğın yayından  ıkarılması” tabiri ve “i erik veya yer saėlayıcılar tarafından i eriğın sunuculardan veya barındırılan i erikten  ıkarılması” tanımı tercih edilmi tir.⁹⁴³ Kanunda birtakım su lar belirlenmi  ve bu su ların olu tuėuna dair yeterli  p e sebebi bulunan i eriğın kaldırılabilceėi   ng r lm   t r.⁹⁴⁴ İ eriğın  ıkarılması kararı, soru turma a amasında h kim, kovu turma a amasında mahkeme tarafından verilebilmektedir.⁹⁴⁵ Ayrıca ba ta belli su  tipleri i in BTK Ba kanı’na re’sen i eriğın  ıkarılması kararı verme yetkisi tanınmı  olsa da bu yetki, su  tespitine baėlı bir nihai tedbirin yargı kararı olmaksızın uygulanmasının masumiyet karinesine aykırı d      nden bahisle Anayasa Mahkemesi’nce iptal edilmi tir.⁹⁴⁶ Mevcut durumda BTK Ba kanı, gecikmesinde sakınca bulunan hallerde istisnai  ekilde i eriğın  ıkarılması kararı verebiliyor olsa da bu kararların yine hakim onayına sunulması gerekmektedir.⁹⁴⁷

Devletler, i erik kaldırma yetkilerini hangi organlarıyla icra edeceklerini yukarıdaki  rnekte olduėu gibi ulusal hukuklarında belirlerler. Akdedilecek bir uluslararası antla ma ile uygulamada yeknesaklık saėlanabilecek olsa da devletlerin yakla ım farklılıkları hasebiyle b yle bir antla manın hen  z  ok uzak bir ideal olduėu a ıkadır. Genel uygulama, i erik kaldırma karar ve talimatlarının, i erik ve yer saėlayıcılara bildirilmesi ve gereğinin yerine getirilmesinin beklenmesi y n ndedir. Hatta   n  rneğinde hizmet saėlayıcıların hukuka aykırı i eriėi proaktif olarak tespit

⁹⁴³ 5651 sayılı Kanun, m.2/1- .

⁹⁴⁴ 5651 sayılı Kanun, m.8/1.

⁹⁴⁵ 5651 sayılı Kanun, m.8/2.

⁹⁴⁶ T.C. Anayasa Mahkemesi, E.2020/76, K.2023/172, 11/10/2023.

⁹⁴⁷ 5651 sayılı Kanun, m.8/2; “(1) Ya am hakkı ile ki ilerin can ve mal g venliėinin korunması, mill  g venlik ve kamu d zeninin korunması, su  i lenmesinin   nlenmesi veya genel saėlıėın korunması sebeplerinden bir veya bir ka ına baėlı olarak h kim veya gecikmesinde sakınca bulunan h llerde, Cumhurbaşkanlığı veya mill  g venlik ve kamu d zeninin korunması, su  i lenmesinin   nlenmesi veya genel saėlıėın korunması ile ilgili bakanlıkların talebi  zerine Ba kan tarafından internet ortamında yer alan yayınlı ilgili olarak i eriğın  ıkarılması ve/veya eri imin engellenmesi kararı verilebilir. Karar, Ba kan tarafından derh l eri im saėlayıcılara ve ilgili i erik ve yer saėlayıcılara bildirilir. İ erik  ıkarılması ve/veya eri imin engellenmesi kararının gereėi, derh l ve en ge  kararın bildirilmesi anından itibaren d rt saat i inde yerine getirilir.

(2) Cumhurbaşkanlığı veya ilgili Bakanlıkların talebi  zerine Ba kan tarafından verilen i eriğın  ıkarılması ve/veya eri imin engellenmesi kararı, Ba kan tarafından, yirmi d rt saat i inde sulh ceza h kiminin onayına sunulur. H kim, kararını kırk sekiz saat i inde a ıklar; aksi h lde, karar kendiliėinden kalkar.”

etmesi, raporlaması ve kaldırması beklenmektedir.⁹⁴⁸ Pratik güçlük ise tabii ki ülke dışında hizmet veren yer ve hizmet sağlayıcılar ile yabancı içerik sağlayıcıların kararları yerine getirmemeleri durumunda yaşanmaktadır. Devletler bu gibi durumlarda aşamalı olarak para cezası, erişim engeli, lisans iptali gibi yollara başvurabilmektedir. Bu noktada fiilen en uygulanabilir olan yöntem İSS'ler aracılığıyla erişim olsa da bu önlemin de etkisi sınırlı kalmaktadır. Sonuçta Yahoo! davasından bu yana devlet kabiliyetlerinde büyük bir sıçrama yaşandığını söylemek güçtür. Esas konsept halen içerik kaldırılmasının doğrudan içeriğe yönelik cebren devlet müdahalesiyle sağlanmasındansa muhataplara yönelik yaptırımlar ya da yaptırım tehditleriyle sağlanmasıdır. Doğrudan müdahalenin de yukarıda değinildiği üzere sunucuları ülkesinde barındıran devletlerin egemenlik haklarını ihlal edeceği görülecektir. En azından başlangıç için siber uzayda adli iş birliğine yönelik ikili antlaşmalarla bu sorunun üstesinden gelmeye çalışmanın devletlerin yararına olacağı kanaatindeyim.

c. Filtreleme ve Erişim Engeli

Hukuka aykırılık durumlarında sunuculara ve süljelere müdahale imkânı bulamayan devletler için en pratik çözüm, halihazırda egemenlikleri altında bulunan kurumsal İSS'ler marifetiyle ilgili içerikleri filtrelemek yahut içeriklere erişimi engellemektir. Söz konusu önlem, içeriğin bulunduğu sunucu ile kullanıcı arasındaki bağın kesilmesini ifade etmektedir. 5651 sayılı Kanun'da da erişimin engellenmesinin, *"Alan adından erişimin engellenmesi, IP adresinden erişimin engellenmesi, içeriğe (URL) erişimin engellenmesi ve benzeri yöntemler kullanılarak erişimin engellenmesi"* anlamına geldiği belirtilmiştir.⁹⁴⁹ Kanun böylece erişim engeli türlerini de saymış bulunmaktadır. Filtreleme ise belli türlerdeki içeriklerin belli kullanıcı gruplarına ulaşmasının engellenmesidir. Kullanıcılar, istenmeyen içeriklere maruz kalmamak için kendi iradeleriyle filtreleme programları kullanabilirken; devletler, içerik bazlı erişim engelinin diğeri bir ifade şekli olarak filtreleme önlemine başvurabilmektedir.

⁹⁴⁸ Çin Halk Cumhuriyeti, Çevrimiçi Bilgi İçeriği Ekosisteminin Yönetişimine İlişkin Hükümler (Çin Siber Uzay İdaresi, 5 Numaralı Emir), m.36 vd.; Hükümlerin İngilizce çevirisi için bkz. <https://wilmap.stanford.edu/entries/provisions-governance-online-information-content-ecosystem> (31.12.2024).

⁹⁴⁹ 5651 Sayılı Kanun, m.2/1-o.

Gözetim, denetim, filtreleme ve erişim engeli kombinasyonunun dünyadaki en meşhur sistematik uygulaması, Çin’de işleyen ve literatürde Çin Seddi’ne ithafen “Çin Güvenlik Seddi (*The Great Firewall of China*)” adıyla anılan programdır. Bu sistem bütün internet trafiğini ve paketlerin içeriğini incelemekte, yasak olan içeriğe erişimi bu yolla engellemektedir. Çin’deki uygulamaların zamanın gereğine göre sıkılaşabildiği, VPN hizmetlerine ve hatta gizlice VPN hizmeti veren Web sitelerine erişimin dahi engellenebildiği, gerek görüldüğünde kullanıcının maksadının anlaşılması adına ifadesinin alınabildiği aktarılmıştır.⁹⁵⁰

Türkiye’de erişimin engellenmesi kararı, içeriğin çıkarılması kararıyla beraber anılarak düzenlenmiştir. İçeriğin çıkarılmasına dair yukarıda değinilen AYM kararı, BTK Başkanı’nın erişim engelleme yetkisine karşı bir tasarrufta bulunmamıştır. Erişim engelinin, engellenen hizmetin türüne göre kalıcı veya belirli süreli olarak getirilmesi mümkündür.⁹⁵¹ Ayrıca en güncel örneklerden olan Instagram Web sitesine erişim engeli kararında olduğu gibi, ilgili internet süjesinin ulusal hukuka uygun davranacağını taahhüt etmesi sonucunda engel kaldırılabilir.⁹⁵² Henüz 2024 Ekim ayında Brezilya’nın, X Web sitesine getirdiği erişim engelini altı hafta sonra kaldırması da benzer bir başka süreç örneğidir.⁹⁵³

⁹⁵⁰ James Griffiths, *The Great Firewall of China: How to Build and Control an Alternative Version of the Internet*, 2’nd Edition, London: Zed Books, 2021, s.28.

⁹⁵¹ 5651 sayılı Kanun, m.8/2.

⁹⁵² Anadolu Ajansı, “Instagram’a Uygulanan Erişim Engeli Kaldırıldı”, 11.08.2024, <https://www.aa.com.tr/tr/info/infografik/40694> (31.12.2024). Her ne kadar erişim engeli kararının gerekçesi olarak söz konusu Web sitesi işletmecisinin hukuka aykırı içeriklerin kaldırılması konusunda gerekli önlemleri almaktan kaçınmakta ısrar etmesi gösterilse de hukuka uygun içeriklerin Web sitesi işletmecisi tarafından kurum politikası gerekçesiyle kaldırılması ve bu suretle özel sansür uygulanması da tetikleyici faktör olmuştur; Serhan Tutak, “Bakan Uraloğlu, Instagram’a Getirilen Erişim Engeline İlişkin Son Durumu Değerlendirdi”, Anadolu Ajansı, 06.08.2024, <https://www.aa.com.tr/tr/bilim-teknoloji/bakan-uraloglu-instagram-a-getirilen-erisim-engeline-iliskin-son-durumu-degerlendirdi/3296674> (31.12.2024).

⁹⁵³ Euronews ve Associated Press, “Elon Musk’s X to be Reinstated in Brazil after Complying with Court”, 09.10.2024, <https://www.euronews.com/next/2024/10/09/elon-musks-x-to-be-reinstated-in-brazil-after-complying-with-court> (31.12.2024); Vakının dikkat çekici bir yönü de Brezilya’da aktif olarak erişim sağlayıcılık hizmeti veren Starlink’in bağlı olduğu SpaceX şirketinin, söz konusu karara uyarak “X” Web sitesine erişimi engellemesidir. SpaceX ve X şirketleri ayrı tüzel kişilikler olsa da günümüzün önde gelen teknolojik iktidar sahiplerinden Elon Musk’ın yönetimi altındadırlar. SpaceX, sahip olduğu teknik avantajlara rağmen Brezilya makamlarının kararını uygulamış, sunduğu hizmetin meşruiyetini muhafaza yoluna gitmiştir. Yaşanan bu gelişmeler, internet süjelerinin, ellerindeki fiili imkanlardan bağımsız olarak ilgili devletlerin otoritelerine uymak suretiyle meşru zeminde kalmaktaki menfaatlerinin, hukukun tatbik edilebilirliğindeki kritik önemine işaret etmektedir; Muhammed Enes Çallı, “Starlink to comply with court orders to block X in Brazil”, Anadolu Ajansı, 04.09.2024, <https://www.aa.com.tr/en/world/starlink-to-comply-with-court-orders-to-block-x-in-brazil/3320971> (31.12.2024).

ABD’de erişim engeli uygulaması farklı yasalara dayanılarak yargı kararıyla icra edilmektedir. DMCA, Çocukların İnternette Korunması Yasası (*Children’s Internet Protection Act* (CIPA)),⁹⁵⁴ Devletlerin ve Mağdurların Çevrimiçi Seks Ticaretiyle Mücadele Etmesine İzin Yasası (*Allow States and Victims to Fight Online Sex Trafficking Act*) ve Seks Tacirlerine Müsaadeyi Durdurma Yasası (*Stop Enabling Sex Traffickers Act*) (FOSTA-SESTA)⁹⁵⁵ gibi düzenlemeler, içeriğin türüne göre önlemler öngörür. Nisan 2024’te ABD Temsilciler Meclisi’nden geçen, Amerikalıları Yabancı Hasım Kontrolündeki Uygulamalardan Koruma Yasası (*Protecting Americans from Foreign Adversary Controlled Applications Act* (PAFACA))⁹⁵⁶ ise ABD Başkanı yahut ilgili birimler tarafından “yabancı hasım kontrolünde” olduğu tespit edilen uygulamaların (yazılım, Web sitesi, mobil uygulamalar vs.) kullanımının belli süre içinde yasaklanmasını düzenlemektedir. Hali hazırda yabancı hasım kapsamına giren devletler Kuzey Kore, Çin, Rusya ve İran’dır.⁹⁵⁷ Bilhassa Çin menşeli TikTok uygulamasına karşı gündeme gelen yasa, içeriğin türüne değil kaynağına ve hatta bizzat yer sağlayıcısının kimliğine göre engelleme öngörmesi bakımından sıra dışı niteliktedir. Yasanın yürürlüğe girmesi halinde, kastedilen türdeki uygulama sahiplerini uygulamalarını satmak ve ABD’de hizmet sunamamak arasında bir seçime zorlayacağı belirtilmiştir.⁹⁵⁸

İnternet içeriğinin tamamen özgür ve devlet denetiminden azade olması artık mümkün ve makul görünmemektedir. Hatta İSS’ler dahi kara liste gibi uygulamalarla devlet ile kullanıcı arasındaki noktada denetim ve engelleme faaliyeti gerçekleştirebilmektedir.⁹⁵⁹ İçeriğe devlet müdahalesinin sınırları da hemen her ülke için yoğun bir tartışmanın konusudur. Uygulamadaki zorluklar ise sorunun diğer bir cephesidir. Kaldırılan içerik neredeyse anında tekrar internette erişebilir hale gelmekte, erişim engelleri ise gerek kullanıcılar gerek engele maruz kalmış Web sitesi işletmecileri veya yer sağlayıcılar tarafından kullanılan yöntemlerle aşılabilmektedir. VPN veya vekil

⁹⁵⁴ Yasa hakkında resmi bilgilendirme için bkz. <https://www.fcc.gov/consumers/guides/childrens-internet-protection-act> (31.12.2024).

⁹⁵⁵ 132 Stat. 1253 – Public Law No.115-164, 11.04.2018.

⁹⁵⁶ Yasa teklifine ve yasama sürecine dair bilgi için bkz. <https://www.congress.gov/bill/118th-congress/house-bill/7521> (31.12.2024).

⁹⁵⁷ 10 U.S. Code, §4872, (d), (2).

⁹⁵⁸ Sapna Maheshwari, David McCabe ve Annie Karni, “House Passes Bill to Force TikTok Sale From Chinese Owner or Ban the App”, The New York Times, 13.03.2024, <https://www.nytimes.com/2024/03/13/technology/tiktok-ban-house-vote.html> (31.12.2024).

⁹⁵⁹ Bkz. dipot.883.

sunucu kullanımı, kullanıcılar tarafından tercih edilen en yaygın usullerdir. Diğer taraftan bir alan adı engellendiğinde hemen benzer yenisini hizmete sunmak ve bu döngüyü sürekli hale getirmek -Türkiye’de bilhassa popülerlik kazanmış korsan yayın, yasadışı bahis ve kumar gibi içerikleri sunan Web sitelerinde de yaygın şekilde görüldüğü üzere- hizmet sağlayıcıların en sık tercih ettiği yollardandır. Sözgelimi xyz.abc alan adlı Web sitesine erişim engellendiğinde, aynı site içeriği sırasıyla xyz1.abc, xyz2.abc gibi sonu gelmeyen alan adı kombinasyonları ile tekrar hizmete sunulmaktadır. Devletler adına ortaya çıkan durum, *Post*’un çekiçe köstebek vurma benzetmesini tekrar haklı çıkarır niteliktedir. Yine de erişim engeli önleminin işlerliğinin, devletlerin tutumlarına büyük ölçüde bağlı olduğu yadsınamaz. Köstebek vurma oyunu, bir bakıma hukukun trajedisi gibi görünse de esasen titiz ve seçici işleyen, internet özgürlüğüne müdahalede ölçülü davranan hukuk sistemlerinde karşılaşılan bir olgudur. Oysa devletlerin açık veya örtülü şekilde VPN hizmeti veren sunuculara erişimi engellemesi, barındırdığı Web siteleri hakkında belli sayıda erişim engeli kararı alınmış yer sağlayıcıların sunucularına kapsamlı erişim engelleri getirmesi, gözetim ve denetim uygulamalarını teknik olarak sıkılaştırması, ileri seviyelerde ülke içinde geniş çaplı internet kesintilerine gitmesi ve hatta ülke dışına bağlantıyı keserek intranet uygulamasına dönmesi gibi radikal seçenekleri de mevcuttur. Hizmet sağlayıcıların, içeriklerini ülkesel ve konum bazlı filtrelerle ulusal hukuk sistemlerine uygun hale getirmesi; adli istinabe süreçlerinin işleyişinde uluslararası mutabakatın genişlemesi ve derinleşmesi; bilhassa çocukların korunması ile uyuşturucu ve insan kaçakçılığı gibi suçların engellenmesi için internet sükjeleri üzerinde etkin şekilde işleyecek bir sistemin uluslararası işbirliği ile tesisine yönündeki girişimler, devletlerin internet üzerindeki yetki icrasında karşılaşılan birçok soruna çözüm olacaktır.

3. Büyük Veri, Bulut Bilişim ve Holizm Bağlamında Veri ve Kişisel Veriler

Siber uzayın veri unsuru, hukuk alanında sıklıkla kişisel veriler ve bir basamak daha altında kişisel verilerin korunması özelinde ele alınmaktadır. Devlete ilişkin tasnifli veri ve belgelere dair hükümlerin fiziksel uzaya kıyasla siber uzay için de uygulanabileceği açıktır. Kişilere ilişkin verilerin ise BİT alanındaki gelişmeler

sonucunda devletlerce hususi hükümlerle korunması gerekmiştir. Devletler, kişilerin başta özel hayatın gizliliği olmak üzere temel hak ve özgürlüklerini güvence altına almak adına kişisel verilerin korunmasına dair kanunlar ihdas etmektedirler. Verilerin toplanması ve işlenmesinde önemli iktisadi menfaatleri olan yatırımcı sermaye gruplarının talepleri ile vatandaşların hakları arasında denge kurmak da bu kanunların bir diğer amacıdır.⁹⁶⁰ Bu minvalde ortaya çıkan hukuki düzenlemeler ve standartlar, ülkelerin sınırlarını aşır GDPR ile uluslararası hukukta da hayat bulmuştur. Devletler bu tür yasal enstrümanlarla kişisel verilerin korunması başlığında kişilerin hak ve özgürlüklerini müdafaa etme çabasıdayken, gelişen teknoloji ile kişisel verilerin devletin bizzat kendi menfaatlerine temas eden yeni odak noktaları doğmuştur.

Devletler, vatandaşlarıyla veya kurumlarıyla ilişkilendirilen ya da ülkelerinden elde edilen veriler üzerinde egemenlik kaynaklı yetkilere sahiptir. Her bir kişinin kendisiyle ilişkilendirilen veriler, kişilik hakları bağlamında hukuka konu edilirken; geniş kitlelerin verileri ulus ve devlet seviyesinde önem arz edebilir. Bu noktada büyük veri kavramı öne çıkmaktadır. Esasen büyük veri, BİT bilimlerine ilişkin teknik bir kavramdır. Fakat günümüzde “moda sözcük (*buzzword*)” konumuna gelmiş ve sosyal bilimler literatürüne, “işlenmesi belirli amaçlara hizmet edebilir nitelikte, kaynak ve format çeşitliliği, akış hızı ve depolanma hacmi yüksek veri setlerini” ifade edecek şekilde yerleşmiştir.⁹⁶¹ Büyük verinin sosyal bilimlerde bulduğu karşılık, *Craig ve Ludloff* tarafından şöyle açıklanmıştır:⁹⁶²

“Bugün, daima açık, dijital bir dünyada faaliyet gösteriyoruz: Çevrimiçi çalışıyoruz, çevrimiçi sosyalleşiyoruz, haberleri ve en sevdiğimiz programları çevrimiçi takip ediyoruz, vergilerimizi çevrimiçi beyan ediyoruz, çevrimiçi bankacılık yapıyoruz, hatta çevrimiçi olarak kumar oynuyor veya cinsel isteklerimizin peşinden koşuyoruz. Ve yaptığımız her şey bir dijital ayak izi bırakıyor, öyle ki buna bir isim vermek zorunda kaldık: büyük veri.”

⁹⁶⁰ TBMM, **Kişisel Verilerin Korunması Kanunu Tasarısı (1/541) ve Adalet Komisyonu Raporu**, Sıra No.117, Yasama Dönemi.26, Yasama Yılı.1, s.5.

⁹⁶¹ Tim Harford, “Big Data: Are We Making a Big Mistake?”, Financial Times, 28.03.2014, <https://www.ft.com/content/21a6e7d8-b479-11e3-a09a-00144feabdc0> (31.12.2024); Mason Pelt, “‘Big Data’ is an Overused Buzzword and This Twitter Bot Proves It”, SiliconANGLE, 26.10.2015, <https://siliconangle.com/2015/10/26/big-data-is-an-over-used-buzzword-and-this-twitter-bot-proves-it/> (31.12.2024); Terence Craig ve Mary E. Ludloff, **Privacy and Big Data**, Sebastopol: O’Reilly Media, 2011, s.4.

⁹⁶² Craig ve Ludloff, s.4.

Büyük veri setlerinin gerçekten ne kadar isabetli sonuçlara ulaştırdığı konusu bir dönem için tartışmalı olsa da⁹⁶³ bugün sosyal ve siyasal açıdan anlamlı çıktılar sunabildiği bilinmektedir. Dahası, veriyi doğru şekilde işleyebilmek ve bunun için gerekli teknoloji ile bilgi birikimine sahip olmak, veriye sahip olmaktan da önemlidir.⁹⁶⁴ Yine de veri setlerinin ortaya çıkması için bu verilerin bir şekilde toplanması gereklidir. Hukukta kişisel verilerin toplanması adına hâkim yaklaşım, rıza esasıdır. Kendilerine ilişkin mahrem bilgileri barındıran verileri kişilerin rızaları dışında edinmenin hukuka aykırılığı kadim bir ilkedir.⁹⁶⁵ Fakat rıza temelli yaklaşımın kritik bir diğer sonucu ise kişinin rızasının varlığı halinde kendisine ilişkin hemen her tür verinin toplanması ve işlenmesinin serbest olmasıdır.⁹⁶⁶ Dolayısıyla devletler, kişilerin rızalarının sağlıklı bir zeminde teşekkül etmesi için hukuki çerçeveler oluştursalar da genellikle sorumluluğu nihayetinde kişilere yüklemişlerdir. *Solove*, mahremiyetin düzenlenmesine ilişkin bu yaklaşımı “mahremiyet özyönetimi” olarak adlandırmıştır.⁹⁶⁷ Alandaki devlet müdahalesiyle arayüzler ve bildirimler belli bir güven seviyesine gelmiş olsa da kullanıcıların genelinin veri sistemini ve ortaya çıkabilecek sonuçların çeşitlilik ve ciddiyetini kavraması hâlen oldukça güçtür. Ayrıca siber uzaydaki birçok hizmeti kullanabilmek için verilerin toplanması ve işlenmesine rıza gösterilmesi ön koşul olarak sunulmaktadır.⁹⁶⁸ Sonuç olarak mezkûr şartlarda mahremiyet özyönetiminin ne ölçüde sıhhatli bir yaklaşım olduğu tartışmaya açıktır.

Kişilerin rızasının sağlam bir temele oturduğu varsayımında dahi büyük veri, barındırdığı potansiyel itibariyle yeni sorunların odağı olacaktır. Holistik bakışla bütünün kendisini oluşturan unsurların toplamından fazla olduğu kabul edilirse, büyük veriyi sadece rızaları dahilinde kişilerden toplanmış veriler bütünü olarak görmek hatalı olacaktır. Zira büyük veri setleri, özünde sistem dahilinde dizilmiş noktalardan ibaret olan bir çizime bakıldığında kim olduğu bilinen bir insanın görülebilmesinden daha çarpıcı

⁹⁶³ Shvetank Shah, Andrew Horne ve Jaime Capellá, “Good Data Won’t Guarantee Good Decisions”, **Harvard Business Review**, Vol.90, Iss.4, (2012), ss.23-24.

⁹⁶⁴ Anja Lambrecht ve Catherine Tucker, “The 4 Mistakes Most Managers Make with Analytics”, *Harvard Business Review*, 12.07.2016, <https://hbr.org/2016/07/the-4-mistakes-most-managers-make-with-analytics> (31.12.2024).

⁹⁶⁵ İslam ıstılahındaki “tecessüs” müessesesinin kapsadığı hususlardan biri de budur; Mustafa Çağrı, “Teccessüs”, **Türkiye Diyanet Vakfı İslam Ansiklopedisi**, Cilt.40, İstanbul: Türkiye Diyanet Vakfı Yayınları, 2011, ss.246-247.

⁹⁶⁶ Daniel J. Solove, “Privacy Self-Management and the Consent Dilemma”, **Harvard Law Review**, Vol.126, Iss.7, (2013), s.1880.

⁹⁶⁷ Ibid.

⁹⁶⁸ Hatipoğlu Aydın, ss.209-210.

hikayelerin konusudur. Bilhassa GAMAM⁹⁶⁹ kısaltmasıyla anılan Google, Amazon, Meta, Apple ve Microsoft başta olmak üzere, çok geniş çapta büyük veriye ve bunu etkin biçimde işleyebilecek teknolojiye sahip şirketlerin geçmiş uygulamaları, meselenin hassasiyeti hakkında ipuçları vermektedir. Hemen her ülkeden milyonlarca kullanıcıya sahip dev şirketlerin, kullandıkları algoritmalar marifetiyle kitlelerin duygu durumlarından siyasi tercihlerine kadar birçok hususu etkileyebildikleri görülmüştür.⁹⁷⁰ O'Neil, bu algoritmik kabiliyetin kötüye kullanılmasını -“kitle imha silahı (*weapon of mass destruction*)” ifadesinden mülhem- “matematik imha silahı (*weapon of math destruction*)” olarak adlandırmıştır.⁹⁷¹ Yazar, zararlı şekilde kullanıldığına dair yeterli delil olmadığı için teknoloji şirketlerinin bilinen uygulamalarını “siyasi matematik imha silahı” olarak tavsif edemediğine fakat kötüye kullanım potansiyelinin çok yüksek olduğuna dikkat çekmiştir.⁹⁷² Ayrıca büyük verinin ayrımcılık ve sosyal çatışma doğuracak şekilde kullanılabilmesi de mümkündür.⁹⁷³ Kötüye kullanım imkanlarından oluşan zincir, nihayetinde devletlerin kamu düzenlerini ve milli güvenliklerini tehdit edecek boyutlara ulaşabilecektir. Sonuç itibarıyla devletlerin salt rızaya dayalı kişisel veri rejimini elden geçirerek, kullanıcılar için geçerli olacak kısıtlamalar, verilerin türüne göre ek şartlar, veri akışına veya depolanma miktarına dair kotalar gibi önlemlere başvurmaları gündeme gelebilir.

Devletler, veriler üzerinde yetki ileri sürebilecek olsalar da uygulamada önemli teknik güçlüklerle karşılaşacaktır. Bunların başlıcası, bulut bilişim modelidir. Verilerin çeşitli ülkelerde bulunan veri merkezleri ile sunucularda dağıtık şekilde depolanması ve işlenmesi, devletlerin yetki icrasını zorlaştırmaktadır.⁹⁷⁴ Bulut bilişime dair milletlerarası özel hukuk uyuşmazlıklarında yetkili mahkemenin tespiti adına da literatürde çeşitli fikirler ileri sürülmüş, klasik usullerle ülkesel temelde yetki tesisinin güçlüğüne dikkat çekilmiştir.⁹⁷⁵ Bulut bilişim aynı zamanda büyük veri alanındaki başat araçlardandır.

⁹⁶⁹ Facebook şirketinin ismi Meta olarak değiştirilmeden önce literatürde bilinen şekliyle GAFAM.

⁹⁷⁰ Örnekler için bkz. Cathy O'Neil, **Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy**, New York: Crown Publishing, 2016, ss.179-197.

⁹⁷¹ Ibid., s.3.

⁹⁷² Ibid., s.185.

⁹⁷³ Solon Barocas ve Andrew D. Selbst, “Big Data’s Disparate Impact”, **California Law Review**, Vol.104, No.3, (2016), s.729.

⁹⁷⁴ Kittichaisaree, ss.26-27.

⁹⁷⁵ Konu hakkında ileri sürülen görüşler ve tartışmalar için bkz. Elif Hande Altıntaş Açıkgöz, “Bulut Bilişim Sisteminde Yer Alan Verilerden Kaynaklanan Uyuşmazlıklarda Milletlerarası Yetkili Mahkemenin Tespiti Meselesi”, **Bilişim Hukuku Dergisi**, Cilt.6, Sayı.1, (2024), ss.97-125.

Buraya kadar anlatılan problemlere binaen devletler, verilerin kendi ülkeleri dışına çıkmasını ve ülke dışında depolanmasını belli şartlara tabi tutma yoluna gitmişlerdir.

Türkiye’de KVKK ile kişisel verilerin yurt dışına aktarılması için birtakım şartlar getirilmiştir.⁹⁷⁶ 5651 sayılı Kanun’da da belli nitelikteki sosyal ağ sağlayıcıların, verileri Türkiye’de barındırma yönünde gerekli tedbirleri almasına hükmedilmiştir.⁹⁷⁷ GDPR 5. Bölüm hükümleri, kişisel verilerin üçüncü ülkelere veya uluslararası örgütlere aktarımı için belli güvenlik şartlarının sağlanmasını aramaktadır.⁹⁷⁸ Çin’de, Siber Güvenlik Yasası ile Çin ülkesinde toplanan verilerin yine ülke içerisinde barındırılması şart koşulmuş, verilerin iş gereği yurt dışına aktarılması gerektiği durumlarda ilgili devlet kurumları tarafından formüle edilen önlemlere uyulması gerekliliği düzenlenmiştir.⁹⁷⁹ Ayrıca 2021 tarihli Kişisel Bilgi Koruma Yasası⁹⁸⁰ 3. Bölüm hükümleriyle Siber Güvenlik Yasası’ndaki söz konusu düzenleme detaylandırılmış; belli başlı kurumların değerlendirmelerinden geçilmesi, belli sertifika ve belgelerin edinilmesi, veri aktarımıyla ilgili bilgilendirmelerde bulunulması ve uluslararası süreçlerde ise mütakabiliyet esasının kabul edilmesi gibi hususlara hükmedilmiştir. Rusya’da da 2014 tarihinde kabul edilen ve Kişisel Verilerin Yerelleştirilmesi Yasası olarak da anılan 242 sayılı Federal Kanun da yukarıdaki hükümlere paralel şekilde, Rus vatandaşlarından toplanan verilerin Rusya’da depolanmasını ve işlenmesini bazı istisnalar dışında zaruri kılmıştır.⁹⁸¹ ABD’de ise ne doğrudan kişisel verilerin korunmasına ne de yerelleştirilmesine ilişkin bir federal yasa bulunmaktadır. Bunun yerine sağlık, eğitim, iletişim, finans gibi hizmetlerden yararlanan kullanıcılar için ayrı ayrı yasal düzenlemelerle veri gizliliği hükümleri getirilmiştir.⁹⁸²

Depolamanın ülke içinde sağlanmasını ifade eden, verileri yerelleştirilme politikaları bir yana; veri üzerindeki devlet yetkisinin verinin konumundan bağımsız olarak geçerli olduğu da kabul görmektedir. Lüksemburg ve Estonya arasındaki örnekte; Estonya devletine ilişkin verilerin Lüksemburg’da satın alınan özel bir veri merkezinde

⁹⁷⁶ KVKK, m.9.

⁹⁷⁷ 5651 sayılı Kanun, Ek m.4/6.

⁹⁷⁸ GDPR, m.44-m.50.

⁹⁷⁹ Çin Siber Güvenlik Yasası, m.37.

⁹⁸⁰ Yasanın İngilizce çevirisi için bkz. http://en.npc.gov.cn.cdurl.cn/2021-12/29/c_694559.htm (31.12.2024).

⁹⁸¹ Alexander Savelyev, “Russia’s New Personal Data Localization Regulations: A Step Forward or a Self-Imposed Sanction?”, *Computer Law & Security Review*, Vol.32, Iss.1, (2016), s.133.

⁹⁸² Konu hakkında özet bilgi için bkz. <https://www.dataguidance.com/jurisdictions/united-states-federal> (31.12.2024).

depolanmasına adına yapılan iki taraflı uluslararası antlaşma ile bu veri merkezi için diplomatik dokunulmazlıklara atıfta bulunan hükümler getirilerek bir çeşit “veri elçiliği” oluşturulmuştur.⁹⁸³ Devlete ilişkin verilerin ülke dışında depolansa da devlet egemenliği ile ilişkilendirilmesi, vatandaşlara ilişkin veriler için de benzer durumu gündeme getirecektir.⁹⁸⁴ Zira bir X Devleti vatandaşının verisinin, Y Devleti ülkesinde yahut sözgelimi açık denizdeki bir veri merkezinde veya birçok ülkedeki veri merkezleri arasında dağıtık biçimde depolanıyor olması fark etmeksizin; söz konusu veri, depolandığı yerden ziyade ilişkilendirildiği süje ile daha sıkı bağlara sahiptir. AB Komisyonu’nun da tespit ettiği üzere; “...veri depolama normalde ülkesinde veri depolanan devlet tarafından herhangi bir kontrolle sonuçlanmaz. Bu tür bir depolamaya çoğu durumda, ticari mülahazalar zemininde sağlayıcı tarafından tek başına hükmedilir”.⁹⁸⁵ Dolayısıyla genellikle veriler depolandıkları ülkede doğrudan etki doğurmadığı için ev sahibi devletin yetkisi olsa da bunları düzenlemekte gerçek bir menfaati olmayacaktır. Sonuçta ise menfaat sahibi olan devletin ve verileri ülkesinde bulunduran devletin mütedahil yetkisi doğacaktır.⁹⁸⁶ Veri yerelleştirme düzenlemeleri de var olan yetkinin uygulanabilirliğinin sağlanması adına devletlerce gerekli görülmeye devam edecektir.

Kişisel verilere dair küresel bir uluslararası antlaşmanın yokluğunda, devletlerin yukarıda görüleceği üzere son 10 yıl içerisinde hızla aldıkları pozisyonlardaki benzerlikler büyük verinin depolanması, işlenmesi ve bulut bilişimin esasları hakkında oluşacak uluslararası örf ve âdet hukukunun ayak sesleri olarak görülebilir. Başta ABD ve siber politik müttefiklerinin bu konuda mümkün olduğunca serbestiyi savunması olağan sonuçtur. Nitekim bir alanda halihazırda hakimiyet sahibi olan devletler ve hakimiyet için rekabete girmiş devletlerin farklı öğretileri savunması *Mare Liberum – Mare Clausum* çatışmasından⁹⁸⁷ bu yana uluslararası hukukun gerçeğidir. Hukukun

⁹⁸³ Bartłomiej Sierzputowski, “The Data Embassy Under Public International Law”, **International and Comparative Law Quarterly**, Vol.68, Iss.1, (2019), s.227.

⁹⁸⁴ Przemysław Roguski, “Layered Sovereignty: Adjusting Traditional Notions of Sovereignty to a Digital Environment”, Tomáš Minárik ve Diğerleri (Ed.), **11th International Conference on Cyber Conflict: Silent Battle** içinde (347-360), Tallinn: NATO CCDCOE Publications, 2019, ss.353-355.

⁹⁸⁵ European Commission, Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for Electronic Evidence in Criminal Matters, 17.04.2018, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2018:225:FIN> (31.12.2024).

⁹⁸⁶ Roguski, s.356.

⁹⁸⁷ Erdem Asıl, “Uluslararası Deniz Hukukuna Hâkim Olan İlkeler Kapsamında Kitle İmha Silahlarının Yayılmasını Engellemeye Yönelik Tedbirlerin Değerlendirilmesi”, **Adalet Dergisi**, Sayı 67, (2021), s.449.

siyasetle en içli dışlı dallarından biri olan uluslararası hukukta, güç ve menfaat dengesi arayışındaki devletlerin nihayet bir noktada mutabakata vararak bu alanda da -en azından bölgesel/kısmi nitelikte dahi olsa- belli başlı normlar üretmeleri kuvvetle muhtemel görünmektedir.

4. Finansal Teknolojiler

Fiziksel uzaydaki birçok olgu gibi finans da zaman içinde dijitalleşerek siber uzayda karşılık bulmuştur. Finansal süreçlerin uzun tarihi bir yana; 1946'da banka kartlarının, 1967'de otomatik para çekme makinelerinin (*automated teller machine* (ATM)) ve 1983'te internet bankacılığının finans alanına giriş yapmasından, yaklaşık 2 milyar insanın çevrimiçi bankacılık müşterisi olduğu günümüze gelene dek⁹⁸⁸ “dijital finans” kavramı literatürdeki önemini arttırmıştır. ATM'ler, internet bankacılığı, elektronik fon transferi sistemleri, satış noktası (*point of sale* (POS)) cihazları, kripto varlıklar ve dijital forma bürünmüş bütün finansal ürün ve hizmetler dijital finans çatısı altında değerlendirilir. Dijital finansın işlemlerini sağlayan teknolojileri ifade etmek için ise son yıllarda hızla yükselen bir popülerite ile finansal teknolojiler (fintek (*fintech*)) terimi literatüre girmiştir.⁹⁸⁹

Siber uzay gibi finans da modern dönemde küresel bir olgu haline gelmiştir. Küresel – uluslararası örtüşmesindeki açıklara⁹⁹⁰ rağmen yıllar neticesinde küresel finans, uluslararası hukuk tarafından önemli ölçüde düzenlenebilmiştir. Fakat siber uzayın finans alanına dahil olması, düzenlenmeye muhtaç yeni olguları beraberinde getirmiştir. Eldeki çalışmanın bu başlığında asli mesele, fintek unsurlarının siber uzayın mantıksal boyutuna dahil olan kısımlarının değerlendirilmesidir. Bu noktada da yetki problemi, -yukarıda İkinci Bölüm'de de değerlendirilen- *Hardy* ve *Lessig* gibi yazarların vurguladığı şekilde “gerçekten yeni” hukuki sorun oluşturan ögelerde ortaya çıkmaktadır.⁹⁹¹ Sözelimi Bankalararası Finansal Telekomünikasyon Derneği (*Society for Worldwide Interbank*

⁹⁸⁸ Türkiye Katılım Bankaları Birliği, “Katılım Bankacılığı Dijital Araştırma Raporu 2021”, <https://tkbb.org.tr/faaliyetler/yayinlar/dijital-arastirma-raporu> (31.12.2024).

⁹⁸⁹ Jan Monkiewicz ve Paweł Gołąb, “Digital Finance: Systemic Framework”, Lech Gąsiorkiewicz ve Jan Monkiewicz (ed.), **Digital Finance and the Future of the Global Financial System: Disruption and Innovation in Financial Services** içinde (13-32), London, New York: Routledge, 2023, s.26.

⁹⁹⁰ Kulick, s.560.

⁹⁹¹ Hardy, s.996; Lessig, 1995, s.1745.

Financial Telecommunication (SWIFT))⁹⁹² ağı veya Türkiye’de işleyen Elektronik Fon Transferi (EFT), Elektronik Menkul Kıymet Transferi (EMKT), Fonların Anlık ve Sürekli Transferi (FAST) gibi sistemler,⁹⁹³ dijital finans unsuru olsalar dahi esasen nakit paraya ve rezervlere dayalı bankacılık sisteminin hızlandırılması ile güvenliğinin sağlanması gibi destekleyici özellikler taşımaktadır ve hukuken sıkı sıkıya düzenlenmiştir. Dolayısıyla bu işlemlerin esaslı özelliği, doğrudan dijital yapıları değildir. Hatta bazı merkez bankaları tarafından tedavüle sokulmaya başlanan “merkez bankası dijital para birimleri (*central bank digital currency* (CBDC))”⁹⁹⁴ dahi kripto varlıklar gibi dağıtık defter teknolojisi (*distributed ledger technology* (DLT)) kullanmak yerine genellikle hesap tabanlı (*account-based*) olarak tasarlandıklarından merkezi nitelikte ve kullanıcı kimliğini hesaplarla eşleştirecek şekilde işleyeceği için halihazırda kullanımda olan nakit paranın dijital formdaki halinden pratikte farkı olmayacaktır. Yine de böyle unsurların mantıksal boyutun bir parçası olarak ilgili devletin yetkisi altında bulunduğuna değinmek gerekir. Ayrıca dijital bankacılık/finans uygulama ve Web siteleri gibi mantıksal unsurlar üzerinde de diğer uygulama ve Web sitelerine paralel biçimde devlet yetkisinden bahsedilebilir.⁹⁹⁵ “Kitle fonlaması (*crowdfunding*)”⁹⁹⁶ ve “P2P kredilendirme (*P2P lending*)”⁹⁹⁷ gibi alternatif finansman usullerine imkân veren

⁹⁹² SWIFT yapısı ve gelişim süreci hakkında bilgi için bkz. Susan V. Scott ve Markos Zachariadis, “Origins and development of SWIFT, 1973–2009”, **Business History**, Vol.54, No.3, (2012), s.462 vd.

⁹⁹³ T.C. Merkez Bankası tarafından işletilen söz konusu mutabakat sistemleri hakkında resmi bilgi için bkz. T.C. Merkez Bankası, “Elektronik Fon Transfer Sistemi – Elektronik Menkul Kıymet Transfer Sistemi – Fonların Anlık ve Sürekli Transferi (FAST) Sistemi”, <https://www.tcmb.gov.tr/wps/wcm/connect/TR/TCMB+TR/Main+Menu/Temel+Faaliyetler/Odeme+Sistemleri/Turkiyedeki+Odeme+Sistemleri/Elektronik+Fon+Transfer+%28EFT%29+Sistemi> (31.12.2024).

⁹⁹⁴ Dünya genelindeki merkez bankalarının CBDC konusundaki güncel pozisyonlarına dair bilgi için bkz. <https://www.atlanticcouncil.org/cbdctracker/> (31.12.2024).

⁹⁹⁵ Günümüzde fiziksel bir şubesi olmadan tamamen dijital enstrümanlarla faaliyet gösteren “neobank” adıyla anılan bankalar da hizmet vermektedir. Türkiye’de de Bankacılık Düzenleme ve Denetleme Kurumu’nun çıkarttığı yönetmelikle neobankların hizmet vermesine imkân tanınmıştır. Anlaşılacağı üzere neobanklar da devlet tarafından verilecek lisansa bağlı olarak özel düzenlemelere tabi şekilde faaliyet göstermektedir; Mustafa Beybur, “Şubesiz Dijital Bankacılık ve Türk Bankacılık Sektörü İçin Öneriler”, **Ankara Hacı Bayram Veli Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi**, Cilt.24, Sayı.1, (2022), s.287 vd.

⁹⁹⁶ Kitleli fonlama ile çok sayıda bağışçı tarafından yapılan nispeten küçük miktarda ödemelerle bağış arayan kişiye finansman sağlanabilmektedir; Francesco De Pascalis, “FinTech Credit Firms: Prospects and Uncertainties”, Iris H-Y Chiu ve Gudula Deipenbrock (ed.), **Routledge Handbook of Financial Technology and Law** içinde (119-137), London, New York: Routledge, 2021, ss.121-122.

⁹⁹⁷ P2P kredilendirme ile herhangi bir bankacılık hizmetine başvurulmaksızın gerçek kişiler arasında kredi ilişkisi kurulabilmektedir; Fatjon Kaja, Edoardo D Martino ve Alessio M Paces, “FinTech and the Law and Economics of Disintermediation”, Iris H-Y Chiu ve Gudula Deipenbrock (ed.), **Routledge Handbook of Financial Technology and Law** içinde (78-95), London, New York: Routledge, 2021, s.83.

uygulama ve siteler de bu kapsama dahildir. Öyle ki söz konusu unsurlara dair düzenlenmelerde asıl olan mantıksal yapı değil; yapı üzerinde gerçekleşen eylemlerdir.⁹⁹⁸

Fintek kapsamında devletin yetkisine dair en özgün ve tartışmalı alanın kripto varlıklar olduğu söylenebilir. Zira bunlar doğrudan mantıksal unsurlardır ve fiziksel uzaydaki bazı olguların kritik farklılıklarla taklidi, hatta ikamesi olarak işleyebilmektedir. Yaklaşık son 10 yılda hızla yaygınlaşan, genç ve çok çeşitli dinamiklere sahip bir teknoloji ürünü olan kripto varlıkların, kimlik gizliliği ve anonimliği fintek sahasına taşınması sonucunda; geleneksel sistemlerin aksine, kripto varlıklar ile oluşan ekonomik akışa yönelik devlet kontrolü ve müdahale enstrümanları oldukça sınırlı kalmıştır.

Kripto varlıklar, konuya dair dünyadaki en güncel hukuki düzenlemelerden olan 7518 sayılı “Sermaye Piyasası Kanununda Değişiklik Yapılmasına Dair Kanun” ile; *“dağıtık defter teknolojisi veya benzer bir teknoloji kullanılarak elektronik olarak oluşturulup saklanabilen, dijital ağlar üzerinden dağıtımı yapılan ve değer veya hak ifade edebilen gayri maddi varlıklar”* olarak tanımlanmıştır.⁹⁹⁹ Bir kripto varlık (*cryptoasset*) türü olan ve ABD Ticaret Bakanlığınca *“bir blok zinciri ağı kullanıcısından diğerine kriptografik olarak gönderilen sistem içindeki dijital bir varlık/kredi/birim”*¹⁰⁰⁰ şeklinde tanımlanan kripto para (*cryptocurrency*) ifadesi ise Türk hukukunda kasıtlı olarak kullanılmamıştır. Nitekim 2021 yılında T.C. Merkez Bankası tarafından yayımlanan “Ödemelerde Kripto Varlıkların Kullanılmamasına Dair Yönetmelik” ile kripto varlıkların doğrudan ya da dolaylı olarak ödeme için kullanılması yahut kullanılmasına yönelik hizmet sunulması yasaklanmıştır.¹⁰⁰¹ Bu hüküm, kripto varlıkların *“itibari para, kaydi para, elektronik para, ödeme aracı, menkul kıymet veya diğer sermaye piyasası aracı olarak”*¹⁰⁰² nitelendirilemeyeceğini belirten hükümle birlikte bir devlet politikasını

⁹⁹⁸ Örnek olarak Türkiye’de gerçek kişilerin P2P kredilendirme yoluyla bir menfaat karşılığında kredi vermesi mümkün değildir. Zira TCK m. 241 hükmüne göre *“kazanç elde etmek amacıyla başkasına ödünç para veren kişi”* tefecilik suçunu işlemiş sayılmaktadır. Kredilendirme işleri, 6361 sayılı Finansal Kiralama, Faktoring, Finansman ve Tasarruf Finansman Şirketleri Kanunu (R. G., 21.11.2012, Sayı.28496) m.7 hükmü uyarınca ancak faaliyet izni almış şirketlerce yapılabilmektedir. Sonuç olarak Türkiye’de faaliyet gösterecek bir P2P kredilendirme sitesi de 5651 sayılı Kanun’un m.8/A/1 hükmüne dayanılarak, suç işlenmesinin önlenmesi ve kamu düzeninin korunması gerekçesiyle erişim engeline konu edilebilecektir.

⁹⁹⁹ R. G., 02.07.2024, Sayı.32590, m.1

¹⁰⁰⁰ U.S. Department of Commerce / The National Institute of Standards and Technology Computer Security Resource Center, Cryptocurrency, Glossary, <https://csrc.nist.gov/glossary/term/cryptocurrency> (31.12.2024).

¹⁰⁰¹ R. G., 16.04.2021, Sayı.31456, m.3/2 ve m.3/3.

¹⁰⁰² Ödemelerde Kripto Varlıkların Kullanılmamasına Dair Yönetmelik, m.3/1.

ifade etmektedir. 7518 sayılı Kanun değişikliği ile bu politika kısmen yenilenmiş, “*kripto varlık alım satım, ilk satış ya da dağıtım, takas, transfer, bunların gerektirdiği saklama ve belirlenebilecek diğer işlemlerin*”¹⁰⁰³ gerçekleştirilebildiği platformların, “kripto varlık hizmet sağlayıcı” sıfatıyla belli teknik şartları sağlamaları ve Sermaye Piyasası Kurulu’ndan (SPK) izin almaları şartları dahilinde faaliyetlerine müsaade edilmiştir.¹⁰⁰⁴ Yurt dışında yerleşik platformların faaliyetlerine ilişkin hükümler ise yabancı Web sitelerinin ülkesel etkisi adına ilgi çekici kıstaslar içermektedir. Söz konusu platformların “Türkiye’de yerleşik kişilere yönelik faaliyette” bulunması, “izinsiz kripto varlık hizmet sağlayıcılığı” olarak kabul edilmiş; Türkiye’de yerleşik kişilere yönelik faaliyet kapsamı da “Türkiye’de iş yeri açılması, Türkçe internet sitesi oluşturulması, sunulan kripto varlık hizmetlerine ilişkin olarak doğrudan ve/veya Türkiye’de yerleşik kişi ya da kurumlar aracılığıyla tanıtım ve pazarlama faaliyetlerinde bulunulması” şeklinde belirlenmiştir. SPK’nın bu kapsam için ayrı kıstaslar getirme yetkisi de saklı tutulmuştur.¹⁰⁰⁵ Böylece kanun koyucunun tercihi, yabancı platformlara erişim engeli getirmek yerine bu platformların doğrudan Türkiye’yi hedef alan faaliyetlerde bulunmasını yasaklamak yönünde olmuştur.

AB’de 2023’te kabul edilen Kripto Varlık Piyasaları Tüzüğü (*The Markets in Crypto-Assets Regulation (MiCA)*)¹⁰⁰⁶ ile kripto piyasa unsurları; kripto varlık, (*crypto-asset*), varlığa dayalı token (*asset-referenced token*) ve e-para token (*e-money tokens*) şeklinde tasnife tabi tutulmuş, her biri için ayrı hukuki düzenlemeler öngörülmüştür.¹⁰⁰⁷ Bir kripto varlık olan “Bitcoin”, ABD’de Emtia ve Vadeli İşlemler Komisyonu (*Commodity Futures Trading Commission (CFTC)*) tarafından “emtia (*commodity*)” olarak kabul edilmiştir. Çin’de ise kripto varlıkların “sanal emtia” niteliğinde olduğu tanınmış fakat ticareti yasaklanmıştır.¹⁰⁰⁸

¹⁰⁰³ 7518 sayılı Kanun, m.1.

¹⁰⁰⁴ 7518 sayılı Kanun, m.3.

¹⁰⁰⁵ 7518 sayılı Kanun, m.8.

¹⁰⁰⁶ Tüzük metni için bkz. <http://data.europa.eu/eli/reg/2023/1114/2024-01-09> (31.12.2024).

¹⁰⁰⁷ MiCA, m.1.

¹⁰⁰⁸ Burada değinilen ABD ve Çin örneği dahil çeşitli devletlerin kripto varlıklara ilişkin düzenlemelerinin mukayeseli hukuk bağlamında ele alındığı çalışmada daha detaylı bilgi için bkz. İrem Akıncı, **Kripto Varlıkların Mukayeseli Hukuk Açısından İncelenmesi ve İncelemelerin Türk Hukukuna Uygulanabilirliği**, İstanbul: On İki Levha Yayıncılık, 2024, ss.61-88.

Doğrudan mantıksal yapıda olmaları bakımından siber uzayın mantıksal boyutunda bulunan kripto varlıklar, uluslararası hukuktaki klasik yetki dayanakları açısından birtakım meydan okumalar sunsa da devletler ilk şoku atlatmış görünmektedir. DLT ve bilhassa blok zincir sisteminin sağladığı imkanlara binaen kullanıcıların kendisine atfettiği değer ile anlam kazanan kripto varlıkların dolaşımında; varlığın ve cüzdanın kime ait olduğu önemsenmeksizin sadece varlığın sistem içinde bulunan cüzdandaki mevcudiyetinin teyidi ve diğer cüzdana aktarımı gerçekleşmektedir. Cüzdanın bir hukuk kişisiyle eşleşmesi yahut yapılan işlemin ülke içerisinde makul ölçüde etki doğurması ile devlet yetkisi somutlaşabilecektir. Bu bakımdan 7518 sayılı Kanun ile mezkûr varlıklar üzerinde tedbir ve haciz gibi işlem taleplerinin kripto varlık hizmet sağlayıcılar tarafından yerine getirilmesine hükmedilmesi¹⁰⁰⁹ örneğinde olduğu gibi tamamen mantıksal yapıdaki bir unsurun devletçe zaptı da mümkün hale gelmiştir. Dolayısıyla kripto varlık hizmet sağlayıcılar vasıtasıyla yapılacak işlemlerde cüzdan sahibinin kimliğinin belli olması, internet erişiminin İSS'ler üzerinden yürütülmesiyle amaç ve sonuç bakımından örtüşmektedir. Fakat tıpkı internet erişiminde kimlik gizlenmesi bir şekilde mümkün olabildiği gibi blok zincire aracısız bağlanan cüzdanlar da anonim kalabilmektedir. Cüzdan sahibinin kimliğinin tespiti ise ancak harici istihbarat ile mümkün olabilmektedir. Kripto varlıkların akışını mümkün olduğunca şirketlerin ele almasını sağlamak, devletler nezdinde bu gerekçelerle makul bir çözüm gibi görünmektedir. Zira içeriği ve trafiği takip edilemeyecek şekilde P2P veya dağıtık kayıt esasıyla gerçekleşen iletişim, devlet adına tek başına bir tehdit olarak görülebilecekken; üstüne bu iletişimin doğrudan ekonomik karşılığının olmasının, devletleri hukuki düzenlemeler yapmaya itmesi oldukça doğal bir sonuçtur. Konu hakkında devlet politikaları ve düzenlemeleri ise her an değişebilmektedir. Bunlardan eldeki çalışmada aktarılanların da kısa sürede güncelliğini yitirmesi muhtemeldir. Sonuç olarak hemen her başlıkta olduğu gibi finansal teknolojiler için de devletlerin pozisyonlarını belirlemelerini müteakip, uluslararası hukuk normlarının oluşumu ile istikrarlı bir hukuki çerçevenin kurulacağını öngörmek mümkündür.

¹⁰⁰⁹ 7518 sayılı Kanun, m.9.

II. SİBER UZAYDA SINIR ÇİZGİLERİ VE EGEMENLİK MÜCADELESİ

A. Siber Uzayda Devlet Egemenliğinin Genel Teorisi

1. Siber Vestfalyacılık

İnsanın varlığını sürdürebilmesi için, uygun vasıflarda “mekân” zorunludur. Modern dönemde mekânlar üzerinde tahakküm kurmuş otorite ise egemen devlettir.¹⁰¹⁰ Ayrıca Birinci Bölüm’de açıklandığı üzere modern devletler sisteminde devlet, meşruiyetini ulustan almakta, ulusun temsilen vücut bulmuş hali olarak diğerleriyle ilişkiler kurmaktadır. Siber uzayın ayrı bir mekân olarak kabul edilip edilmemesinden bağımsız şekilde, ulusların siber uzayla kurdukları bağımlılık ilişkisi, mekân ve devletle kurdukları bağımlılık ilişkisiyle yarışır seviyeye ulaşmıştır. Elektriğin keşfiyle başlayan süreç, neredeyse bütün hayati sistemlerin internete bağımlı olduğu ve sosyal, siyasal, ekonomik, ticari yapının büyük ölçüde dijitalleştiği bir noktaya evrilmiştir. Sistemin işleyişi haricinde, fertlerin ve toplumların siber uzay unsurlarına yönelik değişken seviyelerde psikolojik bağımlılığı da bir vakıa haline gelmiştir. Bazı Web sitelerine, dijital hizmet ve ürünlere erişebilir olmak, insanların çoğunluğu için ihtiyaç sıralamasında büyük öncelik kazanmış durumdadır. Bu durum, ulusal hukuk normlarına dayanarak birtakım yetkileri icra eden hükümetlerin iç siyasette tepki çekmesine neden olabilmektedir.¹⁰¹¹ Teknolojinin sosyal yapı, siyaset, tarih, insan davranışları vb. birçok

¹⁰¹⁰ Açık denizler, Antarktika ve dış uzay gibi istisnai mekanlardan bahsedilebilse de buralarda hem -şimdilik- tam anlamıyla hayatı idame ettirmekteki güçlük ortadadır hem devletler doğrudan egemenlik ileri süremese de ihdas edilen uluslararası hukuk rejimleri yine devlet iradesini mündemiçtir.

¹⁰¹¹ Türkiye’deki bir örnekte, çevrimiçi ödeme sistemi işleten PayPal şirketi hukuki yükümlülüklerini yerine getirmediği için “ödeme kuruluşu” lisansı alamamış ve Türkiye’deki faaliyetlerine son vermek durumunda kalmıştır; ProCompliance, “PayPal ve KVKK Değişikliği – PayPal Türkiye’ye Geri Dönüyor (Mu?)”, 15.03.2024, <https://www.procompliance.net/paypal-ve-kvkk-degisikligi-paypal-turkiyeye-geri-donuyor-mu/> (31.12.2024). Yoğun kullanılan sosyal medya platformlarında ve siyasilerin söylemlerinde, söz konusu sistemin “yasaklandığı” düşüncesiyle ortaya konulan çok sayıda eleştiriyle karşılaşabilmektedir; Sputnik Türkiye, “Kılıçdaroğlu: İktidara Gelir Gelmez PayPal Yasasını Kaldıracağız”, 13.10.2022, <https://anlatilaninotesi.com.tr/20221013/kilicdaroglu-iktidara-gelir-gelmez-paypal-yasagini-kaldiracagiz-1062286099.html> (31.12.2024); <https://eksisozluk.com/paypal-acilsin-kampanyasi--7056151> (31.12.2024); https://www.reddit.com/r/Turkey/comments/pbf0v7/paypalin_yasakli_olmasi_kadar_sacma_bir_sey_yok/ (31.12.2024).

husus üzerindeki dönüştürücü etkisi de sosyal bilimler literatürünün esaslı bir konusu haline gelmiştir.¹⁰¹²

Siber uzayın küreselleşmeyle dirsek temasını ve sosyal etkisini gören bazı devletler; siber uzaydaki olgular üzerinde yetki ileri sürmenin ötesinde, siber uzayda milli sınırlar çizerek, küresel olguyu “uluslararasılaştırma” girişimini başlatmıştır. *Demchak* ve *Dombrowski*, bu girişimi tanımlamak için 2011 yılında Siber Vestfalya kavramını önermiştir.¹⁰¹³ Vestfalyacı devlet tanımının geleneksel realist ekol tarafından özetle “ülke”, “otonomi”, “kontrol” ve “karşılıklı tanıma” esaslarına dayandırıldığını hatırlatan yazarlara göre bir devlet; kendi vatandaşlarınca erişilen siber uzayda değişiklik yapabildiği ve bu yönde hareket etme hakkını “diğer devletler için de tanıdığı” takdirde, kendi siber uzay “ülkesini” ve buradaki “otonomisini” tanımlamaya girişmiştir.¹⁰¹⁴ Siber uzayda “kontrol” ise devletin meşru kuvvet kullanma tekeli ile ilişkilendirilmiştir. Tabii ki siber uzayın soyut ve sınır aşan yapısı, geleneksel anlamda asker – polis marifetiyle sağlanan fiziksel kontrole meydan okumaktadır. Fakat devlet, alt yapı ve kurumları sayesinde kamu düzenini dahili veya harici saldırılardan proaktif olarak korumak ve failleri cezalandırmak suretiyle meşru kuvvet kullanma tekeli elinde tutabilecektir.¹⁰¹⁵ Yazarların Siber Vestfalya sisteminin kaçınılmazlığına yönelik adeta bir manifesto niteliğinde olan ifadeleri dikkat çekicidir.¹⁰¹⁶

“Çok da uzak olmayan bir gelecekte, çoğu devlet bir zamanlar yönetilmeyen, hatta kaotik olan siber uzay zemininde bir dereceye kadar savunulabilir sınırlar çizecektir. İster ezkaza ister karşılıklı ayarlamalarla ister çatışmalarla ya da her üçünün bir kombinasyonu ile olsun; devletler, Münster ve Osnabrück’ün ima ettiği sınırlı yetkilerden, modern ulus-devletin sahip olduğu tüm işlevlere doğru genişledikleri gibi, siber tehditlerin meydan okumasının da üstesinden geleceklerdir. Kendilerine gerekli yetkileri veren iç yasaları ihdas edecek, yetkili askeri ve kolluk kuvvetlerini kuracak, uluslararası antlaşmaları müzakere edecek ve hatta belki de mevcut uluslararası örgütleri devlet kontrolü lehine tadil edeceklerdir. Öncü devletler, zorlukla elde ettikleri

¹⁰¹² Belli başlı çalışma örnekleri için bkz. Concetta Metallo ve Diğerleri (ed.), **Digital Transformation and Human Behavior Innovation for People and Organisations**, Springer, 2021; Anabela Mesquita ve Chia-Wen Tsai (ed.), **Human Behavior, Psychology, and Social Interaction in the Digital Era**, Hershey: IGI Global, 2015; Merritt Roe Smith ve Leo Marx, **Does Technology Drive History?: The Dilemma of Technological Determinism**, The MIT Press, 1994.

¹⁰¹³ Chris C. Demchak ve Peter Dombrowski, “Rise of a Cybered Westphalian Age”, **Strategic Studies Quarterly**, Vol.5, No.1, (2011), s.35.

¹⁰¹⁴ Demchak ve Dombrowski, 2013, s.30.

¹⁰¹⁵ Ibid., s.31.

¹⁰¹⁶ Ibid., s.36-37.

imtiyazlarını korumak için içeride ve dışarıda yavaş ama emin adımlar atacaklardır. Bu geçişteki öngörülemez unsurlardan biri, siber uzay dünya çapında genişleyip derinleşirken Kuzey Amerika ve Avrupa dışındaki ülkelerin, artan pazar güçlerini nasıl kullanacaklarıdır. Tamamen yeni ya da mevcut organizasyonların değiştirilmiş versiyonu olması fark etmeksizin ulusal ve uluslararası hukuk normları ve kurumlar eninde sonunda üstün gelecektir. Tüm bu çıkarıcı hamleler, Siber Vestfalya sistemi ile neticelenecektir.”

Devletlerin -mekânsal bakış açısıyla- siber uzayı çitlerle çevirmesi artık klasik dönemde düşünüldüğü gibi uzak bir olasılık değildir. Hatta internet üzerinde filtreleme veya sansür uygulanması ve dahi internet erişiminin kapatılması gibi önlemleri meşrulaştıracak normlar, kamu düzeni ve milli güvenlik gerekçelerine dayandırılarak hem otoriter hem demokratik devletlerde gündeme gelebilmektedir.¹⁰¹⁷ Fakat Vestfalyacı egemenlik anlayışının modern dönemde aşınmış olduğu da aşikardır. Başta insan hakları alanında olmak üzere uluslararası normlardan kaynaklanan sınırlayıcı yükümlülükler ile belli konularda uluslararası yapılara devredilen yönetim yetkileri (devletlerce iradi olarak kabul edildiği varsayılabilir de) ve uluslararası siyasetteki güç dengelerinin doğurduğu hegemonik ilişkiler bu aşınmanın hem sebep hem sonuçlarıdır.¹⁰¹⁸

2. Siber Egemenlik

Literatürde siber uzayın düzenlemesi ve yönetimi hakkında tasarlanan modellerin çoğu Weberci ideal tiplerdir.¹⁰¹⁹ Siber uzay ile fiziksel uzayın ortaklık ve farklılıklar barındıran ilişki biçimi dahilinde bütün aktörlerce oluşan güç dengesi, ilgili konseptlerde kaçınılmaz olarak az ya da çok sapmaya sebep olmuştur. Klasik dönemdeki özerk “siber hukuk” savunucularının zamanla “küresel yönetim” düşüncesine meyletmelerine benzer şekilde, siber uzayda devlet egemenliğini savunan “siber egemenlik” doktrini de fiili gerçeklerin etkisiyle mutlak Vestfalyacı yaklaşımdan bir nebze uzaklaşıp; uluslararası iş birliği, sürdürülebilirlik, ortak menfaatler ve devletlerin egemenlik

¹⁰¹⁷ Farklı yönetim anlayışlarına sahip devletlerin internet kontrol uygulamalarını ele alan çalışma için bkz. Patricia Vargas-Leon, “Tracking Internet Shutdown Practices: Democracies and Hybrid Regimes”, Francesca Musiani ve Diğerleri (Ed.), **The Turn to Infrastructure in Internet Governance** içinde (167-188), New York: Palgrave Macmillan, 2016.

¹⁰¹⁸ Stephen D. Krasner, **Sovereignty: Organized Hypocrisy**, Princeton: Princeton University Press, 1999, ss.220-228.

¹⁰¹⁹ Coşkun San, “Toplumbilimsel Yöntem Açısından Durkheim ve Weber”, **Sosyoloji Dergisi**, Dizi.3, Sayı.21, (2010), ss.35-36.

haklarına saygı temelinde bir uluslararası hukuk inşası talebine dönüşmüştür.¹⁰²⁰ Zira “iç otorite yapıları dış aktörlerce etkilendiğinde veya belirlendiğinde Vestfalyacı egemenlik ihlal edilmiş olur”.¹⁰²¹ Siber Vestfalyacılık, genellikle internet başlığı altında süregelen, parçalanma (*fragmentation*) ve balkanizasyon olguları (yahut tehditleri) ile birlikte anılmaktadır.¹⁰²² Hatta parçalanmış interneti ifade etmek için “*splinternet*” kavramı türetilmiştir.¹⁰²³ Oysa birbirine bağlı ağların ayrılmasıyla oluşan sonuç, özünde “ağlar ağı” olan internet kavramını karşılamayacaktır.¹⁰²⁴

Çin’in başını çektiği ve literatürde bu sebeple ilgi odağı haline geldiği siber egemenlik doktrini, temelde siber uzayın devletle münasebetinde fiziksel uzaydaki herhangi bir olguya göre imtiyazlı olmadığı ve mevcut hukuk prensipleriyle siber uzayın da devletçe düzenlenebileceği düşüncesine dayanmaktadır.¹⁰²⁵ Yine “siber hukuk” tabiri nasıl zamanla tam aksi anlamda kullanılır hale geldiyse; “internet egemenliği”¹⁰²⁶ kavramı da klasik dönemde internetin istisnacılar tarafından özerk bir yapı olarak kabulünü ifade ederken, 2010’da Çin hükümetinin yayımladığı Beyaz Kitap’ta “Çin’de faaliyet gösteren tüm yabancı BİT şirketlerinin Çin yasalarına uyması ve Pekin’in gözetimine tabi olması gerektiği” anlamında kullanılmıştır.¹⁰²⁷ Çin’in siber egemenlik çıkışı, otoriter devlet uygulamalarını siber uzaya taşımak maksadını güdebilmekle birlikte; DNS yönetiminde reform talebi ve bilhassa ABD’nin siber uzaydaki fiili hakimiyetinden duyulan rahatsızlık gibi gerekçeleri de barındırmaktadır. Diğer taraftan *mare liberum* benzeri özgürlükçü siber uzay yaklaşımı, mezkûr düşüncenin hâkim olduğu 17 ve 18. yy’daki Hollandalı Birleşik Doğu Hindistan Şirketi (*Vereenigde Oost-Indische Compagnie* (VOC)) ve Britanyalı Doğu Hindistan Şirketi’ne (*East Indian Company*)

¹⁰²⁰ Bkz. yukarıda “Başlıca Devlet Pozisyonları”, “Çin”.

¹⁰²¹ Krasner, s.20.

¹⁰²² Kukkola, s.71; Zekoll, s.334; David J. Betz ve Tim Stevens, **Cyberspace and the State: Towards a Strategy for Cyber-Power**, London: Routledge, The International Institute for Strategic Studies, 2011, s.71; Stephane Couture ve Sophie Toupin, “What Does the Notion of ‘Sovereignty’ Mean When Referring to the Digital?”, **New Media & Society**, Vol.21, Iss.10, (2019), s.2313; Derek S. Reveron ve John E. Savage, **Security in the Cyber Age: An Introduction to Policy and Technology**, Cambridge: Cambridge University Press, 2023, s.195.

¹⁰²³ Reveron ve Savage, s.195.

¹⁰²⁴ Işık, s.49.

¹⁰²⁵ Griffiths, s.8; Zeng, Stevens ve Chen, s.434.

¹⁰²⁶ Olgunun halen “genç” olması hasebiyle gerek devletlerin gerek yazarların tercihleri sonucunda “internet egemenliği”, “siber egemenlik”, “siber uzay egemenliği”, “ağ egemenliği”, “dijital egemenlik”, “bilgi egemenliği” gibi ifadelerle literatürde sıklıkla rastlanmaktadır.

¹⁰²⁷ Wu, 2011, s.182.

oldukça benzeyen muktur aktörlerin “standart belirleme oligarşisine” dönüşebilmektedir.¹⁰²⁸

Çin’in siber egemenlik doktrini, 2017 yılından bakıldığında terminoloji ve içerik olarak olgunlaşmamış ve belirsizlikler içeren bir görüntü verirken¹⁰²⁹ 2021’de UNOEWG’ye sunulan pozisyon belgesinde düşüncenin ve beklentilerin daha netleştiği görülebilmektedir.¹⁰³⁰ Bu noktada *Hong* ve *Goodnight*’ın pasajı da tekrar hatırlanabilir:

“Sonuç olarak siber egemenlik, mutlak özerkliğe bir dönüşü kastetmiyor (siber küreye üyelik ilk etapta zaten Vestfalyacı egemenliği aşındırmıştır); ekonomik ve sosyal sorumlulukları yerine getirmek için gerekli olan devlet kapasitesini korumak adına uygulanabilir bir küresel yönetim seçeneği olarak öneriliyor.”

2018’de Fransa Cumhurbaşkanı *Macron*, BM çatısı altında gerçekleşen İnternet Yönetişim Forumu’ndaki (*Internet Governance Forum* (IGF)) konuşmasında kabaca iki tür internet olduğuna yönelik bir tasnif ileri sürmüştür: Bir tarafta Kaliforniya tarzı internet, diğer tarafta Çin İnterneti.¹⁰³¹ Söz konusu konuşma, özellikle veri koruma ve içeriğin düzenlenmesi adına çok taraflı ve çok paydaşlı şekilde uygun uluslararası rejimin oluşturulması temennisiyle devam etmiştir. Sonraki yıl ise yine IGF’de Almanya Federal Şansölyesi *Merkel*’in konuşması aynı istikamette olmuştur.¹⁰³²

“Dijital egemenlik benim anladığım şekliyle korumacılık ya da devlet yetkililerinin hangi bilginin yayılabileceğini söylemesi -yani sansür- anlamına gelmiyor; daha ziyade hem bireylerin hem de toplumun, dijital dönüşümü kendi belirledikleri şekilde şekillendirme kabiliyetini tanımlıyor.

...

Başka bir deyişle, olan biten üzerinde egemenliğe ihtiyacımız var. Ve eğer izolasyonizmin bir egemenlik ifadesi olmadığına, eylemlerimizi ortak bir anlayışa ve ortak değerlere dayandırmamız gerektiğine ikna

¹⁰²⁸ Kulick, s.566.

¹⁰²⁹ Zeng, Stevens ve Chen, s.436.

¹⁰³⁰ Bkz. yukarıda “Başlıca Devlet Pozisyonları”, “Çin”.

¹⁰³¹ *Macron* ayrıca ikisinin de muteber yönlerini kabul etmekle birlikte, birincisini baskın, muktur ve küresel özel aktörler tarafından yönlendirildiği için, ikincisini ise hükümet tarafından kontrol altında tutulduğu için demokratik bulmadığını ifade etmiştir; Emmanuel Macron, “IGF 2018 Speech”, IGF, 12.11.2018, <https://www.intgovforum.org/en/content/igf-2018-speech-by-french-president-emmanuel-macron> (31.12.2024).

¹⁰³² Angela Merkel, “Opening Speech the 14th Annual Meeting of the Internet Governance Forum in Berlin”, Bundesregierung, 26.11.2019, <https://www.bundesregierung.de/breg-en/service/archive/speech-by-federal-chancellor-dr-angela-merkel-opening-the-14th-annual-meeting-of-the-internet-governance-forum-in-berlin-on-26-november-2019-1701494> (31.12.2024).

olduysak; o zaman tam da bu -ortak, özgür, açık ve güvenli bir küresel internete bağlılık- aslında bir egemenlik ifadesidir.”

Siber uzayda devlet egemenliğinin tanındığı önemli bir başka kaynak da Tallin El Kitabı’dır. Çalışmada, siber uzaydaki faaliyetlerin hem zaruri olarak fiziksel bir alana ve nesnelere bağlı olduğu hem sınır aşan özelliklerinin mevcudiyetine ve yer yer egemenlik dışı alanlarda gerçekleşebiliyor olmasına rağmen hepsinin en az bir devletin yetkisine tabi süjeler tarafından icra edildiği vurgulanmıştır.¹⁰³³ Ayrıca insan hakları vurgusuyla şu ifadeye yer verilmiştir:¹⁰³⁴

“Gerçekten de devletler, egemenlik ilkesi uyarınca, kendi ülkelerinde bulunan herhangi bir siber altyapıyı; başta uluslararası insan hakları hukuku alanında olmak üzere antlaşma veya uluslararası örf ve âdet hukuku kısıtlamalarına tabi olmak kaydıyla, tamamen veya kısmen internet ile bağlantısını kesme hakkına sahiptir”

Nihayetinde siber egemenlik, genellikle doğu bloğunun otoriter rejimleriyle anılsa da Tallin El Kitabı’nda, AB düzenlemelerinde ve liderlerin beyanlarında görüleceği üzere batılı devletlerin de en azından ilkesel olarak mutabık oldukları bir kavrama dönüşmüştür.¹⁰³⁵

3. Siber Uzayda Ülkesel Egemenlik ve Kritik Altyapı

Siber uzay, modern uluslararası hukuk paradigmasının zaruri sonucu olarak devlet egemenliği ile ilişkilendirilmiştir. İlişkiyi kuran bağlar güçlendikçe de klasik dönemdeki “soyut mekân” ve “sanal gerçeklik” olgularına dayalı siber uzay tanımlarından vazgeçilmiştir. Gelgelelim gidişat bu şekilde vuku bulmasaydı dahi metaforik olarak sanal bir mekânda devletlerin egemenliğine tabi alanların mevcudiyeti tartışılabilirdi. Fakat metaforu sağlayan kıyas mekanizması doğru kurulmadığı takdirde, böyle bir yaklaşım uygulamada isabetli sonuçlar veremezdi.¹⁰³⁶ Hukukta belirliliğin sağlanması ve hükümlerin uygulamada bulacağı karşılığın etkin ve isabetli olması adına, siber uzayın mümkün olduğunca detaylı analizi ile egemenliğin boyut ve unsurlar üzerinden değerlendirilmesi tercih sebebi olmuştur. Yine de egemenliğin ülkeselliğe ve

¹⁰³³ Tallin El Kitabı, s.12.

¹⁰³⁴ Ibid., s.13.

¹⁰³⁵ Birçok devletin konu hakkındaki ulusal pozisyonuna dair bilgiler için bkz. <https://cyberlaw.ccdcoe.org/wiki/Sovereignty> (31.12.2024).

¹⁰³⁶ Bkz. dipnot.493.

uyrukluğa dayalı bir kavram olması, teoriyi kişiler dışındaki olguları ülkesellik ile ilişkilendirmeye yöneltmiştir. Sonuçta siber uzayın “bir uzay olarak” veya “ayrı bir mekân olarak” ele alınmasının yanında ülkeselleştirilmesi (*territorialisation*) gündeme gelmiştir.

Macron’un yukarıdaki tasnifinde Kaliforniya ve Çin arasında bir noktada bulunmakla beraber, egemenlik doktrinine binaen Çin’e daha yakın olan Rusya;¹⁰³⁷ bilgi uzayı adını verdiği siber uzayı jeopolitik bir yaklaşımla ele alıp, “iç bilgi uzayını” devletin ülkesel sınırlarının devamı olarak kabul etmiştir.¹⁰³⁸ Bu yaklaşım, Türkiye’nin “siber vatan”¹⁰³⁹ doktriniyle de paralellik arz etmektedir. Bu tür kavramlar ele alındığında, ilk bakışta siber uzayın nasıl ülkeselleşeceği sorusu akla gelirken; diğer taraftan siber uzay gibi bir olguyla ilişkilendirileceği zaman ülke mefhumunun nasıl anlaşılması gerektiği sorusuna da eğilme lüzumu doğacaktır.

Ülkesellik ve siber uzayın asli kesişimi fiziksel boyuttur. Siber uzayın varlığı için zaruri olan fiziksel boyutun çok büyük kısmı, devletlerin ülkelerinde bulunmaktadır. Tabii ki bu altyapı üzerinde de devlet egemenliği söz konusudur. Fakat “siber ülke” kavramının kapsamı, fiziksel altyapının ötesine geçmektedir. Ayrıca internet ve internete bağlılık olguları ile ortaya çıkan fakat gün geçtikçe bulanıklaşmakta olan çevrimiçi-çevrimdışı ayırımının da ötesindedir.¹⁰⁴⁰ Fizikselliği aşmış bir ülke düşüncesi, ilk bakışta afaki, hayali veya mistik bir varsayım gibi görülebilir. Oysa hukuken “ülke” mefhumu “toprak”, “deniz” ya da “hava” mefhumlarından farklıdır.¹⁰⁴¹ Ülke, sadece coğrafi ve fiziki bir yapı değil; aynı zamanda “egemen gücün örgütlenme biçimine” atıfta bulunması münasebetiyle hukuki ve siyasi bir yapıdır.¹⁰⁴² Diğer yandan sadece egemenliğe konu bir

¹⁰³⁷ Stadnik, s.162.

¹⁰³⁸ Hakala ve Melnychuk, s.7.

¹⁰³⁹ “Siber vatan”, Emniyet Genel Müdürlüğü Siber Suçlarla Mücadele Daire Başkanlığı’nca hazırlanan SİBERAY Sözlük’te “cyber homeland” çevirisi ile birlikte “bir ülkenin kendi siber uzay alanında sahip olduğu egemenlik haklarını ifade etmektedir” şeklinde tanımlanmıştır; Siberay Sözlük, “Siber Vatan”, <https://www.siberay.com/kurumlar/Siberay.com/SIBERAY-Sozluk.pdf> (31.12.2024). Kalkınma ajansları tarafından da aynı başlıkta siber güvenlik eğitim programları icra edilmektedir; Siber Vatan, “Kalkınma Ajansları Siber Vatan Programı”, <https://www.sibervatan.org/kalkinma-ajanslari-sibervatan-programi> (31.12.2024); T.C. Cumhurbaşkanlığı İletişim Başkanlığı, “Siber Vatan Koruyucuları Sertifikalarını Aldı”, 30.07.2024, https://www.iletisim.gov.tr/turkce/yerel_basin/detay/siber-vatan-koruyuculari-sertifikalarini-al-di (31.12.2024).

¹⁰⁴⁰ Lambach, s.9.

¹⁰⁴¹ Bkz. dipnot.310.

¹⁰⁴² Nicholas Tsagourias, “The Legal Status of Cyberspace: Sovereignty Redux?”, Nicholas Tsagourias ve Russell Buchan (ed.), **Research Handbook on International Law and Cyberspace** içinde (9-31), Cheltenham: Edward Elgar Publishing, 2021, s.13.

nesne değil; aynı zamanda devlet iktidarının ve bağımsızlığının tezahür ettiği bir mekânsal çerçeve olarak değerlendirilmelidir.¹⁰⁴³ Ülkenin “*toplumsal yaşamın gerçekleştiği donmuş bir çerçeve*” olarak görülmesi politik coğrafya açısından da hatalı olacaktır.¹⁰⁴⁴ Sonuçta fiziki mekanlar ancak insan eylemlerine muhatap olduğunda ülkeye dönüşebilir. Dış uzaydaki bir gezegen yüzeyinin “henüz” ülke olarak kabul edilememesi, Dış Uzay Antlaşması ile ihdas edilen hukuki rejim ile birlikte bu vakıanın da bir sonucudur.¹⁰⁴⁵ Diğer yandan -modern devlet özelliklerinden- sınırları kesin olarak çizilmiş ülkelerin uluslararası sistemde yerleşik hale gelmesi 20. yy’ı bulmuştur. Zira asırlar boyunca siyasal iktidar yapıları için asıl olan, sınır çizgilerinden ziyade insanlar ve yerleşimler üzerinde sahip oldukları kontrol olmuştur.¹⁰⁴⁶ Elbette bu hususlar, ülke mefhumunun fiziki unsurların ötesini ifade etmesi gibi iddialı bir düşünce için kesin deliller sunmasa da ülke için fiziki mekân ve üzerindeki kontrolün ötesinde sosyal süreçlerin de belirleyici olduğuna işaret etmektedir. Siber uzayda ülkesel egemenlik de sadece ülkede bulunan kablo, cihaz vs. unsurlar değil; devlet ülkesinden tamamen bağımsız olarak sosyal ve işlevsel karşılıklarından ötürü veriler, mantıksal unsurlar ve bunlarla ilgili trafik için de geçerli olacaktır.¹⁰⁴⁷ Nitekim ülke üzerindeki egemenliğin temel önermesi, devlet için dış müdahaleden korunan ve düzenlenebilir bir bağlam oluşturmaktır.

Rusya’da “dijital egemenlik” bağlamında kullanılan “siber uzayın Rus ulusal segmenti” tabiri,¹⁰⁴⁸ siber uzayın ülkeselleştirilmesini temsil etmektedir. *Kukkola* ve *Ristolainen*, Rus doktrininde ülkesel egemenliğin mahiyetine dair *Bukharin*’in ve

¹⁰⁴³ Roguski, s.350.

¹⁰⁴⁴ Hukuk bağlamında böyle bir özellik zaruri olmasa da mezkûr bağlamda ülke, “*sosyal eylemlerin ve sosyal alanların ayrılmaz bütünlüğüyle oluşan sosyal süreçleri*” ifade eder; Anssi Paasi, “Territory”, John Agnew, Katharyne Mitchell ve Gerard Toal (Ed.), *A Companion to Political Geography* içinde (109-122), Malden, Oxford, Victoria: Blackwell Publishing, 2003, s.110.

¹⁰⁴⁵ *Bilsel*, “hava uzayının” serbesti durumundan çıkıp egemenliğe konu olmuş halini “hava ülkesi” olarak adlandırmıştır. Bu yaklaşım, bir uzayın ülkeye dönüşmesini ifade eden önemli bir terminolojik örnektir; Cemil Bilsel, *Milletlerarası Hava Hukuku*, Cilt.1, İstanbul: İstanbul Üniversitesi Yayınları, 1948, ss.139-146.

¹⁰⁴⁶ Paasi, ss.114-115.

¹⁰⁴⁷ Örnek olarak; kamu kurum ve kuruluşlarının kendi siber altyapılarını işletmesi yerine -birçok devlette halihazırda uygulanan- ticari bulut bilişim hizmet sağlayıcılardan hizmet alması usulüne geçiş, Türkiye’de de “Kamu Bulut Bilişim Stratejisi” bağlamında planlanmaktadır; konuya dair genel bilgi ile Türkiye’deki mevcut durumun analizi hakkında ve diğer devlet uygulamaları hakkında raporlar için bkz. T.C. Cumhurbaşkanlığı Dijital Dönüşüm Ofisi, “Kamu Bulut Bilişim Stratejisi”, <https://cbddo.gov.tr/bulut-bilisim-stratejisi/> (31.12.2024). Kamu hizmetlerinin özelleşmiş altyapılarda icra edilmesi halinde; altyapının fiziksel konumundan ziyade, altyapı üzerinde işleyen mantıksal boyut, devletle ilişki biçimi açısından egemenliğin esaslı konusu haline gelecektir.

¹⁰⁴⁸ Kukkola ve Ristolainen, s.84.

Efremov'un görüşlerini aktarmıştır.¹⁰⁴⁹ *Bukharin*, egemenliği devletin teknik kabiliyetlerine bağlamıştır. Bu bağlamda Rus dijital egemenliğinin teknik bileşenlerini “*arama motorları, sosyal medya, yerli işletim sistemleri ve yazılımlar, mikroelektronikler, ağ bağlantısı ekipmanı, internetin ulusal segmenti, ödeme sistemleri, öz müdafaa, kriptografik algoritmalar ve protokoller, navigasyon sistemleri*” şeklinde on kalemde saymıştır.¹⁰⁵⁰ *Efremov* da benzer yaklaşımla ülkesel egemenliğin bilgi uzayına uygulanmasında kilit konunun, devletin bilgi bağlantılarını düzenleme kabiliyeti olduğunu; bilgi uzayına geçerken fiziksel ülkeye göre egemenliğin azabileceğini fakat egemenlik tanımında ülkeselden işlevsele doğru bir dönüşümün de söz konusu olacağını ileri sürmüştür.¹⁰⁵¹

Yukarıdaki görüşlerden hareketle, Rusya özelindeki siber ülke yaklaşımının, fiziksel ve mantıksal yapıların birlikte ele alınarak kontrol kabiliyetinin sağlanması ve dış müdahalelerden korunması öğretisine dayandığı söylenebilir. Yaklaşık olarak bu kompozisyon, uluslararası hukuk sahasına “kritik altyapı” ya da “kritik bilgi altyapısı” tabiriyle girmiştir. En genel haliyle kritik altyapı, “*temel bir hizmetin sağlanması için gerekli olan bir varlık, tesis, ekipman, ağ veya sistem ya da bir varlığın, tesisin, ekipmanın, ağın veya sistemin bir parçası*”¹⁰⁵² veya “*hayati toplumsal işlevlerin sürdürülmesi için elzem olan varlık veya sistem*”¹⁰⁵³ şeklinde tanımlanır. UNOEWG raporuyla tespit edildiği üzere bunlar arasında tıbbi tesisler, finansal hizmetler, enerji, su, ulaşım ve sanitasyon yer alabilir; fakat hangi altyapıların “kritik” olarak belirleneceği konusunda kesin bir uluslararası düzenleme bulunmadığı için bu tespit devletlerin inisiyatifine bırakılmıştır. Kritik altyapılara karşı gerçekleştirilen zararlı BİT faaliyetlerinin de siyasete, seçimlere ve kamu kurumlarına duyulan inanç ve güveni sarsmasına veya internetin işleyiş ve erişilebilirliğine darbe vurmasına vurgu yapılarak, konunun devletler için önemi ifade edilmiştir.¹⁰⁵⁴ Kritik altyapıların çoğu özel sektöre

¹⁰⁴⁹ Ibid., s.87.

¹⁰⁵⁰ Ibid.

¹⁰⁵¹ Ibid.

¹⁰⁵² Kritik Varlıkların Dayanıklılığı Hakkında AB Direktifi (*Directive on the Resilience of Critical Entities*), m.2/4; Direktif metni için bkz. <http://data.europa.eu/eli/dir/2022/2557/oj> (31.12.2024).

¹⁰⁵³ Livinus Obiora Nweke ve Stephen D. Wolthusen, “A Holistic Approach for Enhancing Critical Infrastructure Protection: Research Agenda”, Jemal H. Abawajy, Kim-Kwang Raymond Choo ve Haruna Chiroma (Ed.), **International Conference on Emerging Applications and Technologies for Industry 4.0 (EATI'2020)** içinde (220-228), Cham: Springer, 2021, s.221.

¹⁰⁵⁴ A/75/816, s.8, para.18.

aittir. Batılı devletlerde sahiplik oranının %80'e yakın olduğu belirtilmiştir.¹⁰⁵⁵ Dolayısıyla kritik altyapıların korunması adına devletler ve özel sektör arasında iş birliği çoğu zaman zaruridir. Buna binaen 2009 yılında, ABD Başkanı Yürütme Ofisi (*Executive Office of the President of the United States*) tarafından “dijital altyapı”, hükümet ve özel sektörce korunması gereken “stratejik ulusal varlık” olarak ilan etmiştir.¹⁰⁵⁶

Devletler, kritik altyapılarını belirleyip ilan etmekte; bunların hem fiziksel hem siber saldırılardan korunması adına politikalar üretmektedir. Enerji, BİT, ulaşım, ekonomi/finans, kamu hizmetleri, sağlık, su, besin, milli güvenlik, eğitim gibi sektörlerle ilişkin altyapılar devletlerce genel olarak kritik sayılmaktadır.¹⁰⁵⁷ Kritik altyapı kapsamındaki sistem ve varlıklar fiziksel veya sanal olabilir.¹⁰⁵⁸ Kritik altyapıların fiziksel olarak korunması, terörle mücadele ve milli güvenlik bağlamında ele alınırken; siber saldırılara karşı korunması, siber güvenlik politikalarının konusunu oluşturmuştur.¹⁰⁵⁹ Kritik altyapının siber uzayda ülkesel egemenlik açısından ehemmiyeti burada ortaya çıkmaktadır. Devletlerin fiziksel ve mantıksal yapıyı birlikte ele alarak “kendi siber uzaylarını”¹⁰⁶⁰ koruma girişimleri, kritik altyapı ve özel olarak kritik bilgi altyapısı üzerine odaklanmıştır. Siber ülkenin, tıpkı fiziksel ülke gibi, başat egemenlik

¹⁰⁵⁵ United Nations Security Council / Counter-Terrorism Committee Executive Directorate (CTED), “Physical Protection of Critical Infrastructure Against Terrorist Attacks”, *CTED Trends Report*, 2017, s.2.

¹⁰⁵⁶ Vargas-Leon, s.180.

¹⁰⁵⁷ 2023 sonu itibariyle devletlerin kritik altyapı belirlemelerine ilişkin istatistik çalışması için bkz. Valentin Weber, Maria Pericás Riera ve Emma Laumann, “Mapping the World’s Critical Infrastructure Sectors”, *DGAP Policy Brief*, No.35, (2023).

¹⁰⁵⁸ US White House, “Improving Critical Infrastructure Cybersecurity”, Executive Order, 12.02.2013, Section.2.

¹⁰⁵⁹ Türkiye’de Ulaştırma ve Altyapı Bakanlığı ve Cumhurbaşkanlığı Dijital Dönüşüm Ofisi Siber Güvenlik Dairesi Başkanlığı, ABD’de İç Güvenlik Bakanlığı (*Department of Homeland Security*) ile Siber Güvenlik ve Altyapı Güvenlik Ajansı (*Cybersecurity and Infrastructure Security Agency*), Çin’de Siber Uzay İdaresi (*Cyberspace Administration of China*), Rusya’da Federal Güvenlik Servisi (FSB) bünyesindeki Ulusal Bilgisayar Olayları Müdahale ve Koordinasyon Merkezi (NCIRC) gibi kurumlar söz konusu işlevi yürüten örneklerdir. İlgili kurumların kritik altyapılar üzerindeki işlevleri hakkında sırasıyla bkz. T.C. Ulaştırma ve Altyapı Bakanlığı Haberleşme Genel Müdürlüğü, “Siber Güvenlik”, T.C. Ulaştırma ve Altyapı Bakanlığı Haberleşme Genel Müdürlüğü, “Siber Güvenlik”, <https://hgm.uab.gov.tr/siber-guvenlik> (31.12.2024); T.C. Cumhurbaşkanlığı Dijital Dönüşüm Ofisi, “Siber Güvenlik Dairesi Başkanlığı”, <https://cbddo.gov.tr/hizmet-birimlerimiz/siber-guvenlik-dairesi-baskanligi/> (31.12.2024); Cybersecurity and Infrastructure Security Agency, “Homeland Security Presidential Directive 7”, <https://www.cisa.gov/news-events/directives/homeland-security-presidential-directive-7> (31.12.2024), Cybersecurity and Infrastructure Security Agency, “Critical Infrastructure Security and Resilience”, <https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience> (31.12.2024); Cyberspace Administration of China, “Cyberspace Administration of China Launches the Initiative on China-Africa Jointly Building a Community with a Shared Future in Cyberspace”, 25.08.2021, https://www.cac.gov.cn/2021-08/25/c_1631480920680924.htm (31.12.2024), National Computer Incident Response and Coordination Center, <https://cert.gov.ru/en/> (31.12.2024). Siber güvenlik bağlamında Çin, Rusya, ABD ve AB’nin güncel terminolojik ve kurumsal yaklaşımlarına dair mukayeseli çalışma için ayrıca bkz. Lora Saalman, Fei Su ve Larisa Saveleva Dovgal, *Cyber Risk Reduction in China, Russia, the United States and the European Union*, Solna: Stockholm International Peace Research Institute (SIPRI), 2024.

¹⁰⁶⁰ Çekya Siber Güvenlik Yasası’ndaki “Çek Siber Uzayı” tabirinin kritik altyapıyla ilişkilendirilmesi örneği hakkında bkz. Svantesson, ss.29-30.

unsurlarından olan milli güvenliğin bir konusu haline geldiği böylece görülecektir. NATO'nun siber uzayı kara, hava ve deniz gibi savunulması gereken bir harekât alanı olarak kabul etmesi de vakıanın bir başka yansımasıdır.¹⁰⁶¹

4. Siber Uzayda Egemenliğe Karşı “Ortak Mal” Yaklaşımı

Teori ve pratikteki gidişat -*Demchak* ve *Dombrowski*'nin öngörüsü kadar keskin olmasa da- devlet egemenliği lehine ilerlerken diğer yandan muhalif görüşler de dile getirilmektedir. Siber uzay hukukunda önemli köşe taşlarından olan “karşı (*against*)” başlıklı metinlerin bir örneği de alanın önde gelen küresel yönetim yanlısı yazarlarından *Mueller* tarafından bu minvalde kaleme alınmıştır.¹⁰⁶² Yaklaşık 30 yıldır süregelen literatür tartışmasına dahil olan söz konusu çalışma, siber uzayda egemenlik karşıtı cephenin en güncel ve kuvvetli argümanlara sahip temsilcilerindendir. “Vestfalyacı” ifadesini tuhaf bulan yazar, bunun aslında “siber uzayda devlet egemenliğine dayalı rejim” anlamına geldiğini ifade ettiği eserinde; son dönemde gittikçe güç kazanan egemenlik yanlısı görüşlere karşı, siber uzayın küresel bir ortak mal (*global common*) olduğunu savunmuştur.¹⁰⁶³ Öncelikle yazarın siber uzaydan bahsederken aslında “internet” olgusunu merkeze aldığını belirtmek gerekir. *Mueller*, siber uzayı ele alırken mantıksal boyuta -özellikle de standart ve protokollere- ağırlık vermiş; bu haliyle küresel bir alan olarak kabul ettiği siber uzayın, klasik egemenlik yaklaşımında geçerli olan ülkesellik ve otoriteyi tek potada eritmeye müsait olmadığını ileri sürmüştür.¹⁰⁶⁴ Nitekim siber uzayın işlerliğini sağlayan standart ve protokoller devletlerin egemenlik alanlarının dışında belirlenmektedir ve kimseye ait değildir. Siber uzay tabii ki doğal bir olgu değildir, insanlarca inşa edilmiştir. Fakat bu ayrımın aslında bir önemi olmadığını savunan *Mueller*,¹⁰⁶⁵ inşa sürecinin devlet dışı işleyerek siber uzayı “zuhur eden bir fenomen” haline getirdiğinden bahisle; öncelikle siber uzayın bu haliyle hızla genişleyip

¹⁰⁶¹ NATO, “Warsaw Summit Communiqué”, 09.07.2016, https://www.nato.int/cps/en/natohq/official_texts_133169.htm (31.12.2024).

¹⁰⁶² Söz konusu çalışma, yukarıda da atıfta bulunulmuş olan “Against Cyberanarchy” (Goldsmith) ve “Against Cyberlaw” (Sommer) başlıklı eserler ile aynı konuda aynı kalıbı kullanmaktadır; Milton L. Mueller, “Against Sovereignty in Cyberspace”, *International Studies Review*, Vol.22, Iss.4, (2020), s.1 vd.

¹⁰⁶³ Mueller, 2020, ss.1-2; Bu düşünce, önceki yıllarda da kurumlar ve yazarlar tarafından çokça dile getirilmiştir; Menthe, ss.83-91, Patrick W. Franzese, “Sovereignty in Cyberspace: Can It Exist?”, *The Air Force Law Review*, Vol.64, (2009), s.14; *Mueller*'in çalışması, küresel ortak mal yaklaşımının başarılı bir temsilcisi olarak hususen incelenebilir.

¹⁰⁶⁴ Ibid., s.2.

¹⁰⁶⁵ Ibid., s.18.

küresel sisteme yerleştiğini ve devletlerin bunu fark ettiklerinde artık çok geç olduğunu ifade etmiştir. Devamında da siber uzayın doğuşundan bu yana ülkesinde neşvünema bulduğu ABD'nin hem liberal politikalar hem Amerikan firmalarının alandaki hakimiyetinden duyduğu memnuniyet gereği, siber uzayın söz konusu şekliyle sisteme entegre olmasının yolunun açıldığını belirtmiştir.¹⁰⁶⁶ Diğer taraftan internet bir “ağlar ağıdır” ve yazar, interneti oluşturan birbirine bağlı altmış binden fazla özel mülkiyete tabi ağ (otonom sistemler) üzerinde yaklaşık iki yüz devletin ayrı ayrı egemenlik ileri sürmesini de makul ve mümkün görmemektedir.¹⁰⁶⁷ Mueller'in bir argümanı da meşru kuvvet kullanma tekelinin siber uzayda bulunmadığı yönündedir. Zira kuvvet kullanma tekeli en başta fiili kabiliyet gerektirmektedir ve yazara göre devletleri devlet dışı aktörlerin üstünde konumlandırabilecek bir siber kapasite söz konusu değildir. Böyle bir kapasitenin varlığı kabul edilse dahi kapasiteyi ve kullanıldığında doğacak etkiyi ülkesel olarak sınırlamak mümkün değildir.¹⁰⁶⁸

Mueller, fiili duruma yönelik olanların yanı sıra ilkesel ve ideolojik eleştirilerde de bulunmuştur. Egemenlikçilerin aslında 19 ve 20. yy'da hâkim sistem olan ve elverişsizliği sebebiyle terk edilen posta, telefon, telgraf (PTT) tekellerine dönüşü kastettiği;¹⁰⁶⁹ siber uzayın bütün halinde küresel yönetişimi gibi uygulanagelen ve iş birliğine dayalı bir sistem yerine, çoğu çatışma durumundaki 200 civarı devletin yönetimine dayalı ve bölünmeye sebep olacak bir sisteme geçilmesinin makul olmadığı;¹⁰⁷⁰ milli egemenliğin uyumluluk ve küresel erişimden daha önemli kabul

¹⁰⁶⁶ Ibid., ss.15-16.

¹⁰⁶⁷ Ibid., ss.13-14.

¹⁰⁶⁸ Ibid., s.12-13. Yazar, ülkesel egemenlik iddialarının paradoksal olarak sınır aşan etkiler doğuracağı yönündeki düşüncesini şu örnekle açıklamıştır: “Buna bir örnek olarak Fransa'nın “unutulma hakkını” tesis etme girişimi verilebilir; bu hak muhtemelen ABD'de anayasaya aykırı bulunacak ve diğer pek çok yargı mercii tarafından tanınmayacaktır. Bu sözde hakkın pratikte uygulanması, Google'ın küresel arama sonuçlarının, sözde unutulma hakkını ihlal eden bilgi kaynaklarına yönelik tüm arama sonucu listelemelerinin bağlantısını kaldırarak şekilde düzenlenmesi gerektiği anlamına gelmektedir. Eğer Fransa egemen modele dar bir şekilde bağlı kalır ve sadece Fransa'nın google.fr alan adındaki arama sonuçlarını düzenlerse, Fransız kullanıcıların bunun yerine google.com'u kullanarak düzenlemeleri aşması kolaydır. Google, hizmetlerini Fransız internet servis sağlayıcılarına tahsis edilen IP adreslerini tanıyacak şekilde yapılandırır bu aşma imkânı daraltılabilir; ancak Fransız vatandaşları sanal özel ağ kullanırsa veya ağa başka ülkelerden erişirse bu mekanizmalar aşılabılır. Dolayısıyla Fransa, arama sonuçları üzerindeki yargı yetkisini tam olarak uygulamak istiyorsa ya Google'ı tamamen engellemeli ya da VPN'leri engellemelidir ki her iki durumda da önemli ve faydalı internet kabiliyetleri sekteye uğrar. Diğer seçenek ise küresel şirkete para cezaları ya da başka cezalar uygulayarak arama sonuçlarını küresel olarak kaldırmaya Google'ı zorlamaktır. Fransa'nın yapmaya çalıştığı bu seçenek (Schwartz 2018), Fransa politikasını ve yetkisini dünyanın geri kalanına dayatacağıdır ki bu da egemenlik ilkesinden açık bir sapmadır. Siber faaliyetlerin karşılıklı bağımlılığı nedeniyle, siber uzayda egemenlik dayatma çabalarının ülkesel yetki ve ülke dışı etkilerle ilgili bu tür birçok paradoksla karşılaşması muhtemeldir.”;

Ibid., s.19.

¹⁰⁶⁹ Ibid., s.15.

¹⁰⁷⁰ Ibid., s.14.

edilmesi durumunda, halihazırda ortak mal olan standart ve protokollerin de millileştirilmesiyle yeknesaklığın kaybolabileceği¹⁰⁷¹ gibi görüşleri bu kapsamdadır.

Mueller'in önerisi, siber uzayı küresel bir ortak mal olarak kabul edip yönetim usullerini geliştirmektir.¹⁰⁷² Siber uzay, literatürde çokça kıyaslandığı üzere açık denizler ve dış uzay gibi egemenliğe istisna teşkil eden alanlara benzer statüde değerlendirilmelidir. Devletler, gemiler ve uzay araçları üzerinde egemen olsalar da açık deniz ve dış uzay üzerinde egemen değillerdir. Dolayısıyla bu alanlara hangi araçların girdiği ve neler yaptığı konusunda kontrol yetkileri yoktur.¹⁰⁷³ Devlet dışı aktörlerin de yönetime dahil olduğu ve devletlerin bu bakımdan bir üstünlüğünün olmadığı¹⁰⁷⁴ yönetim modeli, küresel ortak alanın rejimi olacaktır.

Sonuç olarak *Mueller*, ortak alan düşüncesinin siber güvenlik ve siber suç gibi sorunları çözeceğini iddia etmemekte fakat bunun, egemenlik dayatmanın oluşturacağı çatışma ortamından ve yönetim problemlerinden daha iyi bir fikir olduğunu ileri sürmektedir. Nihai kanaatini ise şöyle açıklamıştır:¹⁰⁷⁵

“İdeal olarak, fiziksel dünyada egemenliğin karşılıklı tanınması, her devlete meşru kuvvet kullanma tekeli icra edebileceği rekabetsiz bir alan tahsis ederek çatışmayı sınırlandırır. Organize ikiyüzlülüğe rağmen, egemenlik ilkesi bazen çatışmadan kaçınmaya ve uyumsuzlukları bu şekilde çözmeye yardımcı olabilir. Ancak internet protokollerinin birincil işlevi; teknolojiler, medya ve ülkeler arasında uyumluluğu ve bilgi alışverişini kolaylaştırmaktır. Bilgi ve iletişim sektörüne yeni bir karşılıklı bağımlılık egemenliği tanımı yazılmaktadır. Bu da ülkesel egemenlik iddialarını, düzenden ziyade bir çatışma kaynağı haline getirir. Hukuka dönüşmesi halinde, bu tür iddialar siber uzayın temelden yeniden düzenlenmesine yol açacak ve kamu güvenliğine çok az katkıda bulunan engeller oluşturacaktır. Küresel uyumlu bir internete sahip olabiliriz ya da dijital teknolojiyi siyasi sınırlarla uyumlu hale getirmeye çalışabiliriz. İkisini birden yapamayız.”

¹⁰⁷¹ Ibid., s.16.

¹⁰⁷² Ibid., s.2.

¹⁰⁷³ Ibid., s.12.

¹⁰⁷⁴ Ibid., s.18.

¹⁰⁷⁵ Ibid., s.20.

5. Genel Değerlendirmeler

Devletin siber uzayın boyut ve unsurları üzerinde düzenleme, icra ve yargı yetkisine sahip olması, çoğu durumda ortak ve mütedahil yetki senaryolarını doğurmaktadır. Teorideki devlet yetkilerinin pratikteki karşılığı, fiziksel uzaydaki devlet egemenliğine dayalı uluslararası sistemin yapısal özellikleriyle sınırlanmaktadır. Böylece devletler adına ortaya çıkan sonuç, *Mueller* tarafından aşağıdaki gibi yorumlanmıştır.¹⁰⁷⁶

“(Devletler) Sadece otoritelerine tabi olan insanların -veya şeylerin- küresel siber uzaya erişim şeklini düzenleyebilirler. Üstün kontrol uyguladıkları bir "ulusal siber uzay" yoktur; bunun yerine, paylaşılan bir küresel siber uzay vardır ve kendi ülkelerindeki aktörler ve fiziksel cihazlar üzerindeki egemenliklerini, belirli sitelere veya uygulamalara olan bağlantıları -kusurlu ve sınırlı bir şekilde- kısıtlamak için kullanırlar.”

Devletin siber uzay ile hukuki münasebetindeki konumunu fiili duruma göre yorumlamak, sıklıkla tercih edilen yöntemdir. Bilhassa yetkinin icra edilmesinden bahsedildiğinde, devletlerin siber kapasitelerinin belirleyici faktör olduğu görülmektedir. Fakat kapasite dahilinde ortaya çıkan fiili durumun her şartta meşru olduğu düşünülemez. Bazıları yönetim biçimlerine ve ideolojik pozisyonlarına göre değişkenlik gösterebilse de devletlerin korunması gereken çok sayıda maddi ve manevi menfaatleri vardır. Menfaatlerini uluslararası hukukta devlet egemenliğine hâkim ilkeler çerçevesinde müdafaa etmek her devletin hakkıdır.¹⁰⁷⁷ Hükümetlerin bu amaca hizmet edecek doktrinler geliştirme ve siber kabiliyetlere erişme mücadelesi sürmektedir. Siber uzayda egemenliğe ilişkin devlet iddiaları da aynı kapsam dahilindedir. Tartışmanın özü buradadır.

Çocuk istismarı, yasadışı kumar, korsan yayın, dezenformasyon, soykırımın ya da terörün övülmesi/propagandasının yapılması, ülkedeki kritik tesislere zarar verilmesi, vatandaşların sağlık verilerinin çalınması, egemenlik alametlerine saygısızlık, rekabet halinde olunan bir devlete karşı dezavantajlı konuma düşülmesi, ülke içindeki muhalif grupların güç kazanması gibi sayısız olgu, devletler ve hükümetler için mücadele konusu olabilir. Bunların bazıları tamamen siber uzaya özgü ve “yeni” iken; bazıları siber uzayda

¹⁰⁷⁶ Ibid., s.12.

¹⁰⁷⁷ Bkz. yukarıda, “Modern Uluslararası Hukukta Devlet Egemenliğine Hâkim İlkeler”.

da karşılığı görülebilen, fiziksel uzayda yerleşik hale gelmiş meseleler olabilir. Bazıları hukuki, bazıları siyasi saiklere dayanabilir. Bazılarının etkisi münhasıran ülke içinde kalırken, bazıları diğer devletleri de etkileyebilir. Bu ayrımlar alt başlıklarda müspet veya menfi anlam kazanmakla birlikte genel olarak devletlerin iç ve dış egemenlik iddialarıyla ilişkilendirilir. Dolayısıyla bütünü ifade edecek teori “siber uzayda devlet egemenliği” başlığı ile anılmıştır.

Devletlerin siber uzayda egemenlik taleplerini Vestfalyacılık fikrine indirgemek, modası geçmiş bir anlayışa atıfla, bugün bilinen siber uzayın bölünerek yok olacağına yönelik korku uyandırmak demektir. İdeal tip ifade eden tüm modellerde olduğu gibi egemenlik modelleri de tarihte hep sapmalarla var olmuştur. Uluslararası ilişkilerin hiyerarşik olmayan yapısı ve asimetrik güç dengesi hem Vestfalyacı hem modern anlamda egemenliği “organize ikiye bölünme” konusu haline getirmiştir.¹⁰⁷⁸ Fakat sistemli şekilde ihlal ediliyor ve klasik karşılığından uzaklaşmış olsa da devlet egemenliğinin yok sayılması söz konusu değildir. Teknolojinin gelişmişlik düzeyinin ve değişim hızının siber uzaydaki bütün süjeler için sayısız seçenek sunması da genellikle egemenlik aleyhine görülür. Oysa teknoloji, kapasite sahibi devletler için tarihte görülmemiş ölçüde kontrolü ve cebir tekeli elde etme imkânı da sunmaktadır.

Siber uzayda devletin egemenlik iddialarına konu olan bütün unsurları ayrı ayrı noktalar halinde değerlendirmek analiz yönteminde isabet oranını arttıracak olsa dahi holistik yaklaşımla noktaları birleştirip anlamlı bir gövde oluşturmak da tercih edilebilir. Siber uzayın ayrı bir mekân olarak ele alınıp, bu mekândaki egemenliğe tabi bölümlerin tespitine dayalı yöntem bir yana; mezkûr noktaların birleştirilmesiyle oluşan gövdeyi mekânsal terminolojiyle değerlendirmek de mümkündür. Zira egemenliği mekândan bağımsız düşünmek, kurulacak teoriyi dağınık ve afaki gösterebilir. Yoksa *Efremov*’un yukarıda aktarılan görüşünde işaret ettiği gibi mekândan ziyade işleve dayalı yaklaşıma geçiş de muteberdir. Egemenliğe konu olması itibarıyla mekân metaforu kullanılacak olduğundaysa “alan”, “bölge” ve tabii ki “ülke” kavramlarının gündeme gelmesi doğal sonuçtur. Fakat son tahlilde siber uzayda egemenliği “ülkesel egemenlik” ya da “siber

¹⁰⁷⁸ Krasner, ss.40-41.

ülke” kavramları altında değerlendirmek ancak nominal fayda sağlayacaktır. Ayrıca bu noktada Tsagourias’ın da tespitleri de önemlidir.¹⁰⁷⁹

“Ülke, egemenliğin bir yönü olsa da ve egemenlik tarafından korunsa da egemenlikle eşanlamı değildir. Egemenliğin bir kabıdır; ancak egemenlik, otorite ve güç olarak ülkenin ötesine uzanabilir. Başka bir deyişle, egemenlik hem ülkeseldir hem değildir. İkinci durumda, egemenliğin kapsamı ve getirilen sınırlamalar ülkeyle değil; egemenliğin kendisiyle ilişkilidir. Bu nedenle bu bölümde ‘ülkesel egemenlik’ yerine ‘egemenlik ilkesi’ veya ‘devlet egemenliği’ terimini kullanıyorum.”

Eldeki çalışmada siber uzayın “devlet egemenliğinin bir konusu olarak” ele alınması da bu yönde bir mülahazanın sonucudur. Yine de uluslararası hukukta belirgin ve etkin bir normatif çerçeve oluşana dek başta ülkesellik olmak üzere çeşitli metaforların kullanılması, böyle bir normatif çerçevenin oluşumuna hizmet edebilecektir.

Ortak mal yaklaşımı, tam aksi istikametteki siber ülke düşüncesiyle benzer şekilde siber uzayın mekansallaştırılması üzerinden hareket etmektedir. Siber uzayın açık denizler, Antarktika ve dış uzaya kıyasla küresel ortak mal olduğunun kabul edilmesi, makul önermeler içermekle birlikte kuvvetli eleştirilere de maruz kalmıştır.¹⁰⁸⁰ *Res communis* ya da insanlığın ortak mirası olmak, ilgili alanlar için doğal bir nitelik değildir. Devletler, uluslararası hukuk bağlamında iradelerini ortaya koyarak bu alanların niteliklerini tespit etmişlerdir. Siber uzayın da küresel ortak mal olarak kabul edilebilmesi için devletlerin bu yönde irade göstermeleri gereklidir. Oysa uygulamada egemenlik talepleri istikrarlı biçimde yükselmektedir. DNS yönetimi ile standart ve protokollerin belirlenmesinin devlet dışı mecralarda gerçekleşiyor olması da devletlerin işleyişe uyum sağlamasının sonucudur. Bu bakımdan siber uzayın büyüklük ve yerleşiklik itibarıyla kontrolden çıktığını ve devletler için artık çok geç olduğunu ileri sürmek fazla iddialı bir yaklaşımdır. Kontrol ve cebir adına siber uzayın yapısal özelliklerinden kaynaklı güçlükler olduğu aşîkardır. Şirketlerin kabiliyetleri de göz önüne alındığında, egemenlik gibi mutlak bir otorite ifadesinin kullanımında tereddütler doğması olağandır. Fakat devlet, egemenliğiyle birlikte sistemin içindedir; egemenlik kaynaklı kuvvet kullanma tekelinde ise kurucu unsur meşruiyettir. Fiziksel ülke içerisinde dahi devletlerin kontrolü

¹⁰⁷⁹ Tsagourias, s.13.

¹⁰⁸⁰ Ibid., s.30; James A. Lewis, “Sovereignty and the Role of Government in Cyberspace”, *The Brown Journal of World Affairs*, Vol.16, No.2, (2010), s.62.

kaybettikleri ve kuvvet kullanma tekeli fiilen yitirdikleri senaryolar yaşanabilmektedir. Bu durumlarda devletin yok olmasından ve ülke üzerinde egemenliğin ortadan kalkmasından bahsedilememektedir.¹⁰⁸¹ Siber uzayın değerlendirilmesinde yapılan bir hata da yalnızca mantıksal boyutuyla yekpare bir sanal yapı olarak ele alınmasıdır. Böyle bakıldığında küresel sanal yapının bütünü üzerinde bir devletin egemenlik iddiası mümkün olamayacağı için siber uzayın egemenlik dışı soyut bir mekân olduğu sonucuna varılmaktadır. Oysa siber uzay, boyut ve unsurlarından müteşekkildir. Bunlar ayrı ayrı egemenlik konusu olabilmektedir. Holistik düşünce, siber uzayın tamamı için geçerli olabileceği gibi devletler adına egemenlik konusu edilmiş noktalar için de geçerli olabilecektir. Bu durumda birleşen -fiziksel veya mantıksal- noktalar da devletlerin ulusal siber ülkesini/bölgesini teşkil edebilecektir.

Siber uzayda devlet egemenliğine Vestfalyacılık anlatısı üzerinden yaklaşmak, küreselleşme düşüncesini savunan yazarların en sık kullandığı yöntemlerdendir. Zira Vestfalyacılık siber uzayda parçalanmanın, balkanizasyonun ve çatışmanın kaynağı olacaktır. Toplumların ve devletlerin en ince kılcallarına kadar ulaşmış ve hayati konuma yerleşmiş internet gibi siber uzay öğelerinin “olması gerektiği gibi” çalışmaması yahut ortadan kalkması, birçok açıdan yıkıcı sonuçlar doğurabilecektir. Fakat fiziksel uzayda yerleşik egemen devletler sistemi finans, ticaret, ulaşım, taşımacılık gibi önemli uluslararası sektörlerin sonunu getirmemiştir. Her devletin kendi kudreti nispetince belirlediği ve uyguladığı normların yanında, iş birliği neticesinde oluşmuş uluslararası hukuk normları kabul edilebilir bir uyum içerisinde yürümektedir. Kuzey Kore gibi radikal bir örnek de dahil olmak üzere hiçbir devlet, kapılarını tamamen kapatıp uluslararası ilişkileri kesme yoluna gitmemekte veya gidememektedir. Sınır aşan süreçler, bölgesel ya da küresel olsun devamlılığını korumaktadır. Devletlerin katkıları ve iradi mutabakatlarıyla modern uluslararası hukukta egemen devletler sistemi dönüşüm geçirmiştir. Zira egemenlik, devletin uluslararası hukuktan doğan yükümlülüklerine aykırı davranma gerekçesi olarak sunulamaz. İrlanda'nın UNOEWG'ye sunduğu pozisyon belgesinde yakındığı üzere, insan hak ve özgürlüklerini haksız şekilde kısıtlama

¹⁰⁸¹ Shaw, ss.159-160.

maksatlı devlet girişimlerinde de egemenliğin gerekçe olarak sunulması vaki olsa dahi¹⁰⁸² bu tür sapmalar hem siber uzaya özgü değildir hem egemenliğin mevcudiyetine ilişkin esaslı geçersiz kılmayacaktır. Sonuç olarak bu tabloda siber uzayın istisnai bir konuma oturtulup, devletlerin egemenlik taleplerinin, doğrudan yıkıcı sonuçlar doğuracağı gerekçesiyle dışlanması gerçekçi ve akılcı görünmemektedir.

Siber uzayda devlet egemenliği kabul edilirken sıradaki güçlükler; parça parça tespit edilen egemenlik konularının bir gövde haline getirilmesi, bu gövdenin niteliklerinin belirlenmesi ve egemenlik sınırlarını belirleyecek kıstasların tespit edilmesidir. Mekânsal analogilere tekrar başvurmak gerekirse, deniz yetki alanlarının tespiti üzerinden kıyasa gidilebilir. Denizler, insanlığa içinde yerleşik yaşam alanı sunmadan dünya yüzeyinin yaklaşık %70'ini oluşturması, biyokütlenin yaklaşık %90'ını barındırması ve dünya ticaretinin yaklaşık %90'ının deniz ticaret filosunca gerçekleştirmesi hasebiyle, hukuki rejimi küresel bağlamda en kritik öneme sahip mekân türüdür.¹⁰⁸³ Siber uzayı *res communis* olarak kabul edenler için temel ilham kaynağı olan açık denizler, devlet egemenliği dışında bırakılmıştır ve uluslararası hukukun öngördüğü sınırlar dahilinde “kullanıcılar” için serbesti söz konusudur.¹⁰⁸⁴ Eldeki çalışma adına anahtar soru ise denizde karaya yaklaştıkça devletlerin yetkilerini arttıran mevcut sistemde sınırların neye göre belirlendiğidir. Çünkü modern devletin ayırt edici özelliklerinden biri, belirlenmiş sınırlardır. Kara sınırları, ülkesel egemenliğin çekirdeği olan kara ülkesini belirler. Ardından kara ülkesine nispetle deniz ülkesi ve kara ile deniz ülkelerinin üzerinde belli bir irtifaya kadar hava ülkesi belirlenir. Deniz ve hava ülkelerinin sınırlarının tespitine dair esaslar, bilhassa uluslararası antlaşmalar marifetiyle günümüzde büyük ölçüde kökleşmiş durumdadır. Lakin tabii ki erken dönemlerde bu denli net normların varlığından bahsedilemez. *Bynkershoek* tarafından 1703'te “*kara egemenliği, silah gücünün sona erdiği yerde biter*” ifadesiyle özetlenen ilkenin deniz egemenliğindeki karşılığı, karadaki silah gücünün denizdeki tesir haddinde yani “top menzili” ilkesinde bulunmuş; buna binaen üç mil esası erken dönemde kabul

¹⁰⁸² UN/Open-ended Working Group on Information and Communication Technologies, Position Paper on the Application of International Law in Cyberspace by Ireland, Working Papers, 07.07.2023, [https://docs-library.unoda.org/Open-Ended-Working-Group-on-Information-and-Communication-Technologies-\(2021\)/Ireland-National-Position-Paper.pdf](https://docs-library.unoda.org/Open-Ended-Working-Group-on-Information-and-Communication-Technologies-(2021)/Ireland-National-Position-Paper.pdf) (31.12.2024).

¹⁰⁸³ Alp Eren Tanyeri, *Uluslararası Hukukta Özel Hassas Deniz Alanları ve Türk Suları*, Ankara: Seçkin Yayıncılık, 2022, ss.18-19.

¹⁰⁸⁴ BMDHS, Kısım VII.

görmüştür.¹⁰⁸⁵ Sınır tespitinde antlaşma varsa, doğal ve beşerî faktörler perde arkasına çekilir. Ancak hukuk yapımına giden süreçte bu faktörler belirleyicidir. Cari uluslararası hukukta deniz yetki alanları, açık denizlerden iç sulara kadar katmanlı şekilde normatif olarak belirlenmiş olsa da sürecin arka planında doğal ve beşerî faktörlerin etkisi malumdur. Siber uzayda yetki alanlarını ve egemenlik sınırlarını belirleyen uluslararası hukuk normlarının yokluğunda da siber uzayın yapısal özellikleri ve sosyal/siyasal faktörler benzer şekilde rehberlik edecektir. Bu yolda temel sorun, siber uzayın mekânsal kabulündeki uyumsuzluklardır. Zira siber uzayın mekân olma bakımından denizlerle arasındaki farklılıklarının burada tekrar izahına dahi lüzum yoktur. Bu sebeple mekânsallığa mutlak şekilde bağlı kalmadan ve siber uzayın özgün yapısını göz ardı etmeden, benzerlikler üzerinden hareket etmekte fayda olacaktır. Roguski'nin "katmanlı egemenlik" yaklaşımı da tam olarak bu prensibe dayanmaktadır. Nasıl ki denizlerde, devlet egemenliğinin çekirdeği olan kara parçalarına yaklaşıldıkça devlet yetkisi ve egemenlik hakları güçlenmektedir; siber uzayda da devletin asli menfaatleriyle kurulan irtibatın derecesine göre -UAD'nin Nottebohm ve Barcelona Traction davalarında ülke dışı yetkinin tespiti için kullandığı "hakiki irtibat (*genuine connection*)" kriterine benzer şekilde- katmanları tespit edecek bir yakınlık testi geliştirilebilir.¹⁰⁸⁶ Ancak bu test, mevcut şartlar gereği, denizlerdeki kadar belirgin sınırlar çizmek yerine somut olaya göre devletin irtibat derecesini tespit etmeye yarayacaktır. Kodifikasyona giden yol, bu tür usullerden geçecektir.

Katmanlı yaklaşım tercih edildiğinde, çekirdek katmanın ülkede bulunan fiziksel unsurlar olduğu çıkarımı henüz ilk kertede yapılabilir. Kara ülkesinden uzaklaşıldıkça, denizde ve havada bulunan fiziksel unsurlar için de deniz yetki alanlarının ve hava sahasının hukuki rejiminin izdüşümü geçerli olacaktır. Mantıksal boyut ve veri ise yakınlık testinin esas önem arz ettiği başlıklardır. Egemenlik irtibatı, sözgelimi bir bakanlık Web sitesi veya askeri veri tabanı gibi unsurlarda mutlak görünümdeyken; bir vatandaşa yönelik hakaret ifade eden içerikte yahut ülkede mukim kişilerin Web'de güneş gözlüğü aramasına ilişkin verilerde bulanıklaşmaktadır. Bu noktada nitelikli etkiler doktrini gibi etki esaslı ya da söz konusu unsurları işlevine veya cinsine göre

¹⁰⁸⁵ Toluner, s.84.

¹⁰⁸⁶ Roguski, s.356.

sınıflandırılmak suretiyle tasnif esaslı yöntemler kullanılabilir. Belirli bir kapasitenin veya trafiğin üstündeki sunucu ve veri merkezleri, kurulacak uluslararası denetim ve yaptırım mekanizmalarına tabi tutulabilir. Böylece devletlerin veya vatandaşların taleplerinin meşruiyetinin hem yer sağlayıcı, web sitesi işletmecisi ya da bunların bulundukları devlet dışında bir merci tarafından değerlendirilmesi hem icra edilebilirliğin güvence altına alınması sağlanabilir.

Yalnızca katmanlı egemenlik teorisi bağlamında katmanların tespitine ilişkin esasların belirlenmesi dahi tek başına mufassal bir çalışmanın konusu olabilir. Fakat son tahlilde siber uzayın egemenlik dışı tutulmasının artık mümkün olmadığı aşıkarken; siber uzayın boyut ve unsurlarının da hepsinin devlet egemenliği ile eşit derecede irtibatlı olmadığı ve söz konusu derece farklılıklarına dair hükümlerin -bilhassa kapsamlı uluslararası antlaşmalarla “Uluslararası Bilişim Hukuku” normatif olarak şekillenene dek- her somut olgu ve olay için ayrı değerlendirilmesi gerektiği görülecektir.

Güncel şartlarda, uluslararası ilişkilerdeki dengeler ve devlet doktrinlerindeki farklılıklardan kaynaklı kutuplaşma nedeniyle küresel mutabakat zemini bulunması güç görünmektedir. Eldeki çalışmada yer yer vurgulandığı gibi söz konusu güçlük siber uzaya özgü değil; uluslararası hukukun genel problemidir. 1945 sonrası süreçteki küresel kodifikasyon rüzgârı dineli uzun zaman olmuş ve normların daha çok bölgesel iş birlikleri ile belirlendiği bir döneme girilmiştir. Sonuç olarak, muhakkak zaman alacak olsa da eninde sonunda devletlerin ilke ve esaslar üzerinde mutabakata varıp, siber uzayda analogilerden ve metaforlardan arındırılmış bir hukuk inşa edecekleri kanaatinde olduğumu ifade etmek isterim. Zira BİT’nin gelişim hızı, (uluslararası) hukuk disiplinindeki boşlukları devlet otoritesinin tahammül dairesinin dışında itecek görünmektedir.

B. Siber Uzayda Egemenliğin İhlali

1. İlke Olarak Egemenlik ve Kural Olarak Egemenlik

Uluslararası hukukta egemenlik, Birinci Bölüm’de bahsedilen ilkeler ve unsurlar ile çerçevelenmiştir. Devletin belirli ve münhasır bir alan (ülke) ile vatandaşları (uyrukluk) üzerinde yasama, yürütme ve yargı fonksiyonlarını (kontrol) başka bir üst

otoriteye tabi olmadan ve otoritesini paylaşmadan (bağımsızlık ve otonomi) kullanması ve diğer devletlerle karşılıklı olarak bu tür bir kullanıma saygı gösterilmesi (karşılıklı tanıma) esasına dayalıdır. Egemenliğin, kendisinden “kuvvet kullanma yasağı” ve “iç işlerine müdahale yasağı” gibi kurallar türeyen bir uluslararası hukuk ilkesi mi yoksa doğrudan ihlal edilebilir bir uluslararası hukuk kuralı mı olduğu sorunu, literatürde tartışma konusudur. Tartışmanın en yaygın görüldüğü bağlam ise siber uzaydır.¹⁰⁸⁷ Siber uzayın fiziksel ülkelerden bağımsız olarak devletlerin asli menfaatlerine zarar verebilecek eylemlere imkân tanınması, tartışmayı doğuran kök sebeptir. Egemenlik, siber uzayda geçerli bir olgu ise bu olgunun mahiyeti, ihlalin sonuçlarını belirleyecektir. “Egemenliğin ihlalinin (*violation of sovereignty*)” mümkün olduğu, UAD’nin Nikaragua¹⁰⁸⁸ ve Korfu Kanalı¹⁰⁸⁹ kararlarında da yansımaları görüleceği üzere uluslararası hukukun köklü bir gerçeğidir.

İlke-kural tartışmasının neden önemli olduğuna dair ileri sürülen gerekçe, ilke olarak egemenliğin ihlali ile kural olarak egemenliğin ihlalinin uluslararası hukukta farklı sonuçlar doğuracağıdır. Literatürdeki tartışma, Tallin El Kitabı’nın yayımlanmasına binaen 2017’de gerçekleşen bir sempozyumda, egemenliğin doğrudan hukuki sonuçlar doğuran bir kural değil ancak bir ilke olduğunu savunan *Corn ve Taylor*¹⁰⁹⁰ ile karşıt görüşteki *Schmitt ve Vihul*’un¹⁰⁹¹ sunumlarının ardından hararetlenmiştir. Hemen sonra *Schmitt ve Vihul* uluslararası hukukun birincil normlarından kabul ettikleri “egemenliğe

¹⁰⁸⁷ Konuyu tartışan bazı çalışmalar için bkz. Kevin Jon Heller, “In Defense of Pure Sovereignty in Cyberspace”, *International Law Studies*, Vol.97, (2021), s.1432 vd.; Henning Lahmann, “On the Politics and Ideologies of the Sovereignty Discourse in Cyberspace”, *Duke Journal of Comparative & International Law*, Vol.32, No.1, (2021), s.61 vd.; Steven Wheatley, “Election Hacking, the Rule of Sovereignty, and Deductive Reasoning in Customary International Law”, *Leiden Journal of International Law*, Vol.36, No.3, (2023), s.675 vd.; Metodi Hadji-Janev, “Filling the *Opinio Iuris Vacuum* on Sovereignty in Cyberspace: A Call for the South-Eastern European States to Act”, *Cybersecurity and Law*, Vol.6, No.2, (2021), s.151 vd.

¹⁰⁸⁸ “Amerika Birleşik Devletleri’nin, Nikaragua toprakları üzerindeki uçuşları yöneterek veya bunlara izin vererek... Nikaragua Cumhuriyeti’ne karşı, uluslararası örf ve âdet hukuku uyarınca başka bir devletin egemenliğini ihlal etmeme yükümlülüğünü ihlal ettiğine... Amerika Birleşik Devletleri’nin, 1984 yılının ilk aylarında Nikaragua Cumhuriyeti’nin iç veya karasularına mayın döşeyerek, Nikaragua Cumhuriyeti’ne karşı, uluslararası örf ve âdet hukuku uyarınca başka bir devlete karşı kuvvet kullanmama, içişlerine müdahale etmeme, egemenliğini ihlal etmeme ve barışçıl deniz ticaretini kesintiye uğratmama yükümlülüklerini ihlal ettiğine...”; *Military and Paramilitary Activities in and Against Nicaragua* (Nicaragua v. United States of America), Merits, **Judgment**, ICJ Reports, 1986, s.137.

¹⁰⁸⁹ “12 ve 13 Kasım 1946 Operasyonu sırasında İngiliz Donanması’nın Arnavutluk sularındaki eylemleri nedeniyle, Birleşik Krallık’ın Arnavutluk Halk Cumhuriyeti’nin egemenliğini ihlal ettiğine...”; *Corfu Channel Case*, Merits, **Judgment**, ICJ Reports, 1949, s.36.

¹⁰⁹⁰ Gary P. Corn ve Robert Taylor, “Sovereignty in the Age of Cyber”, *American Journal of International Law Unbound*, Vol.111, (2017), s.211.

¹⁰⁹¹ Michael N. Schmitt ve Liis Vihul, “Sovereignty in Cyberspace: *Lex Lata Vel Non?*”, *American Journal of International Law Unbound*, Vol.111, (2017), s.214.

saygı” kavramını ele alan bir çalışma yayımlamıştır.¹⁰⁹² Devam eden süreçte tartışmaya katılan yazarlardan *Heller*, devlet uygulamalarından, UAD kararlarından ve önde gelen yazarların görüşlerinden delil getirerek egemenliğin uluslararası hukukun birincil normlarından olduğunu savunur.¹⁰⁹³ Tallin El Kitabı’nda “Egemenliğin İhlali” başlığı altında, “*bir devlet, başka bir devletin egemenliğini ihlal eden siber operasyonlar yürütemez*” ifadesiyle yer alan 4. Kural da bu görüşün temsilcilerindendir.¹⁰⁹⁴ Karşıt görüşteki yazarlardan *Lahmann* ise “kural olarak egemenlik” düşüncesinin uluslararası hukukta ana akım haline geldiğini kabul ederken;¹⁰⁹⁵ aslında “egemenliğin ihlali” kastın, sözgelimi ihlal edilen “kuvvet kullanma yasağı ‘kuralı’ ile korunan menfaat olarak egemenliğin” ihlali olduğunu ileri sürmüştür.¹⁰⁹⁶ *Goldsmith* ve *Loomis* de “Tallin El Kitabı yazarlarının yalnızca mer’i (*lex lata*) uluslararası örf ve âdet hukukunu tespit ettikleri ve olması gereken ya da gelecekte olacak hukuka (*lex ferenda*) yönelik bir iddiada bulunmadıkları yönündeki beyanlarına” işaret ederek; 4. Kural’ın uluslararası örf ve âdet hukukunu yansıttığına yönelik yeterli delilin bulunmadığından bahisle egemenliğin kural olarak kabulünü eleştirmişlerdir.¹⁰⁹⁷ Son bir örnek olarak *Wheatley*, bütün bu görüşler ışığında tümevarım ve tümdengelim metotlarıyla örf ve âdet hukukunu tespit etmeye çalıştığı makalesinde; egemenlik kuralını “kurucu (*constitutive*)” ve “düzenleyici (*regulative*)” ayrımına tabi tutmuştur. Yazara göre doğru ifade şöyledir: “*Devlet olarak sayılan bir siyasi topluluk (kurucu egemenlik kuralı) başka bir devletin egemenliğini ihlal etmemelidir (düzenleyici egemenlik kuralı)*”.¹⁰⁹⁸

Yukarıda ana hatlarıyla özetlenen literatür tartışmasındaki iki görüşten hangisinin doğru olduğundan ziyade, asıl problem; egemenlik ihlali, egemenliğin ilke veya kural olmasının, uluslararası hukuktaki sonuçları itibarıyla gerçek bir farklılık doğurup doğurmayacağıdır. Konunun öncelikli bağlamı olan siber uzay özelinde odaklanılan nokta, fiziksel zarara sebep olmayan ve hükümet işlevlerinin kullanımına engel teşkil etmeyen (düşük yoğunluklu) siber operasyonların hukuki durumudur. Kural olarak

¹⁰⁹² Michael N. Schmitt ve Liis Vihul, “Respect for Sovereignty in Cyberspace”, *Texas Law Review*, Vol.95, Iss.7, (2017), s.1639 vd.

¹⁰⁹³ *Heller*, ss.1439-1444.

¹⁰⁹⁴ Tallin El Kitabı, s.17.

¹⁰⁹⁵ *Lahmann*, s.66.

¹⁰⁹⁶ *Ibid.*, ss.94-95.

¹⁰⁹⁷ Jack Goldsmith ve Alex Loomis, “‘Defend Forward’ and Sovereignty”, *Hoover Working Group on National Security, Technology, and Law*, Aegis Series Paper No.2102, 29.04.2021, s.7.

¹⁰⁹⁸ *Wheatley*, 2023, s.697.

egemenlik savunucuları, kuvvet kullanma ve iç işlerine karışma yasaklarını ihlal etmeyen siber casusluk gibi eylemlerin devlet egemenliğini ihlal edeceğine; fakat bu yöndeki birincil uluslararası hukuk normunun yokluğunda, egemenlik tek başına kural olarak kabul edilmezse hukuka aykırılığın ileri sürülemeyeceğine işaret eder.¹⁰⁹⁹ Böyle bir ihtimal de siber kabiliyetleri yüksek devletlerin emperyal amaçlarına hizmet edeceği gerekçesiyle eleştirilmiştir.¹¹⁰⁰ Birleşik Krallık'ın pozisyonu¹¹⁰¹ ile paralel görüşteki *Corn* ve *Taylor*'ın düşüncelerine karşı, bu yazarların ABD Savunma Bakanlığı ile iltisaklarından bahisle ilgili kurumun operasyonel hareket alanını korumaya çalıştıkları yorumunda bulunulması,¹¹⁰² bu eleştirinin uzantılarından biridir.

Esasen bu başlık altındaki tartışma, *Wheatley*'in benzetmesiyle, ışıktan çok ısı üretmektedir.¹¹⁰³ Siber uzayda kural olarak egemenlik mutlak biçimde kabul edildiğinde; siber uzayın özgün yapısı nedeniyle, devletlerin çok düşük yoğunluklu eylemlerinin dahi bir anda uluslararası hukuku ihlal etmesi sebebiyle uluslararası sorumluluk doğurması gündeme gelebilir. Diğer taraftan ise kuvvet kullanmama ve iç işlerine karışmama gibi net yasak içeren birincil uluslararası hukuk normlarının siber uzay için yokluğunda; egemenlik ihlaline tek başına uluslararası sorumluluk doğuracak hukuki sonuç tanınmazsa, devletlerin menfaatlerinin gerçekten tehdit altında kalacağı da aşıkardır. Özünde egemenlik, ilke ya da kural olmanın ötesinde modern uluslararası hukukun kurucu unsurudur. İhlal edilmesi “devletin uluslararası hukuktan doğan yükümlülüğün ihlali” sayılabilecek normların çoğu bu unsorda mündemiçtir. UAD kararlarında da ilkeler ve kurallar arasındaki farka ve hiyerarşik ilişkiye hiç girilmeden iki terimin eş anlamlı kullanılması temayülü görülmektedir.¹¹⁰⁴ Pratikteki gerçek sorun ise, bu hususlardan bağımsız olarak, hangi fiillerin uluslararası hukuka aykırılık teşkil edeceğine dair “eşik (*threshold*)” tespiti. Bunun için de önce genel esasların belirlenmesi,

¹⁰⁹⁹ Heller, ss.1487-1488.

¹¹⁰⁰ Lahmann, ss.67-77; Schmitt ve Vihul, “Sovereignty in...”, 2017, s.214.

¹¹⁰¹ Birleşik Krallık, 2018’de UNGE raporunu reddederek düşük yoğunluklu siber operasyonların uluslararası hukuka aykırı olmadığına yönünde en net pozisyon belirleyen devlet olmuştur; Heller, s.1436 ve s.1445.

¹¹⁰² Schmitt ve Vihul, “Sovereignty in...”, 2017, s.214.

¹¹⁰³ Wheatley, 2023, s.697.

¹¹⁰⁴ Maurice Mendelson, “The International Court of Justice and the Sources of International Law”, Vaughan Lowe ve Malgosia Fitzmaurice (Ed.), **Fifty Years of the International Court of Justice: Essays in Honour of Sir Robert Jennings** içinde (63-89), Cambridge: Cambridge University Press, 1996, s.80

ardından ihlal potansiyeli barındıran fiillerin kategorize edilmesi, farazi örneklerin ve yaşanmış vakaların bağlam içinde değerlendirilmesi gereklidir.

2. Genel Esaslar

a. Metoda Dair

Tallin El Kitabı'nda, siber uzayda egemenliğin ihlaline dair esaslar, örnekleri ve sonuçlarıyla tafsilatlı biçimde ele alınmıştır.¹¹⁰⁵ Ancak eser, en önemli noktalara değinmekle birlikte pek tabii bütün sorunlara çözüm getirmiş değildir. Ayrıca bazı yaklaşımları eleştiriye açık durumdadır. Eserin disiplindeki kuvvetli hakimiyetine rağmen, eldeki çalışmanın bu kısmının bir Tallin El Kitabı anlatımına dönüşmemesi adına; oradaki esasları referans edinip yeniden haritalandırarak, önce teoride ve uygulamada yerleşik hale gelmiş esasları vurgulayıp, sonrasında tartışmalar ve örnekler üzerinden devam ederek konuyu ele almanın amaca uygun olacağı kanaatindeyim.

Konuya özgü ve kapsamlı bir uluslararası antlaşmanın yokluğunda, ahkama yönelik bütün akademik çalışmalar ancak örf ve âdet hukukunu tespit çabası ya da *de lege ferenda* teklif denemesi niteliğinde üretilebilmektedir. Haliyle devlet uygulamaları, yargı kararları ve öğretideki görüşler, yazarlara bu yolda rehberlik etmektedir.

b. Fail ve Siber İsnat

Devletler, özel hukuk kişilerinin fiilleri üzerinde iç egemenlik bağlamında geniş yetkilere sahiptir. Bu aktörlerce devlete ve kamu düzenine karşı icra edilen en ağır eylemler dahi nihayetinde ulusal hukuk ihlalidir. Hedef alınan devlet, eylem öncesi ve sonrasında, uluslararası hukuka aykırı olmamak kaydıyla ulusal hukukunda öngördüğü her türlü önlem ve yaptırıma başvurabilir. İhlal ülke dışından kaynaklandığında, ihlali gerçekleştiren aktörün tabiiyetinde olduğu devlet veya ihlalin kaynaklandığı ülke devleti, ihlalin önüne geçilmesi adına gerekli özeni göstermelidir. Aksi halde mağdur devlet, söz konusu devlete karşı da birtakım meşru yollara başvurabilir. Bunlar arasında, sözgelimi

¹¹⁰⁵ Tallin El Kitabı, ss.17-27.

uluslararası terörizme karşı meşru müdafaa yahut sorumluluk hukukundan kaynaklı önlemler örnek olarak gösterilebilir.¹¹⁰⁶

Ulusal hukuk ihlalleri bir yana, egemenlik ihlali, uluslararası hukuka özgü bir kavramdır. Dolayısıyla bir devletin egemenliğini ancak başka bir uluslararası hukuk süjesi ihlal edebilecektir. Bu noktada devlet ile devlet arasında karşılıklı olarak egemenlik ihlali mümkünken; uluslararası örgütler ile devletler arasında asimetrik bir ilişki söz konusudur. Uluslararası örgütler, uluslararası hukuk süjesi olmaları itibarıyla gerçekleştirdikleri eylemlerle devlet egemenliğini ihlal edebilirler. Diğer taraftan uluslararası örgütler egemen yapılar olmadıkları için, devlet eylemlerinin uluslararası örgütlerin egemenliğini ihlal etmesi söz konusu olamaz.¹¹⁰⁷ Yine de pratikte uluslararası örgütlerin devlet kaynaklı zararlı siber faaliyete maruz kalmaları halinde, faaliyetin türüne göre, mağdur altyapıyı ülkesinde bulunduran devletin egemenliğinin ihlal edildiği veya uluslararası örgüte verilen zarardan ötürü devletin uluslararası sorumluluğunun doğduğu senaryolar gerçekleşebilir.

Egemenlik ihlali, uluslararası hukuk süjeleri için geçerli olduğuna göre, ihlalin doğması için ön koşullardan biri, fiilin bir uluslararası hukuk süjesine isnat edilebilmesidir. Siber uzayda egemenlik ihlal eden fiilin, hangi ülkeden kaynaklandığı ve hangi kişiler eliyle işlendiğinden bağımsız olarak hangi uluslararası hukuk süjesine (özellikle de devlete)¹¹⁰⁸ isnat edilebildiği önemlidir. Uluslararası sorumluluk hukukundaki, A/RES/56/83 sayılı taslak maddeler belgesinde normatif sunumu yapılan isnat hükümleri¹¹⁰⁹ bu hususta da geçerlidir.

İngilizce literatürde “siber isnat (*cyber attribution*)” tabiri kullanılan “siber uzayda gerçekleşen eylemlerin devlete isnat edilmesi” sürecinde büyük ispat güçlükleriyle karşılaşmaktadır. Çoğu eylemin kaynağı tespit edilememekte, edildiğinde ise gerçek kişilere ulaşılmakta ve bunların eylemi devlet kontrolü ya da yönlendirmesi

¹¹⁰⁶ Erkiner, Uluslararası Terörizme..., 2021, ss.173-175.

¹¹⁰⁷ Tallin El Kitabı, ss.155-156.

¹¹⁰⁸ Buradan itibaren “uluslararası hukuk süjesi” yerine “devlet” ifadesi tercih edilecektir. Teoride mümkün olsa da uygulamada rastlanmaması, uluslararası örgütlerin ihlal faili olması halinin göz ardı edilmesine sebep olmuş görünmektedir. Bu nedenle, eldeki çalışmada, ancak uluslararası hukuk süjelerinin fail olabileceği ilkesel olarak belirtilip konunun devletler üzerinden ele alınmasının, ifade kolaylığı açısından faydalı olacağı kanaatindeyim.

¹¹⁰⁹ UN/General Assembly, Responsibility of States for Internationally Wrongful Acts, A/RES/56/83, 28.01.2002, ss.2-4, Bölüm II.

altında işlediklerine yönelik kesin delil bulunamamaktadır. Kayıtlara geçen çok sayıda eylemden ancak 2014'te Çin'e isnat edilen siber casusluk vakası¹¹¹⁰, 2017'de gerçekleşip Kuzey Kore'ye isnat edilen (Kuzey Kore iddiaları reddetmiştir) WannaCry saldırısı ve yine 2017'de Rusya'ya isnat edilen (Rusya iddiaları reddetmiştir) NotPetya ve Bad Rabbit saldırıları¹¹¹¹ gibi sınırlı sayıda örnekten bahsedilebilmektedir.¹¹¹² Diğer yandan birçok platformda ABD ve İsrail'in gerçekleştirdiği iddia edilse de isnada dair resmi açıklama yapılmayan, İran nükleer tesislerine yönelik 2010 tarihli Stuxnet saldırısı ve 2020'de yine İran nükleer tesislerinde meydana gelen patlamalar (bir fiziksel saldırı mı yoksa siber saldırı mı sonucu oluştuğuna dair kesin bilgi verilmemiştir) gibi örnekler de mevcuttur.¹¹¹³

c. Teşebbüs, Kast ve Rıza

Siber uzayda devlet egemenliğinin ihlali, bir uluslararası hukuk normunun ihlali olarak görüldüğü takdirde uluslararası haksız fiil teşkil edeceğinden sorumluluk hukukunun belli başlı esaslarına kısaca değinmek gerekir. Öncelikle -ihlal edilen ayrı bir hususi norm yoksa- egemenlik ihlalinin doğması için eylemin sonuçlarının gerçekleşmesi gerekecektir. Operasyonel hatalar veya karşılaşılan siber güvenlik önlemleri nedeniyle teşebbüs aşamasında kalmış bir siber faaliyet, egemenlik ihlali sayılmayacaktır.¹¹¹⁴ Devletin uluslararası sorumluluğunda kusursuz sorumluluk ilkesi geçerli olduğu için¹¹¹⁵ ihlalin gerçekleşmesinde kast ya da ihmale dayalı bir kusurun varlığı da aranmayacaktır. Ayrıca normal şartlarda egemenliği ihlal edecek bir siber faaliyet, ilgili devletin rızasının varlığı halinde uluslararası hukuka aykırılık teşkil etmeyecektir. Bunun en bariz örnekleri,

¹¹¹⁰ Bkz. dipnot.570.

¹¹¹¹ WannaCry ve NotPetya saldırılarında ilgili devletlere isnatta bulunan öncü devletler Birleşik Krallık ve ABD olmuştur. ABD Ulusal İstihbarat Direktörü Ofisi (*Office of the Director of National Intelligence*) tarafından 2018'de yayımlanan Siber Isnat Rehberi'nde; söz konusu isnatlar için yordam (*tradecraft*), altyapı (*infrastructure*), kötü amaçlı yazılım (*malware*), niyet (*intent*) ve dış kaynaklı göstergeler (*indicators from external sources*) kistasları bağlamında yeterli delile ulaşıldığı ileri sürülmüştür; United States/Office of the Director of National Intelligence, **A Guide to Cyber Attribution**, 14.09.2018. Bad Rabbit saldırısı ise Birleşik Krallık ve Avustralya tarafından Rusya'ya isnat edilmiş ve uluslararası hukukun ihlali olarak nitelendirilmiştir; Chircop, s.374.

¹¹¹² William Banks, "Cyber Attribution and State Responsibility", **International Law Studies**, Vol.97, (2021), ss.1042-1045.

¹¹¹³ Ibid., s.1049; Töner Şen, ss.146-147.

¹¹¹⁴ Tallin El Kitabı, s.24.

¹¹¹⁵ Hakkı Hakan Erkiner, **Devletin Haksız Fiilden Kaynaklanan Uluslararası Sorumluluğu**, İstanbul: On İki Levha Yayıncılık, 2010, s.115.

siber kapasite paylaşımında, tatbikatlarda ve kolluk gibi doğası itibariyle devlete ait işlevlerin egemenlik altındaki siber unsurlarda kullanımına izin verilmesinde görülebilir.

3. Devletin Fiziksel Ülkesinde Gerçekleşen Yabancı Siber Faaliyet Kaynaklı Egemenlik İhlali

Egemenlik ihlali olduğu çıkarımında bulunulması en rahat olan eylemler, fiziksel anlamda ülkesel egemenliği ihlal edenlerdir. Bir devlete ait araçların yahut resmi görevlilerin diğer devlet ülkesinde izinsiz bulunmaları ve faaliyet göstermeleri, devletin ülkesi üzerindeki egemenliğinin ihlalidir. Öyle ki bir zarar doğmasa bile ihlal gerçekleşmiş sayılacaktır. Dolayısıyla bir devletin ülkesinde gerçekleşen ve başka bir devlete isnat edilebilen siber faaliyetler de bu anlamda ülkesel egemenlik ihlalidir. Ancak tabii ki böyle bir ihlalin siber uzayla ilişkisi nispeten zayıftır. Sözelimi yabancı bir istihbarat elemanının, ülkede bulunan bir siber altyapı unsuruna zarar verecek şekilde sabotajda bulunurken patlayıcı veya taşınabilir bellek kullanması arasında “ülkesel egemenliğin” ihlali bakımından fark yoktur.

Ülkesel egemenlik kaynaklı devlet yetkisinin istisnalarından olan devlet temsilcileri, gemileri ile hava araçlarına ve diplomatik misyon ile konsolosluk mensuplarına dair dokunulmazlık ve bağışıklıklar, siber uzay unsurları için de geçerlidir.¹¹¹⁶

Ülkede gerçekleşen yabancı faaliyetler bakımından tartışmalı husus “casusluk” faaliyetidir. Yukarıda İkinci Bölüm sonunda da değinildiği gibi; casusluk, hemen her devletin ulusal hukukunda suç kabul edilmesine rağmen uluslararası hukukta casusluğu yasaklayan bir norm gelişmemiştir. Nitekim devletlerin de bu yola sıklıkla başvurduğu bilinmektedir. Ancak hiçbir devlet de casusluğun uluslararası hukuka aykırı olmadığını iddia etmemiştir. Uluslararası hukukta gri bölgede kalan casusluğun, ülkeye izinsiz giriş ve fiziksel zarar gibi unsurları kapsamayacağını burada vurgulamak gerekir. Zira bunlar ülkesel egemenliğin açık ihlali olacaktır. Gözetleme ve bilgi sızdırma gibi faaliyetler ise tartışmanın esas konusudur. Tallin El Kitabı’nda yazarlar; fiziksel olarak bulunan ülkede casusluk faaliyeti gerçekleştirmenin, yaygın bir devlet uygulaması olduğunu kabul

¹¹¹⁶ Tallin El Kitabı, s.15.

etmekle birlikte, egemenlik ihlali olacağı yönünde görüş bildirmişlerdir. Yazarlardan bazıları ise; şayet altyapıya zarar verilmesi, verilerin silinmesi veya değiştirilmesi gibi unsurlar bulunmaksızın sadece veri sızdırma ve gözetleme söz konusu ise egemenlik ihlali olmadığı kanaatindedir.¹¹¹⁷ Bu görüşler de -isabet derecesi bir tarafa- siber uzayda devlet egemenliğinden (belli düzeyde ilişkisi olsa da) ziyade fiziksel uzaydaki ülkesel egemenlik ile ilgilidir. Siber ağırlıklı eylemler esasen ülke dışından kaynaklananlardır.

4. Devletin Fiziksel Ülkesi Dışında Gerçekleşen Siber Faaliyet Kaynaklı Egemenlik İhlali

Siber uzayın özgün sorunları, özgün yapısından ileri gelenlerdir. Bu bağlamdaki en önemli hususiyeti ise çok kez değinildiği üzere sınır aşan yapısıdır. Fiziksel uzayın herhangi bir noktasında işlenen fiil, yine herhangi bir başka noktada anında etki doğurabilmekte; hatta etki tamamen mantıksal boyutta gerçekleşse de devletlerin asli menfaatlerine zarar verebilmektedir. Ülke dışından kaynaklanan “uzaktan (*remote*) siber faaliyetler” yoluyla devlet egemenliğinin ihlali, iki unsura yönelik gerçekleşebilir; ülke ve kontrol.¹¹¹⁸ “Ülkesel bütünlüğün ve siyasi bağımsızlığın”¹¹¹⁹ müdahaleden korunması, egemen devletler sisteminin temel esaslarındandır. Ülke olarak egemenlikten türeyen kurallar yahut kural olarak egemenliğin unsurları, sonuçta bu esasları ifade eder.

¹¹¹⁷ Ibid., s.19.

¹¹¹⁸ Bir devletin insan unsuruna yönelen hukuka aykırı yabancı devlet eylemleri, doğrudan egemenlik ihlali olarak görülmemektedir. Yabancı bir devletin hukuka aykırı fiiline maruz kalan kişi, vatandaşı olduğu devlet ülkesinde bulunabileceği gibi fiili işleyen devlet ülkesinde yahut üçüncü bir devlet ülkesinde bulunabilir. Zaten ilk durumda fiil, kişinin vatandaşı olduğu devletin hem ülkesel egemenliğine hem vatandaşlık sebebiyle kişi üzerindeki egemenliğine yönelmiş bir ihlal olarak ele alınacaktır. İkinci ve üçüncü durumlarda ise fiilin gerçekleştirildiği ülke devletin ülkesel egemenliği, hukuka aykırı fiile maruz kalan kişinin vatandaşı olduğu devletin kişi üzerindeki egemenliğine göre öncelikli ve kuvvetli konumda görülmektedir. Böyle bir durumda devletler, vatandaşlarının mağduriyetlerine karşı “diplomatik koruma” müessesesine başvurabilirler. Özellikle 19. yy’da Avrupalı devletlerin, vatandaşlığa bağlı hak ve yetkilerini çok geniş değerlendirerek bunu diğer devletlere karşı askeri müdahalelere varan derecede baskı unsuru olarak kullanmalarına zamanla yükselen itirazlar, ülkesel egemenliğin söz konusu mukayesede öncelikli konuma yerleşmesine kapı açmıştır; Chittharanjan F. Amerasinghe, **Diplomatic Protection**, Oxford University Press, 2008, s.14. Oysa 20 yy’ın ilk yarısı geride kaldığında dahi, devletin ülkesi dışındaki vatandaşlarının can ve mal güvenliğini korumak için kuvvet kullanması ya da kuvvet kullanma tehdidine başvurusu meşru müdafaa kapsamında değerlendirilmekteydi; Derek W. Bowett, **Self-Defence in International Law**, Manchester: Manchester University Press, 1958, s.87 vd. Madalyonun diğer tarafında, devlet başkanları ile diplomatik temsilcilere tanınmış ayrıcalık ve bağışıklıklar ise; bu kişilerin devlet ile yüksek ilişki düzeyinin, temsil ettikleri devletin egemenliğini, ülkesinde bulundukları yabancı devletin ülkesel egemenliğine karşı öncelikli konuma getirdiğinin göstergesidir. Mevzubahis denklem, kişilere yönelmiş hukuka aykırı siber faaliyetler için de kıyasen geçerlilik arz edecektir.

¹¹¹⁹ BM Şartı, m.2/4.

a. Uzaktan Siber Faaliyet ile Ülkesel Bütünlüğe Müdahale Edilmesi

Bir devlete karşı yöneltilmiş siber faaliyetler amaç, yöntem ve etki itibariyle geniş bir çeşitliliğe sahiptir. Siber saldırıların tanımlanması ve sınıflandırılması, başlı başına ayrı bir çalışmanın konusudur.¹¹²⁰ Literatürde ülkesel bütünlüğe yönelik siber faaliyetler genellikle kuvvet kullanma yasağı kapsamına girme ve nihayetinde meşru müdafaa hakkı doğuracak şekilde silahlı kuvvet kullanımı sayılma ihtimalleri açısından ele alınmıştır. Hem günlük dilde hem resmi ve akademik literatürde çoğu kez siber uzayda rıza dışı hasmane faaliyetler¹¹²¹ siber saldırı (*cyber attack*) olarak adlandırılırken;¹¹²² Tallin El Kitabı örneğindeki gibi bazı çalışmalar, kişilerde yaralanma veya ölüm ya da fiziksel unsurlarda hasar veya yıkım oluşturan siber faaliyetleri (*cyber opeartion*) siber saldırı olarak kabul etmiştir.¹¹²³ Bu ayırım, genel kapsamda yüksek kavramsal titizlik gerektirmese de uluslararası hukuk bağlamında devletler için yasaklanmış “saldırı” eyleminin siber uzaydaki karşılığını ifade etmesi bakımından anlamlıdır. Konu hakkında içerdiği tespitlere sıklıkla başvurulmuş çalışmaları *Hathaway* ve *Diğerleri*, siber saldırılara dair incelemenin “araç”, “hedef” ve “etki” esasları üzerinden yapılabileceğini, kendilerinin ise etki esaslı yaklaşımı tercih ettiklerini belirtmişlerdir.¹¹²⁴ Esasen sadece silahlı kuvvet kullanımı değil, genel olarak egemenlik ihlalinden bahsedilirken de bir siber faaliyetin hangi araçla ve ne için icra edildiğinden ziyade, ortaya çıkardığı sonucun siber uzayda devlet egemenliğini ihlal edecek ölçüde olup olmadığı önemlidir. Bu test için genel kabul görmüş üç tip etki derecesi bulunmaktadır; “fiziksel zarar”, “siber unsurlarda işlev kaybı” ve “işlev kaybı eşiğinin altındaki sonuçlar”.¹¹²⁵

¹¹²⁰ Tanım ve türlere ilişkin bkz. Can Bolat, “Siber Saldırılarına Karşı Meşru Müdafaa Hakkının Uluslararası Hukuk Açısından İncelenmesi”, (**Doktora Tezi**, İstanbul Üniversitesi Sosyal Bilimler Enstitüsü, 2020), s.27 vd.; Töner Şen, ss.15-19 ve ss.122-134; Yunus Emre Gül, **Savaş Hukuku 2.0: Siber Saldırıları ve Hukuk**, İstanbul: Hukuk Akademisi Eğitim ve Yayıncılık, 2021, ss.28-33; Thanapat Chatinakrob, “Interplay of International Law and Cyberspace: State Sovereignty Violation, Extraterritorial Effects, and the Paradigm of Cyber Sovereignty”, **Chinese Journal of International Law**, Vol.23, Iss.1, (2024), ss.30-38.

¹¹²¹ Hasmane siber faaliyetlerin hukuki kategorizasyonunu dair bkz. Lucas Kello, “Cyber legalism: Why It Fails and What to Do About It”, **Journal of Cybersecurity**, Vol.7, Iss.1, (2021), s.9.

¹¹²² Örnekler için bkz. T.C. Ulaştırma ve Altyapı Bakanlığı, **Ulusal Siber Güvenlik Stratejisi ve Eylem Planı (2020-2023)**, s.10.; Herbert S. Lin, “Offensive Cyber Operations and the Use of Force”, **Journal of National Security Law & Policy**, Vol.4, No.1, (2010), s.63.

¹¹²³ Tallin El Kitabı, s.415.

¹¹²⁴ Oona A. Hathaway ve Diğerleri, “The Law of Cyber-Attack”, **California Law Review**, Vol.100, No.4 (2012), s.845.

¹¹²⁵ Tallin El Kitabı, s.20.

Uzaktan bir siber faaliyet ile bir devlet ülkesinde veya siber altyapısında patlama, yangın, yıkım, su baskını, ölüm, yaralanma vs. sonuçlara sebep olmanın, bu devletin ülkesel egemenliğini ihlal edeceği artık aşıkardır. Böyle bir faaliyetin silahlı kuvvet kullanımı kabul edilerek meşru müdafaa hakkı doğurması ise birtakım kriterler sağlandığı takdirde mümkün olacaktır.¹¹²⁶

Uzaktan siber faaliyet sonucunda oluşabilecek bir başka etki, siber uzay unsurlarında işlev kaybıdır. Ülkesel bütünlükle doğrudan alakalı olanlar ise fiziksel boyutu oluşturan unsurlardır. Uluslararası hukuk ihlallerinde daima karşılaşılan eşik problemi, bu husus için de geçerlidir. Siber uzayda devlet egemenliğini ihlal edecek ölçüde bir işlev kaybından ne anlaşılması gerektiği konusu tartışmaya açıktır. Tallin El Kitabı'nda, bu unsurlarda onarım veya değişim gerektirecek düzeyde bir işlev kaybının fiziksel zarara benzemesi hasebiyle unsurların bulunduğu devletin egemenliğini ihlal edeceği yönünde bir mutabakatın olduğu görülmektedir.¹¹²⁷ Fakat fiziksel unsurlarda onarım veya değişim gerektirmese de mantıksal unsurların beklenen şekilde çalışmasına engel olan yahut verilerin silinmesi veya değişmesiyle sonuçlanan faaliyetlerin de egemenlik ihlali olduğu söylenebilir. 2007'de Estonya'ya karşı gerçekleştirilen ve ülke çapında başta bankacılık ve iletişim olmak üzere birçok alanda sistemleri işlemez hale getiren siber terör saldırısı;¹¹²⁸ WannaCry vakasında Birleşik Krallık sağlık sisteminin siber işleyişinin bozulması;¹¹²⁹ 2012'de Shamoon virüsünün Suudi Aramco Şirketi'nin 30.000'e yakın bilgisayarında işlev kaybına sebep olması;¹¹³⁰ 2014'te Sony Şirketi'nin ABD'deki bilgisayar ve veri tabanlarında işlev ve veri kaybına sebep olunması,¹¹³¹ 2015'te Ukrayna'ya karşı gerçekleşen siber faaliyet ile elektrik kontrol sistemleri devre dışı bırakılarak Kiev ve ülkenin batı kısmında uzun süreli elektrik kesintisine sebep

¹¹²⁶ Mehmet Yayla, "Uluslararası Hukukta Siber Saldırıların Karşı Kuvvet Kullanma", **Türkiye Barolar Birliği Dergisi**, Sayı.107, (2013), ss.214-217.

¹¹²⁷ Tallin El Kitabı, s.21.

¹¹²⁸ Bu saldırıdan başta Rusya sorumlu tutulsa da Rus hükümeti tarafından iddialar reddedilmiş; milliyetçi saikler taşıyan Rus asıllı bir grubunun eylemi olduğu anlaşılmıştır. Saldırı, uluslararası siber güvenlik çalışmalarının ivmelenmesi adına dönüm noktası olmuş ve sonraki süreçte Tallin, bu alanın merkezi haline gelmiştir. Detaylı bilgi için bkz. Stephen Herzog, "Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses", **Journal of Strategic Security**, Vol.4, No.2, (2011), s.49 vd.; Esma Dilek, Özgür Talih ve Türksel Kaya Bensghir, "Estonia 2007 Siber Saldırıların İncelenmesi ve Ülkelerin Ulusal Siber Güvenlik Politikalarına Etkileri", **Bilgi Yönetimi Dergisi**, Cilt.6, Sayı.2, (2023), s.332.

¹¹²⁹ Banks, s.1043

¹¹³⁰ AlArabiya News, "Saudi Aramco Says Cyber Attack Targeted Kingdom's Economy", 09.12.2012, <https://english.alarabiya.net/articles/2012/12/09/254162> (31.12.2024).

¹¹³¹ Chircop, s.372.

olunması¹¹³² ve 2017’de Bad Rabbit fidyeye yazılımı ile Kiev’deki bir havaalanının ve metro sisteminin hedef alınması¹¹³³ gibi örnekler, işlev kaybının çeşitli boyutlarını yansıtmaktadır.¹¹³⁴

Ülkesel bütünlüğe etkisi bağlamında en tartışmalı uzaktan siber faaliyet tipi, fiziksel zarara ve işlev kaybına yol açmadan, rıza dışı ve muhtemelen hasmane nitelikte gerçekleşenlerdir. Bu tür düşük yoğunluklu siber faaliyetler BİT sistemlerine izinsiz giriş, gözetleme, veri sızdırma gibi özünde siber casusluk unsurları olan eylemleri kapsar. Ayrıca bir devlete ekonomik anlamda zarar verecek fintek bazlı faaliyetler de bu kapsamda bir örnektir. Sonuçları işlev kaybı eşiğinin altında kalan siber faaliyetlerin ülke dışından kaynaklandığında egemenlik ihlali sayılmayacağı iddiası, mer’i uluslararası hukukta casusluk ve ekonomik yaptırımlar gibi olguların egemenlik ihlali sayılması hususundaki boşluktan kaynaklanmaktadır. Savaş ve barış dikotomisi üzerinde inşa edilen hukuk; gelişen teknolojiyle büyük çeşitlilik kazanan, savaş eşiğine ulaşmayan ancak barışsızlık (*unpeace*) oluşturan devlet eylemlerine karşı yetersiz kalmıştır. *Kello* bu analizi, mevcut durumun batılı devletlerin söz konusu hasmane eylemlere karşı hoşgörüsünün değil hukuki ve doktrinel yetersizliğin göstergesi olduğu yönündeki düşüncesiyle ifade etmiştir.¹¹³⁵ Siber uzayda egemenliğin etkin savunucularından *Roguski* de Tallin El Kitabı’nda kabul edilen “egemenliğin ana hedef ve amacının, ülkesel bütünlüğün fiziksel ihlalden korunması olduğu” yönündeki anlayışı eleştirmiştir. Yazara göre ülkesel egemenliğin amaç ve hedefi “devlet otoritesinin kendi topraklarındaki münhasırlığının korunmasıdır”. Nitekim hava sahasına izinsiz girişler veya kişilerin sınır ötesine kaçırılması gibi vakalar, genellikle ülkede zarar yahut kalıcı bir fiziksel etki doğurmasa da ülkesel egemenliğin ihlali olarak görülürler.¹¹³⁶

¹¹³² Nadiya Kostyuk ve Yuri M. Zhukov, “Invisible Digital Front: Can Cyber Attacks Shape Battlefield Events?”, *Journal of Conflict Resolution*, Vol.63, Iss.2, (2019), s.317.

¹¹³³ Chircop, s.372.

¹¹³⁴ Söz konusu faaliyetler, bir devlete isnat edilebilmesinden bağımsız olarak, sonuçları itibarıyla bu başlığa örneklik teşkil etmektedir. Uluslararası hukuk bağlamında egemenliğin ihlalinin ancak ve yine uluslararası hukuk süjelerince işlenebileceği unutulmamalıdır.

¹¹³⁵ Kello, s.4.

¹¹³⁶ Przemysław Roguski, “Violations of Territorial Sovereignty in Cyberspace—an Intrusion-based Approach”, Dennis Broeders ve Bibi van den Berg (Ed.), *Governing Cyberspace: Behavior, Power, and Diplomacy* içinde (65-84), London: Rowman & Littlefield, 2020, s.74.

Siber casusluğun uluslararası hukukta egemenlik ihlali sayılıp sayılmayacağı sorunu, tabii olarak öncelikle fiziksel uzaydaki casusluğun mer'î uluslararası hukuktaki durumu üzerinden değerlendirilmektedir. Ancak velev ki fiziksel uzayda casusluk eylemleri uluslararası hukuka uygun kabul edilsin; siber casusluk yine müstakilen ele alınmalıdır. Tallin El Kitabı'nda siber casusluğun uluslararası hukuku tek başına ihlal etmeyeceği fakat kullanılan yöntem, ihlal edilen farklı menfaatler veya ortaya çıkan zarar nedeniyle başka uluslararası hukuk normlarının ihlalinin oluşabileceği anlatılmıştır.¹¹³⁷

Fiziksel uzayda görülen birçok fiil, siber uzayın sağladığı imkanlar sayesinde çok daha kolay işlenmektedir. Bunun sonucu da öncelikle ulusal hukuk normlarında ortaya çıkmıştır. Örnek olarak, BİT sistemlerinin sağladığı kolaylıktan yararlanılması, ceza hukukunda bazı suçlar için nitelikli hal teşkil etmektedir.¹¹³⁸ Nitelikli haller, temel suç tipine eklenen bazı unsurların fiildeki haksızlık içeriğini arttırması veya azaltmasına göre yaptırımı şekillendirir.¹¹³⁹ Kolaylaştırıcı unsurlar da failin suçu daha az riskle gerçekleştirebilmesini, bundan sebep cesaretlenmesini, ilgili haksız fiilin yaygınlaşmasını veya ortaya çıkaracağı zararın büyümesini sağlaması açısından fiilin haksızlık düzeyimi arttırabilir. Ayrıca kamu düzeninin korunması ve hakkaniyetin tesisi açısından da bu tür nitelikli haller ceza hukukunun önemli bir parçasıdır. Bu noktada maksadım tabii ki uluslararası hukukun yapısına oldukça zıt olan ceza hukukunu devletlere teşmil etmek değildir. Keza nitelikli hallerin fiilin haksızlık içeriğini arttırsa da suç olmayan bir fiili suça dönüştürmediği de aşıkardır. Diğer taraftan, sözgelimi çevreyi kirleten eylemlerde olduğu gibi, haksızlık içeren eylemin ağırlığına göre kabahat veya suç olarak düzenlenebilmesi; “yalan söylemek” fiilinde olduğu gibi, fiil özünde haksız olsa dahi yalın haliyle hukuki yaptırıma tabi tutulmayıp, bazı özel durumlarda (yalan tanıklık, resmi belgenin düzenlenmesinde yalan beyan vs.) hukuka aykırılık teşkil etmesi gibi durumlar, haksızlık eşiğine ilişkin sonuçlardır. Bir fiilin haksızlık içeriğinin ve dolayısıyla hukuki sonuçlarının belli şart ve unsurlar eşliğinde değişebildiği açıklıkla görülmektedir. Uluslararası hukukta devletler arasındaki münasebetleri düzenleyen normların iradeci yapısı göz önüne alındığında, siber casusluğun bir uluslararası hukuk

¹¹³⁷ Tallin El Kitabı, ss.168-174.

¹¹³⁸ Bazı örnekler ve yargı kararları için bkz. Ömer Şişek, **Suçun Nitelikli Halleri**, Ankara: Seçkin Yayıncılık, 2023, ss.86-87.

¹¹³⁹ Mahmut Koca ve İlhan Üzülmüş, **Türk Ceza Hukuku Genel Hükümler**, 16. Baskı, Ankara: Seçkin Yayıncılık, 2023, s.143.

ve egemenlik ihlali olarak kabul edilmesinin -en azından- devletlerin *opinio juris* unsuru içeren uygulamalarına bağlı olduğu -*lex lata* adına- söylenebilir. Ancak gerek uluslararası antlaşma ile ihdas edilsin gerek örf ve âdet hukuku kuralı olarak ortaya çıksın, normların, hukuk ilkelerinde ve hakkaniyet zemininde kökleri bulunur. Zira devletler nezdinde de sesler bu yönde yükselmeye başlamıştır.¹¹⁴⁰ Ezcümle; siber casusluğun ve bir ülkede ekonomik açıdan olumsuz sonuçlar doğuran siber faaliyetlerin, siber uzayın sağladığı imkanlar çerçevesinde, süreç ve sonuçları itibarıyla fiziksel uzayda alışlagelmiş konseptlerin büyük ölçüde dışına çıktığı görülmektedir. BİT kullanımının hasmane fiillere sağladığı kolaylığın hukuk yoluyla dengelenmesi, hakkaniyete uygun bir yaklaşımdır. Ayrıca “siber ülke” kavramının gövdesi belirginleştikçe, izinsiz giriş gibi eylemler, fiziksel ülkedeki halleri ile paralel biçimde hükme bağlanacaktır.¹¹⁴¹ Sonuç olarak, *de lege ferenda* bir değerlendirme ile de olsa, bu tür devlet fiillerinin uluslararası hukuk bağlamında siber uzayda devlet egemenliğini ihlal edeceği kanaatindeyim.¹¹⁴²

b. Uzaktan Siber Faaliyet ile Siyasi Bağımsızlığa Müdahale Edilmesi

Egemen devletler sisteminin gereği olarak, “ülke” nasıl diğer devletlerin müdahalesinden korunuyorsa, ülke üzerinde egemen olan “siyasi yapı” da aynı gerekçe ile koruma altındadır. Siyasi yapının bağımsızlığı ve iradesinin hürriyeti, temelde self-determinasyon ilkesinin ve ilkeyle temellenip kurulan devletin egemenliğinin bir sonucudur.¹¹⁴³ Gerek ülkesel bütünlüğün gerek siyasi bağımsızlığın korunması, müdahale etmeme ilkesiyle teminat altına alınmıştır. Müdahale etmeme ilkesinin ana hatlarına,

¹¹⁴⁰ Henüz 2024 Temmuz ayında Rusya, UNOEWG-2 kapsamında sunduğu bilgilendirmede, ABD istihbaratının casus yazılımlarla sınır ötesinde gözetleme yapmasını; “*Vaşington, uluslararası arenada kötü şöhretli ‘demokratik değerleri’ savunurken, uygulamada temel insan hak ve özgürlüklerinin korunmasını, BM Şartı’nı ve egemen eşitlik ile devletlerin iç işlerine karışmama gibi temel uluslararası hukuk ilkelerini açıkça ihmal etmektedir*” ifadeleriyle yorumlamıştır; UN/Open-ended Working Group on Information and Communication Technologies, Non-paper "on spyware and its use by US intelligence services" by Russian Federation, Non-papers, 10.07.2024, [https://docs-library.unoda.org/Open-Ended-Working-Group-on-Information-and-Communication-Technologies-\(2021\)/Spyware-and-its-use-by-US-intelligence-services-ENG-0.pdf](https://docs-library.unoda.org/Open-Ended-Working-Group-on-Information-and-Communication-Technologies-(2021)/Spyware-and-its-use-by-US-intelligence-services-ENG-0.pdf) (31.12.2024).

¹¹⁴¹ Heller, bu düşüncenin siber uzayda “tam egemenlik” anlayışını yansıttığını fakat “görelî egemenlik” anlayışına sahip Tallin El Kitabı’nın da etkisiyle az sayıda yazar tarafından savunulduğunu, devletlerden ise ancak Fransa, İran ve İsviçre’nin açık şekilde tam egemenlik yönünde pozisyon almış olduğu belirtmiştir; Heller, s.1499.

¹¹⁴² Tallin El Kitabı’nda da uzmanların bir kısmının, casusluk eyleminin -sızdırılan bilgilerin ehemmiyet ve gizlilik seviyesi itibarıyla- mağdur devlet adına ciddiyeti yüksek olduğu takdirde egemenlik ihlali sayılabileceği yönünde kanaat bildirdiği fakat bu düşüncenin *lex lata*’yı yansıtmadığı gerekçesiyle eleştirildiği ifade edilmiştir; Tallin El Kitabı, s.171. Nihayetinde, arz ettiğim gerekçelerle siber casusluk gelecekte uluslararası hukuka aykırı kabul edilse dahi eşik problemi bu konuda da geçerliliğini koruyacaktır. Belirli ve objektif bir ciddiyet eşliğinin tespit edilmesi, hükmün makul ve adil uygulanması açısından isabetli olacaktır.

¹¹⁴³ Nicholas Tsagourias, “Electoral Cyber Interference, Self-Determination, and the Principle of Non-intervention in Cyberspace”, Dennis Broeders ve Bibi van den Berg (Ed.), **Governing Cyberspace: Behavior, Power, and Diplomacy** içinde (45-64), London: Rowman & Littlefield, 2020, s.51.

Tallin El Kitabı'nda kabul edilen metodolojiye ve buna yönelik eleştirel görüşlere yukarıda Birinci Bölüm'de yer verilmiştir.¹¹⁴⁴ Tallin El Kitabı'nda, doğası itibarıyla hükümete ait olan fonksiyonlar, devletin münhasır yetki alanından; söz konusu fonksiyonların gaspı da müdahaleden ayrılmıştır.¹¹⁴⁵ Ayrıca fonksiyon gaspı için “bir devlet ülkesinde bulunan sunucularda, bir kolluk faaliyeti türü olarak delil toplamaya girişen devlet” örneği verilip; böyle bir eylemin zorlama unsuru içermediği için müdahaleden ayrıştığı ileri sürülmüştür.¹¹⁴⁶ Oysa müdahale yasağı bağlamında zorlama unsuru, bir devleti, bir şeyi yapmaya ya da yapmamaya zorlamaktan ibaret değildir. Daha geniş şekilde, mağdur devletin münhasır yetki alanında iradesi dışında sonuçlar doğurmayı kapsamaktadır.¹¹⁴⁷

Genel olarak, bir X süjesinin belli bir eylemi gerçekleştirmesini sağlamak için diğer Y süjesinin başvurabileceği çeşitli yollar vardır. *Feinberg*, bu spektrumun sırasıyla basit talep, ayartma, ikna ve manipülasyondan, baskı, tehdit, manevi cebir ve fiziksel cebire kadar uzandığını; neyin zorlama sayılacağını belirleyecek çizginin ise ikna ve manipülasyon arasında çizildiğini belirtmiştir.¹¹⁴⁸ Asıl olan, millete (devlete) kendi seçimlerini yaparken makul ölçüde alternatif seçenek bırakılıp bırakılmamasıdır. “Ya paran ya canın” şeklindeki bir tehdidin, muhatap kişiye canından olma seçeneğini de sunduğu gerekçesiyle, kişiyi parasını verme yönünde zorlamadığını söylemek makul değildir. Böyle bir seçeneksiz bırakma, fiziksel güç kullanımı veya tehdidiyle olabileceği gibi farklı enstrümanlarla da gerçekleştirilebilir. *Wheatley* de devletler hukukundaki zorlama eşiğini tespit etme yolunda, kişiler arasındaki zorlama ilişkisi ile analogi kurmayı tercih etmiş ve konuyu bir örnekle açıklamıştır:¹¹⁴⁹

“P, Q'nun bir odada kalmasını istiyorsa şunları yapabilir: kapıyı kapalı tutabilir (cebir (compulsion)), Q'ya odadan çıkarsa onu öldüreceğini söyleyebilir (zorlama (coercion)), Q'ya dışarıda intihar yelekli bir terörist olduğunu söyleyebilir, oysa bu doğru değildir (manipülasyon), Q'ya odadan çıkarsa P'nin üzüleceğini söyleyebilir (yine

¹¹⁴⁴ Bkz. yukarıda, “Müdahale Etmeme ve Karışmama İlkesi”.

¹¹⁴⁵ Tallin El Kitabı, s.24.

¹¹⁴⁶ Ibid., s.22.

¹¹⁴⁷ Roscini, s.155.

¹¹⁴⁸ Joel Feinberg, *Harm to Self*, Oxford: Oxford University Press, 1986, s.189. Ayrıca “compulsion” ve “coercion” için kullanılan “cebir” ve “zorlama” çevirisinin gerekçesine dair bilgi için ve iradeye etkileri bakımından burada bahsedilen kavramlar arasındaki ilişkiye dair örneklerle desteklenmiş çalışma için bkz. Melih Furkan Çiçekçi, “Genel Hukuk Teorisi ve Zorlama Kavramı”, (*Yüksek Lisans Tezi*, Bursa Uludağ Üniversitesi Sosyal Bilimler Enstitüsü, 2024), s.1 vd.

¹¹⁴⁹ Wheatley, 2020, s.179.

manipölasyon), Q'ya odada kalırsa 1.000 dolar kazanacağını söyleyebilir (ayartma) veya sadece Q'dan odada kalmasını isteyebilir (eylem talebi). Her durumda P'nin amacı aynıdır: Q'nun odada kalmasını sağlamak. Ayrım, P'nin Q'ya anlamlı bir seçenek bırakan eylemleri ile bırakmayan eylemleri arasındadır.”

Bir devletin münhasır yetki alanında iradesi dışında sonuçlar oluşturmak, mağdur devleti bir şeyi yapmaya veya yapmamaya zorlama yönünde olabileceği gibi; mağdur devletin münhasır yetki alanındaki iradesinin yerine geçmek suretiyle de gerçekleşebilir.¹¹⁵⁰ Bir devletin mevzuatındaki yetkilendirme şartlarını yok sayıp ülkesinde uydular vasıtasıyla internet erişim hizmeti verilmesi buna örnektir. Bir başka örnek olarak; .gov uzantılı bir devlet kurumunun Web sitesine karşı icra edilen siber faaliyet ile orada beyan edilen bir bilgiyi değiştirmek, sitedeki içeriğin ve site fonksiyonunun işlevi ne olursa olsun devletin münhasır alanına müdahale olarak görülmelidir. Ülkedeki sunuculara erişip delil toplama amaçlı kolluk faaliyeti icra etmek de bu bağlamdadır. Zira .gov uzantılı Web sitesindeki içeriği belirlemek veya ülkesinde bulunan sunucuya gerektiğinde cebren erişmek, devletin kendi siyasi ve hukuki düzeni içerisinde münhasıran salahiyyet sahibi olduğu hususlardandır. Ayrıca bir devletin münhasır alanındaki yetkisini uygun şekilde kullanmasını engelleyecek türden siber faaliyetler de evleviyetle müdahale kapsamında görülebilir.¹¹⁵¹

Devlet kurumlarına ait sosyal medya hesaplarının egemenlikle ilişkisi ise .gov uzantılı Web siteleri kadar belirgin değildir. Bir devlet kurumunun, özel hukuk kişilerinin de aktif bulunduğu bir sosyal ağ üzerinde paylaşımda bulunması, Tallin El Kitabı'ndaki kabule göre doğası itibarıyla hükümete ait bir fonksiyon olarak değerlendirilemez. Bu tür hesapların kullanımında, devlet kurumlarının hizmet sağlayıcılarla ilişkisinin *acta jure gestionis* kapsamında olduğu da açıktır. Fakat devlet ile resmi olarak ilişkilendirilmiş bir hesap üzerinden paylaşılan içeriği belirlemek, ilgili devlet kurumunun iradesine tabidir. Ayrıca bu nitelikteki bir hesaptan yapılan paylaşım nedeniyle devletin uluslararası sorumluluğunun doğuşuna ilişkin girişilecek olası bir sorgulamada fiil, devlete isnat

¹¹⁵⁰ Roscini, s.155.

¹¹⁵¹ Bir devletin fiziksel ülkesinde bulunan internet sükeler üzerindeki yetkisi yukarıda anlatılmıştır. Söz konusu sükelere, devletin yetki icrasını engelleyecek düzeyde dışarıdan anonimlik sağlamak, ilgili verileri manipüle etmek gibi eylemler egemenlik ihlali olacaktır.

edilebilecektir. Dolayısıyla kullanımı münhasıran devlet iradesine isnat edilebilen bir aracın kullanım biçimine karışmak, bu bakımdan egemenlik ihlali olarak görülebilir.

Siyasi bağımsızlığa karşı yönelebilecek en düşük yoğunluklu müdahale ise manipülasyondur. Lakin bu konu da uluslararası hukukun gri bölgesindedir. Konuya hususen eğilen yazarlardan *Wheatley*, manipülasyonu etki bağlamında değerlendirir.¹¹⁵² Yazara göre siber nüfuz faaliyetleri (*cyber influence operations*), yıkıcı propaganda kapsamına girdiğinde ya da maruz kalan devletin hür iradesiyle tercihte bulunması gereken hususlarda iradesine yönelik zorlama teşkil ettiğinde uluslararası hukuka aykırı kabul edilmelidir.¹¹⁵³ Faaliyet türlerine göre ulaştığı sonuçlar şöyledir: Başka bir devletin iç işlerini etkilemek amacıyla vatandaşlarına, ele geçirilen “gerçek bilgileri” açıklamak (*doxfare*), bilgiler yüksek hassasiyette olsa dahi uluslararası hukuka aykırılık oluşturmaz.¹¹⁵⁴ Ancak bilgiler gerçek dahi olsa bir ülkede baskın bir siyasi anlatı geliştirecek ve aksi sesleri bastırarak vatandaşlara sunulan seçenekleri kısıtlayacak ölçüde haber ve yorum bombardımanı, müdahale etmeme ilkesini ihlal eder.¹¹⁵⁵ Bir devletin münhasır alanındaki işleyişi zorlama ölçüsünde değiştirme kabiliyetine sahip yalan haberler (seçim öncesi, bir adayın reşit olmayan kişiyle cinsel ilişkisine dair kurmaca görsel unsurlarla desteklenmiş yalan haber örneğindeki gibi) müdahale niteliğinde sayılabilir.¹¹⁵⁶ Millet iradesinin sağlıklı teşekkül etmesini engelleyecek, karar alma mekanizmalarını kilitleyecek ölçüde dezenformasyon faaliyetleri de müdahale yasağına aykırıdır.¹¹⁵⁷ Bu yorumlar tabii ki etki temelli yaklaşımın ürünüdür. Haber ve yorum bombardımanı, yalan haber, dezenformasyon, kamu düzenini ve seçmen davranışlarını etkilemek için sosyal ağlarda algoritma kullanımı gibi yöntemler, ekonomik yaptırımlara benzer şekilde taraflara ve kabiliyete göre etki derecesi açısından değişiklik gösterir. Ekonomik ve siyasi açıdan çok güçlü bir devletin, çok zayıf olan bir devlete karşı ekonomik yaptırım tehdidi ile zayıf olanın kuvvetli olana karşı tehdidi, kesin olarak irade üzerinde aynı zorlayıcılıkta değildir. Sonuçta ortada bir hukuka aykırılık ve egemenlik

¹¹⁵² Wheatley, 2020, ss.187-197

¹¹⁵³ Ibid., s.187.

¹¹⁵⁴ Ibid., s.188.

¹¹⁵⁵ Ibid., s.190.

¹¹⁵⁶ Ibid., s.191.

¹¹⁵⁷ Ibid., s.195.

ihlali olduđu kabul edilecekse, bunun deęerlendirmesi, eylemin nitelięinden de doęurduđu etkiye g re  ekillenecektir.

Devletlerin fiili durumları arasında zaman zaman uęurum derecesine ulařan farklılıklar, egemenlik d ř ncesinin yumuřak karnıdır. Organize ikiye zl l ę n meřhur bir veęhesi de k ğıt  zerinde b t n devletlerin egemen olduđu kabul edilmesine raęmen fiiliyatta bazı devletlerin egemen vasfının gerektirdięi  zelliklerden b y k  lę de yoksun olmasındır. Egemenlik ne kadar idealize edilse de uluslararası iliřkilerin uluslararası hukuk uygulamasındaki etkisi yalıtılamayacaęından, kural dıřlıklar ve sapmalar kaınılmazlıęını s rd recektir. Bilhassa k reselleřme, getirdięi yenilik ve imkanlarla devletlerin egemen yapılarını g n ll  veya g n ls z řekilde ařındırmaktadır.¹¹⁵⁸ Egemenlięin devlet kapasitesiyle iliřkisine bu geręeęi g z ardı etmeden bakmak gerekir. Hele ki siber uzay baęlamında devletlerin siber kapasiteleri, m nhasır yetki alanlarındaki kontrol ve yetki icrası iin ok daha belirleyici niteliktedir. Dolayısıyla somut olaylarda egemenlik ihlalinden bahsederken, devletlerin mutlak egemenlik konumundan iradi veya “ister istemez” sapmaları ile gerek ihlalleri ayırt edecek bir makuliyet  l s  dahilinde deęerlendirme yapmak gerekecektir.

Bilhassa  lkelerdeki seimlere y nelen siber n fuz faaliyetleri iin gerek literat rde gerek devlet pozisyonlarında hukuka aykırılık d ř ncesi g lenmektedir.¹¹⁵⁹ Lakin siber uzaya iliřkin birok mevzuda olduđu gibi burada da genel bir uluslararası antlařmanın yokluęunda, bu y nde bir uluslararası  rf ve  det hukuku kuralının oluřtuęunu s ylemek hen z g  g r nmektedir.¹¹⁶⁰

¹¹⁵⁸ H seyin Sevim, “Uluslararası İliřkilerde K reselleřme Olgusu ve Ulus-Devlet Kavramını Yeniden D ř nmek”, **Uluslararası İliřkiler Dergisi**, Cilt.3, Sayı.9, (2006), ss.105-115

¹¹⁵⁹ Bařta in, Rusya ve İran olmak  zere siber egemenlik destekisi devletlerin konu hakkındaki yaklařımları hakkında bkz. Lahmann, s.80 vd.

¹¹⁶⁰ Roscini, s.400.

SONUÇ

Modern uluslararası hukukun asli unsuru olan egemen devletler, siber uzay üzerinde de egemendir. Bu basit önerme cümlesi, yüzlerce yıllık bir sürecin sonucunda kurulabilmektedir. Önce modern egemen devlet, çeşitli siyasal iktidar yapıları içinden sıyrılarak günümüze ulaşmış; siyasal iktidar yapıları arasındaki hukuki ilişki türleri içinden de egemen devletler arasındaki hukuku ifade eden uluslararası hukuk aynı başarıyı yakalamıştır. Siber uzay kavramı ise gelişen teknoloji sayesinde on yıl içinde bilimkurgudan hukuk literatürüne hızlı bir geçiş yapmıştır. Her şeyin her şey ile alakalı olduğu hakikatince, söz konusu olguların analizi için her şeyden bahsedilmesi mümkün ve faydalı olacak olsa da bir tez çalışması içerisinde ancak daha alakalı olan şeyler üzerinden hareket edilebilmektedir. Eldeki çalışmada da konu bütünlüğünün korunması için çizilmesi zaruri olan sınırlar müsaade ettiği ölçüde birçok husus incelenip, nihayetinde elde edilen bu paragrafın ilk cümlesinin ispatı ve muhtevasının tespiti adına bazı sonuçlar aktarılmıştır.

Siber uzayın kökleri, sibernetik kavramında aranmış; siberin popüler bir ön eke dönüşürken geçirdiği anlamsal değişim, sibernetiğin ortaya çıkışı ve mahiyeti üzerinden açıklanmıştır. Yönetim bilimi ve sistem teorisi zemininde neşvünema bulan ifade, bilgi ve iletişim teknolojileriyle ilişkili her olgu için kullanılır hale gelmiştir. Bu bağlamda literatürde karşılaşılan bazı bilgi ve kavram karışıklıkları da açıklığa kavuşturulmuştur.

Siber uzayın aslında ne olduğuyla ilgili görüş farklılıkları değerlendirilerek hem vakıayı isabetle karşılayacak hem kavramın devlet egemenliğiyle ilişkilendirilmesine uygun düşecek bir tanım tespit edilmeye çalışılmıştır. Bu vetirede öncelikle kavramın orijinindeki sanal gerçeklik fikrinden zamanla uzaklaşıldığı; daha gerçek bir zemine oturtulmasına yönelik bazı tanımlarda da “ağlar ağına” yani özünde internete vurgu yapıldığı görülmüştür. İncelemeler sonucunda siber uzay kavramının, somut olmamakla birlikte ismiyle müsemma, bir uzay olduğu; bu uzayın da mekânsallık anlamında bir “alan” olmaktan ziyade “teorik uzay” kategorisine girebileceği kanaatine varılmıştır. Bu bakımdan, “devletin siber uzayda egemen olması” ifadesi esasen “devletin siber uzay üzerinde egemen olması” durumunu karşılamaktadır. “Orta Dünya” benzeri hayali bir mekânın, fiziksel uzaya hâkim devletlerin egemenliğiyle ilişkilendirilmesi abesle iştigal

edecektir. Bununla birlikte, teknolojinin insan algısına sunduğu dijital ve sanal unsurların birer vakıa olduğu ve yapılarının düzenlenebilirliği de herkesçe malumdur. Sonuç olarak siber uzay fikri, siyasal iktidar müdahalesine açık bu olguların konumlandırılması, haritalanması ve iktidar ile ilişki biçimlerinin tespiti adına işlevsel bir kavram doğurmuştur. Eldeki çalışmada insan ve dijital verinin, fiziksel ve mantıksal boyutlar içindeki konum ve hareketlerinin belirlenmesine imkân sunacak bir teorik uzay düşüncesi kabul edilmiştir. Bu düşüncenin zemini de literatürdeki katmanlı yaklaşımlara dayanmaktadır. Ayrıca internet – Web – siber uzay ilişkisinin çözümlemesi de bu yolla yapılabilmektedir.

İnsan ve cansız varlık ilişkisinde “siber” noktasına geliş, mantıksal boyutun varlığı ile gerçekleşir. Bu durum, siber uzayın mantıksal boyuttan ibaret görülmesi illüzyonunu doğurmuştur. Devletin “sanal alemi” düzenlemesinin imkânı da uzun müddet aynı bağlamda tartışılmıştır. Gelineen noktada hem öğretinin hem uygulamanın daha kapsayıcı ve bütüncül yaklaşımlara yöneldiği görülmüştür. Çalışmada veri – bilgi ilişkisinde literatür ve mevzuattaki karışıklığa da dikkat çekilmiş, kavramlar arasındaki fark siber uzay bağlamında açıklanarak, ifadelerin kullanımında hassas davranılması gerektiği vurgulanmıştır.

Siber uzayın boyut ve unsurlarını -ayrıca boyutların da kendilerini oluşturan unsurlarını- ortaya koymak, her tür iktidarın olası temas alanlarının tespitini sağlamıştır. İktidar türleri arasından siyasal iktidar söz konusu olduğunda da siyasal iktidar türleri arasından tekelleşerek bugüne ulaşan modern egemen devletin ne olduğunu açıklamak gerekmiştir. Siyasi iradenin ve doğruyu belirleme iktidarının, ulus ve ulus devlet kavramlarının doğuşuyla geldiği konumun tespiti, bu açıklamanın çekirdeğini teşkil etmiştir. Tanrısal vasıflar atfedilen modern devletler arasındaki ilişkiler de Yunan mitolojisindeki Olimpos Dağı’nı andıran uluslararası hukuk nezdinde düzenlenmektedir. Böyle bir kabul zincirinin, işlevselliğinin yanında arızaları da getirmesi kaçınılmaz olmuştur. Eldeki çalışmada da siber uzay bağlamına geçmeden önce, devletlerin egemenliği esasına dayalı uluslararası hukuk sistemini ortaya çıkaran şartlara ve mevcut anlayışa yönelik eleştirilere yer verilmiştir. Pozitif hukuka dönüldüğünde ise devlete

egemen sıfatının sağladığı vasıfların, insanın temas ettiği bütün olguları olası bir iktidar konusu haline getirdiği görülmüştür. Siber uzay da bunlardan biridir.

Devletin siber uzay üzerindeki iktidarı, çok kez vurgulandığı üzere siber uzayın sınır aşan yapısı itibariyle, uluslararası hukukta devlet egemenliğine hâkim ilkelerle sıkı bir bağımlılık ilişkisi içindedir. Çalışmada, siber uzay üzerinde devlet egemenliğinin tespiti ve uygulanması için bir referans alanı oluşturmak amacıyla bu ilkelerin incelenmesine yer verilmiş; devamında da siber uzay üzerinde devletin egemen olduğu çıkarımının ve buna dayanarak varılan sonuçların çoğunun, söz konusu ilkelerle uyumlu olduğu sonucuna varılmıştır. Öğretide ve uygulamada görülen bazı yaklaşımlar, ilkelere aykırılık teşkil ettiği kanaatine varılarak eleştirilmiştir.

Siyasal iktidarın temel fonksiyonları, belli bir alan içinde karar vermek, kural koymak ve bunu uygulamaktır. Siber uzay üzerindeki egemenlik, siber uzayın hukuki düzenlemelere konu olabilirliliği kabulüne dayalıdır. Siber uzayın özellikleri, ortaya çıktığı dönemde, düzenlenebilirliğin doğrudan kabulünü sorgulanabilir kılmıştır. Literatürdeki tartışmalar, siber uzayın hukuki düzenlemelere konu olabileceği sonucuna ulaşırken bunun gerekliliğini, makuliyetini ve usulünü de yoğun şekilde ele almıştır. Sürecin doğru değerlendirilebilmesi adına eldeki çalışmada bir dönemlendirme girişiminde bulunulmuştur. Öğretinin erken, klasik ve modern dönemlerdeki gelişimi, dönemlerin karakteristik özellikleriyle anlatılmıştır.

Erken dönemde henüz siber uzay terimi kullanıma girmemişken bilişim hukukunun ilk sorunları ortaya çıkmaya başlamıştır. 1990'lı yıllarda hızla hukuk literatürüne giren siber uzaya mekansallık izafe etmek ve metaforik yaklaşımlar üzerinden analogiler kurmak, klasik dönemin hâkim tercihi olmuştur. Siber uzayın düzenlenemeyeceği fikrinin savunulmasıyla tartışmaların zirve noktasına ulaşması da klasik dönemin son demlerine tekabül etmiştir. Devletlerin hızla oyuna müdahil olduğu modern dönemde, düzenleme karşıtı görüşler törpülenmiş fakat düzenlemeci yaklaşımlara getirilen eleştiriler de kesilmemiştir. Metafor ve analogilere başvurma geleneği halen devam ediyor olsa da artık genellikle, siber uzaya dair sorunların neye benzediğinden çok, ne olduğu sorusuna cevap aranmaktadır. Mimariyi belirleyen kodun siber uzay için Yasa olduğu ve hukukun kodu düzenleyebileceği görülmüştür. Modern

dönem yaklaşımları, At Hukuku eleştirisini de büyük ölçüde gündemden düşürmüştür. Hayattaki bütün meselelere genel ilkeler üzerinden yorum ile hukuki çözüm getirilebileceği gibi; her bir meseleyi ayrı ayrı düzenleyen normlar ihdas edilmesi yoluna da gidilebilir. Eldeki çalışmada, ideal olanın iki uç arasında bir denge noktası yakalamak olduğu sonucuna ulaşılmıştır. Siber uzay için bu denge noktasının, “Bilişim Hukuku” disiplinin gelişimiyle yakalanacağı düşünülebilir.

Siber uzayın hukuk ile düzenlenmesindeki etkisi ve önemi itibariyle; her bir devletin kendi ülkesinde ihdas ettiği ulusal hukuk normları ve devletlerden müteşekkil uluslararası topluluğun iradesiyle belirlenen uluslararası hukuk normları at başı gitmektedir. Hal böyle olunca mercek uluslararası hukuka çevrilerek, siber uzay ile ilişkili hususları konu edinen belli başlı uluslararası antlaşmalara değinilmiş, antlaşmaların getirdiği yenilikler ve eksik yönleri ele alınmıştır. Bilişim suçlarıyla mücadele ve siber güvenlikte iş birliği konulu bölgesel antlaşmalar uluslararası hukukun önemli kazanımları olsa da siber uzay gibi küresel bir olguyu kapsamlı biçimde ele alan geniş katılımlı bir uluslararası antlaşmanın yokluğunun birtakım sorunlar doğurduğu görülmüştür. Bilhassa BM bünyesindeki çalışma gruplarına sunulan belgelerden ve devletlerin ulusal hukuk düzenlemelerinden, siber uzayda devlet egemenliğinin esaslarına ve siber uzayın düzenlenme ile yönetim usullerine dair yorumlanmış biçimindeki yaklaşım farklılıkları kolayca tespit edilebilmiştir. Başta politik menfaatler olmak üzere birçok sebebe dayanabilen bu görüş ayrılıkları, küresel bir mutabakata varılmasını oldukça güçleştirmektedir. Nihayetinde siber uzay politikası bağlamında devletler iki ana gruba ayrılmıştır. Devletlerin ideolojik tutumları bir yana, siber uzay yönetişimi konusunda ABD öncülüğündeki grup, pozisyonunu küresel ve serbest internet anlayışı üzerine inşa edip mevcut yönetim modelinin çok paydaşlı katılımı ile sürdürülmesini savunurken; Çin ve Rusya öncülüğündeki diğer grubun, devlet egemenliğini ön plana çıkarıp, mevcut yönetim modelinin mümkün olduğunca uluslararası topluluk nezdine çekilmesi gerektiği ısrarıyla BM ve ITU’yu adres gösterdiği belirtilmiştir. Bu ve benzeri gerilim hatları dahilinde, uluslararası hukukun ve iş birliğinin gidişatına dair hem betimleyici bir çerçeve çizilmiş hem de geleceğe yönelik öngörülere elverişli bir zemin oluşturmaya çalışılmıştır. Neticede bütün teorik ve teknik çabalara rağmen, bu konuda da hukukun akıbetinin siyaset ve güç dengelerine göre şekillenmesi kuvvetle muhtemeldir.

Egemenlik, özünde son derece soyut ve muğlak bir kavramdır. Egemenlik fikri üzerine inşa edilen hukuki ve siyasi müesseseler vasıtasıyla birtakım somut ve keyfiyeti belirli görünümeler teşekkül etmiştir. Devletin yasama, yürütme ve yargı erkleriyle ülkesi ve vatandaşları üzerindeki yetkilerini icra etmesi, iç egemenliğin; diğer devletlerle ilişkisinde bağımsız ve diğer devlet yargılarından bağışık olması, dış egemenliğin sonuçları olarak kabul edilir. Bu ayrıma dayanarak, öncelikle devletin siber uzaydaki yetkisine ilişkin hususlar; sonrasında da devletin siber uzaydaki münhasır alanının diğer devletlerin müdahalesinden korunmasını ifade eden siber egemenlik düşüncesi ve sonuçları incelenmiştir.

Fiziksel boyutu oluşturan öğeler üzerindeki yetki genel olarak daha yerleşik esaslara tabidir. Nitekim ülkesellik, siber uzaya dair birçok yetki probleminin çözümündeki ilk dayanaktır. Fiziksel olan hemen her şeyin de ülke ile irtibatının kurulması mümkündür. Ancak siber uzayın fiziksel boyutu, ülkesel egemenliğe istisna teşkil eden alanlara da uzanmaktadır. Bu durum, açık deniz sualtı kabloları ve siber kapasiteli uydular ile uzay araçları hakkında süregelen tartışmaların kaynağıdır. Söz konusu unsurların bilhassa kötü niyetli müdahalelerden korunmasına yönelik uluslararası düzenleme ihtiyacının sürdüğüne dikkat çekilmiştir.

Siber uzayın kişi unsuru, işlev ve eylemlerine göre kategorilere ayrılmıştır. Siber uzayın en az bir boyutuyla herhangi bir şekilde irtibatı olan her bir gerçek veya tüzel kişi, bu kapsama girmektedir. Çalışmada, sayısız irtibat türü içerisinde devletin yetkisine dair sorunlarla en çok ilişkili olanların seçilmesi gerekmiştir. Dolayısıyla ilk olarak “internet sükjeleri” üzerindeki yetki problemi masaya yatırılmıştır. Öncelikle internet sükjeleri tasnif edilmiş, kişilerin hangi eylemleri gerçekleştirdiğinde hangi sıfatları kazanacağı açıklanmış; her bir sükje tipinin üzerinde hâkim olan yetki ve sorumluluk rejimi tespit edilmiştir. Mevzubahis ister internet sükjeleri olsun ister siber uzayın diğer kişileri, yetki bakımından esas problemin ülke dışındaki kişiler üzerindeki yargı yetkisinin kullanımı olduğu sonucuna ulaşılmıştır. Malum olduğu üzere bu sorun, uluslararası hukukun genel bir sorunudur. Devletler, köstebek vurma oyununa devam etmektedir. Siber uzayın önemi ise ülke dışında gerçekleşip ülke içinde etki doğuran fiilleri ve çeşitlerini radikal ölçüde arttırmasından kaynaklıdır. Siber uzay ile ilişkili eylemlerde bulunan milyarlarca insan

ve binlerce şirket, herhangi bir ülkede etki doğurabilmektedir. Bu etki, sadece sağlanan bir içeriğin ülke içinde erişilebilir olması şeklinde görülebileceği gibi; kamu güvenliğini tehdit edecek, ülke ekonomisini derinden sarsacak, hatta fiziksel yıkıma ve can kaybına neden olacak şekilde de gerçekleşebilir. Bu nedenle makul ve meşru bir yetki iddiasının dayanması gereken esasların tespiti için öğretilerde görüşler çalışmada ele alınmıştır. Mevcut şartlarda nitelikli etki doktrini, sorunun çözümü adına en öne çıkan yaklaşım olarak kabul edilmiştir. “Öngörülebilir, doğrudan ve esaslı” tabiriyle tanımlanan nitelik eşiğinin tespitinin objektif zemine oturtulması ise devlet uygulamalarıyla gelişecek bir ortak anlayışla mümkün olabilecektir. AB mevzuatında, birçok ulusal kanunda ve yargı kararında belli başlı fiillerin ülke içinde etki doğurduğu kabulünü yansıtan kriterler belirlenmeye başlamıştır.

Otonom araçların eylemlerinde ve yapay zekâ sistemleri tarafından üretilen içeriklerde isnat sorunu, devletin yetkisi bağlamında ele alınmıştır. Konuya dair öğretilerde tanımlara ve görüşlere genel olarak yer verilmiştir. Bu noktada genellikle üzerinde durulan sorunun, hukuka aykırılıklarda ve zarar durumlarında sorumluluğun hangi süjeye yükleneceğinin belirlenmesi olduğu görülmüştür. Sorumluluk rejiminin tespiti çalışma kapsamı dışında kaldığı için, aktarılan tespitlerle iktifa edilmiş; herhangi bir usulle belirlenen sorumlu süjenin, diğer süje tipleriyle aynı yetki rejimine tabi olacağı belirtilmiştir.

Mantıksal boyut ve dijital veri, siber uzayın en özgün elemanlarıdır. İnsan algısındaki karşılığı soyut ve sanal nitelikte olan mantıksal boyut, en başından bu yana siber uzay ve hukuk bağlamındaki tartışmaların merkezinde yer almaktadır. Hukuki belirliliğin sağlanabilmesi adına, mantıksal boyutun ele alınışının -mümkün olduğunca- metaforik zeminden realist zemine çekilmesi için çaba sarfedilmiştir.

Egemenliğin mantıksal boyuttaki görünümleri içerisinde ilk olarak fikri mülkiyet meselesi seçilip değerlendirilmiştir. Ulusal ve uluslararası hukuk normlarından örneklerle devletlerin, dijital unsurların fikri mülkiyetine dair düzenleme yetkilerini nasıl kullandıklarına ve konuya ilişkin yaklaşımlarına değinilmiştir. Dijital unsurlar üzerinde fikri mülkiyet korumasının, sürdürülebilirlik ve gelişmenin finansmanı gibi çeşitli hususlarda önemli ve gerekli olduğu kabul edilmiştir. Ancak kullanmakla ve paylaşmakla

tükenmeyen dijital unsurların “ortak olmayan malların trajedisine” mahkûm edilmemesi için, mevcut fikri mülkiyet rejiminin tekrar gözden geçirilmesi ihtiyacı vurgulanmıştır.

Mantıksal boyutun en önemli unsuru, internet üzerinde işleyen mantıksal yapıdır. Bu yapının da yine en önemli unsurları Web siteleri ve barındırdıkları içeriklerdir. Devletler tüm bu unsurlar üzerinde gözetim ve denetim yetkilerini kullanarak; gerekli durumlarda içerik kaldırma, filtreleme ve erişimi engelleme gibi önlemlere yaygın şekilde başvurabilmektedir. Söz konusu süreçlerde özgürlük ve güvenlik ikilemi belirgin biçimde ön plana çıkmaktadır. Her bir devletin izlediği politika ve korumayı öncelediği menfaatler farklılık arz edebilse de hukuka aykırılık durumlarında imkân dahilindeki önlemleri almaktan kaçınmadıkları tespit edilmiştir. Bu başlıktaki devlet uygulamaları, kullanıcıların ve özel sektör temsilcilerinin sıklıkla şikâyet ve itirazlarına sebep olsa da devletin kendi münhasır alanına tesir eden bir olguya göz yummasını beklemek, egemenlik tanımı gereği imkân dışıdır. Özellikle de bir devlet ülkesinde etkin biçimde hizmet sunarken o devletin hukukuna aykırı eylemlerde bulunma hakkının bir ayrıcalık olarak Web sitesi veya uygulama işletmecilerine tanınmasına makul bir gerekçe sunmaktaki güçlük aşıkardır. Elbette devletlerin ilgili yetkileri politik saiklerle kötüye kullanma ihtimali mevcuttur. Fakat söz konusu ihtimal, devletin yetki kullanımlarının hemen hemen hepsi için geçerlidir. Böylesine genel bir problemin önüne geçme yolunun, internet ve Web’e istisnai ve dokunulmaz bir konum öngörmekten geçtiğini düşünmek, isabetli bir yaklaşım olmayacaktır. Hatta karşı zaviyeden bakıldığında, devletlerce başvuru alan önlemlerin Web’de karşılaşılan hukuka aykırılıkların engellenmesi, giderilmesi ve faillerin yaptırıma tabi tutulması hususlarındaki yetersizliği de görülecektir. Ancak bu yetersizlik, hukukun ve icrasının zaaflarından çok, siber uzayın mimarisinden kaynaklanmaktadır. Devletler, hukukun siber uzaydaki sükeler üzerinde icra edilebilirliğinin sağlanması için mimarinin uygun şekilde teşekkül etmesini sağlamaya çalışmalıdır. Örneğin anonimlik, belli mecralarda ve belli ölçülerde kabul edilebilir ve hatta teşvik edilebilir. Ancak siber uzay mimarisi, hukukun gerektirdiği durumlarda kimlik tespitinin tamamen imkânsız hale gelmesinin önüne geçilecek şekilde kurgulanmalıdır.

Devletin veriler üzerindeki yetkisi, genellikle kişisel verilerin korunması bağlamında değerlendirilmektedir. Bulut bilişimin yaygınlaşması ile bazı devletler, vatandaşlarına ait verilerin yerleştirilerek ülke içindeki sunucularda tutulmasını hizmet sağlayıcılar için şart koşmaya başlamıştır. Bu çalışmada genel hukuki durumun ortaya konulmasının yanı sıra büyük veri kavramı da holistik bakışla ele alınarak, salt rızaya dayalı klasikleşmiş kişisel veri rejimine yeni yaklaşımlar getirilmesi gerekliliği vurgulanmıştır. Böylece kullanıcı cephesinde geçerli paylaşım kısıtlamaları, veri türüne göre ek şartlar, veri akışına veya depolama miktarına dair kotalar gibi önlemlere başvurulabilecektir.

Mantıksal boyut üzerinde devletin yetkisine ilişkin son inceleme, finansal teknolojileri konu edinmiştir. Para akışının dijitalleşmesi, blokzincir teknolojisinin gelişimi, kripto varlıkların yaygınlaşması, fintek sektörünün büyümesi gibi gelişmeler, sağladığı büyük fırsatın yanı sıra devletlerin finans alanındaki birçok menfaatini de tehdit etmiştir. Son dönemde bu alana yönelik düzenleyici faaliyetlerin hızlandığı gözlemlenmiştir. İhvas edilen düzenlemelerin önde gelenleri ve devlet pozisyonlarındaki çeşitlilik mukayeseli olarak ele alınmıştır.

Bir devletin egemenliğinin diğer devletlere bakan yönü, ülkesel bütünlüğünün ve siyasi bağımsızlığının dokunulmazlığını ifade eden dış egemenlik terimiyle adlandırılmaktadır. Fiziksel uzayda dış egemenliğin teoriden pratiğe geçişi en başta sınır çizgileriyle temsil edilir. Siber uzayda devlet egemenliği, klasik dönemde daha çok siber uzayın düzenlenmesiyle ilişkilendirilmiştir. Düzenleme kültürü oturdukça, devletler siber uzayda münhasır yetki alanları ileri sürmeye başlamıştır. Böylece siber uzay hakkındaki mekânsallık tartışmalarına bir de ülkesellik tartışması eklenmiştir. Modern devletin vasıflarından olan sınır çizgilerinin siber uzayda çizilmesi fikri, “siber egemenlik” kavramını böylece yeni bir boyuta taşımıştır. Bu süreçte ortaya çıkan bir diğer kavram da “siber ülke” olmuştur.

Öğretide siber egemenliğin siber Vestfalyacılık olarak yorumlanması, siber uzayın *res communis* olduğunun ileri sürülmesi, kritik altyapılar üzerindeki egemenliğin siber ülke için bir nüve olarak görülmesi gibi yaklaşımlarla süregelen yoğun tartışmalar halen devam etmektedir. Eldeki çalışmada, söz konusu tartışmalar incelenmiştir.

Devletlere ait -varsa- münhasır yetki alanlarının ve sınırların belirlenmesi gündeme geldiğinde; siber uzayın teorik bir uzay olarak tanımlanması, ilk bakışta ayrı bir mekân olarak kabul edilmesi kadar işlevsel görünmemektedir. Fakat çalışmada benimsenen usul, siber uzayı yekpare bir mekân olarak ele almak yerine analitik yaklaşımla değerlendirmektir. Metaforik düşünceyle sanal bir mekânı bölümleyip, “bu bölge devletin ülkesidir” demek hukuk adına sağlıklı bir metot değildir. En realist yaklaşım, teorik bir uzay olan siber uzayda devletin egemenlik iddialarına konu olan bütün unsurları ayrı ayrı noktalar halinde değerlendirmektir. Böylece analiz yönteminde isabet oranı artacak ve hukuk için aranan belirlilik ve öngörülebilirlik kriterlerine daha uygun bir sonuç elde edilecektir. Fakat yine holistik yaklaşımla bütün bu noktaları birleştirip anlamlı bir gövde oluşturmak da birçok açıdan sağlayacağı faydaya binaen tercih edilebilir. Hatta ortaya çıkan gövde, kendisini oluşturan noktaların toplamından farklı bir şey olacağı için, hukuka konu edilmesinde doğacak nüanslar da kıymet arz edebilir. Sonuç olarak çalışma içinde de ifade edildiği gibi; *“siber uzayın ayrı bir mekân olarak ele alınıp, bu mekândaki egemenliğe tabi bölümlerin tespit edilmesine dayalı yöntem bir yana; mezkûr noktaların birleştirilmesiyle oluşan gövdeyi mekânsal terminolojiyle değerlendirmek de mümkündür”*. Bu yöntem ile “siber ülke” fikri de daha belirli bir zemine oturacaktır.

Eldeki çalışmada incelenen ve sonuçlar elde edilen son husus, siber uzayda egemenliğin ihlali olmuştur. “Her şey zıddıyla kaimdir” düsturunca, bir olgu üzerinde egemenlikten bahsedilebildiği takdirde egemenliğin ihlalinden de bahsedilecektir. Ancak ihlal edilebilirlik söz konusu olduğunda, egemenliğin bir ilke mi yoksa bir kural mı olduğu sorusu gündeme gelmiştir. Uluslararası hukukta bir ilkenin ihlal edilmesinin sonuçları ile bir kuralın ihlal edilmesinin sonuçları arasında fark olduğu düşüncesiyle başlayan akademik tartışmalar güncelliğini korumaktadır. Ancak özellikle UAD kararlarında bu ayrıma gidilmemiş olması ve pratikteki sorunlara çözüm getirecek asıl hususun; ilke mi kural mı sorusuna cevap aramaktansa, hangi fiillerin siber uzayda devlet egemenliğini ihlal edeceğine dair eşiği tespit etmek olduğunun görülmesi sonucunda, bu tartışmanın aktarımı ile iktifa edilmiştir.

Uluslararası hukukta egemenlik ancak devletlere tanınmıştır. İhlal ise uluslararası hukuk süjesi olmaları hasebiyle hem devletler hem uluslararası örgütlerce

gerçekleştirilebilir. Egemenliği ihlal eden fiiller, kuvvet kullanma ve müdahale yasakları bağlamında incelenmiştir. İncelemede sıklıkla Talin El Kitabı'na başvurulmuştur. Devlet tarafından icra edildiğinde egemenlik ihlali olarak nitelendirilecek siber faaliyetler hakkında uygulamadaki en büyük güçlüğü, faaliyeti devlete isnat etmekte olduğu görülmüştür. İsnadın kısmen de olsa yapılabildiği vakalar aktarılmıştır.

Devlet egemenliğini ihlal eden siber faaliyetler, egemenliği ihlal edilen devlet ülkesinin içinde veya dışında gerçekleşmesine göre iki ayrı başlıkta ele alınmıştır. Devamında da ülke dışında icra edilen -uzaktan- siber faaliyetler, BM Şartı m.2/4 hükmündeki ifadeyi yansıtır şekilde, ülkesel bütünlüğe ve siyasi bağımsızlığa karşı yönelmesi bakımından yine iki ayrı başlıkta incelenmiştir.

Ülkede fiziksel zarara veya vatandaşların ölümüne ya da yaralanmasına sebebiyet veren siber faaliyetlerin kuvvet kullanma yasağını ihlal ettiği artık genel olarak kabul görmektedir. Doğrudan fiziksel zarar doğurmamakla birlikte siber unsurlarda işlev kaybına sebebiyet veren faaliyetlerin de mağdur devletin egemenliğini ihlal ettiği kabul edilmiştir. Fiziksel zarara veya işlev kaybına sebep olmaksızın sosyal, ekonomik vb. zararlar doğuran siber faaliyetler yahut mantıksal boyuta veya verilere yönelmiş izinsiz giriş gibi faaliyetler için ise eşik tartışmaları sürmektedir. Bu gri bölgenin en önemli unsurlarından olan siber casusluğun mer'i uluslararası hukuk hükümlerine göre egemenlik ihlali olarak kabulündeki güçlük görülmekle birlikte, en azından *de lege ferenda* bir değerlendirme ile uluslararası hukuk bağlamında siber uzayda devlet egemenliğini ihlal edeceği kanaati bildirilmiştir. Siyasi bağımsızlığa müdahale edilmesine gelindiğinde, konu müdahale etmeme ilkesi çerçevesinde değerlendirilmiştir. Çalışmada, müdahale etmeme ilkesine dair tartışmalı hususlar Birinci Bölüm dahilinde aktarılmış; Üçüncü Bölüm sonunda ise bu hususların siber uzaya nasıl yansıdığına ilişkin gözlemler aktarılmıştır.

KAYNAKÇA

Kitaplar

- Abbate, Janet, **Inventing The Internet**, Cambridge, Massachusetts, London: The MIT Press, 1999.
- Ağaoğulları, Mehmet Ali, Cemal Bali Akal ve Levent Köker, **Kral Devlet ya da Ölümlü Tanrı**, Ankara: İmge Kitabevi Yayıncılık, 1994.
- Akal, Cemal Bali, **İktidarın Üç Yüzü**, Birinci Baskı, Ankara: Dost Kitabevi, 1998.
- Akal, Cemal Bali, **Modern Düşüncenin Doğuşu: İspanyol Altın Çağı**, 2. Baskı, Ankara: Dost Kitabevi Yayınları, 1997.
- Akın, İlhan F., **Devlet Doktrinleri**, 3. Baskı, İstanbul: Beta, 2016.
- Akıncı, İrem, **Kripto Varlıkların Mukayeseli Hukuk Açısından İncelenmesi ve İncelemelerin Türk Hukukuna Uygulanabilirliği**, İstanbul: On İki Levha Yayıncılık, 2024.
- Aksar, Yusuf, **Teoride ve Uygulamada Uluslararası Hukuk – 1**, 6. Baskı, Ankara: Seçkin Yayıncılık, 2021.
- Alsın, Zeki Mesud, **Devletler Hukuku Dersleri**, Ankara: T.C. Millî Eğitim Bakanlığı Siyasal Bilgiler Okulu Yayınları, 1947.
- Amerasinghe, Chittaranjan F., **Diplomatic Protection**, Oxford University Press, 2008.
- Ampère, André Marie, **Essai sur la Philosophie des Sciences ou Exposition Analytique d'une Classification Naturelle de Toutes les Connaissances Humaines: Seconde Partie**, Paris: Bachelier, Libraire-Éditeur, Quai Des Augustins, 55, 1843.
- Aristoteles, **Politika**, Mete Tuncay (Çev.), 16. Basım, İstanbul: Remzi Kitabevi, 2010.
- Baran, Paul, **On Distributed Communications Networks**, The RAND Corporation, R-2626, Santa Monica, 1962.
- Başeren, Sertaç Hami, **Uluslararası Hukukta Devletlerin Münferiden Kuvvet Kullanmalarının Sınırları**, Ankara: Ankara Üniversitesi Basımevi, 2003.
- Berners-Lee, Tim, **Weaving the Web: The Original Design and Ultimate Destiny of the World Wide Web by It's Inventor**, New York: Harper Collins Publishers, 2000.
- Betts, Raymond F., **Decolonization: The Making of the Contemporary World**, Second Edition, Cornwall: Routledge, 2004.

- Betz, David J. ve Tim Stevens, **Cyberspace and the State: Towards a Strategy for Cyber-Power**, London: Routledge, The International Institute for Strategic Studies, 2011.
- Beyer, Jessica Lucia, **Expect Us: Online Communities and Political Mobilization**, New York: Oxford University Press, 2014.
- Bilsel, Cemil, **Devletler Hukuku: Giriş**, İkinci Bası, İstanbul: İstanbul Üniversitesi Yayınları, 1940.
- Bilsel, Cemil, **Milletlerarası Hava Hukuku**, Cilt.1, İstanbul: İstanbul Üniversitesi Yayınları, 1948.
- Bowett, Derek W., **Self-Defence in International Law**, Manchester: Manchester University Press, 1958.
- Brownlie, Ian, **Principles of Public International Law**, Seventh Edition, New York: Oxford University Press, 2008.
- Cassese, Antoino, **International Law**, Second Edition, New York: Oxford University Press, 2005.
- Craig, Terence ve Mary E. Ludloff, **Privacy and Big Data**, Sebastopol: O'Reilly Media, 2011.
- De Vattel, Emer, **The Law of Nations**, Thomas Nugent (Çev.), Béla Kapossy ve Richard Whatmore (Ed.), Indianapolis: Liberty Fund, 2008.
- Degan, Vladimir Đuro, **Sources of International Law**, The Hague: Martinus Nijhoff Publishers, 1997.
- DeNardis, Laura, **Protocol Politics: The Globalization of Internet Governance**, Cambridge, Massachusetts: The MIT Press, 2009.
- Dixon, Martin, **Textbook of International Law**, Seventh Edition, Oxford: Oxford University Press, 2013.
- Doctorow, Cory, **Information Doesn't Want to Be Free: Laws for the Internet Age**, San Francisco: McSweeney's, 2015.
- Dodge, Martin ve Rob Kitchin, **Mapping Cyberspace**, New York: Routledge, 2001.
- Duguit, Leon, **Kamu Hukuku Dersleri**, Süheyye Derbil (Çev.), Ankara: Ankara Üniversitesi Hukuk Fakültesi Yayınları, 1954.
- Dunham Ken ve Jim Melnick, **Malicious Bots: An Inside Look into the Cyber-Criminal Underground of the Internet**, Auerbach Publications, 2009.

- Epps, Valerie, **International Law**, Fifth Edition, Durham: Carolina Academic Press, 2014.
- Erdoğan, Birsen, **Humanitarian Intervention and the Responsibility to Protect: Turkish Foreign Policy Discourse**, Palgrave Macmillan, 2017.
- Erkiner, Hakkı Hakan, **Devletin Haksız Fiilden Kaynaklanan Uluslararası Sorumluluğu**, İstanbul: On İki Levha Yayıncılık, 2010.
- Erkiner, Hakkı Hakan, **Uluslararası Terörizme Karşı Meşrû Müdâfaa**, 2. Baskı, Ankara: Seçkin Yayıncılık, 2021.
- Feinberg, Joel, **Harm to Self**, Oxford: Oxford University Press, 1986.
- Fitzmaurice, Gerald, **The General Principles of International Law: Considered from the Standpoint of the Rule of Law**, Leiden: A.W. Sijthoff, 1958.
- Friedmann, Wolfgang, **Legal Theory**, Fifth Edition, New York: Columbia University Press, 1967.
- Gay, Joshua (ed.), **Free Software, Free Society: Selected Essays of Richard M. Stallman**, Boston: GNU Press, 2002.
- Gencer, Bedri, **Gelenekten Modernliğe Osmanlı**, İstanbul: Ketebe Yayınları, 2019.
- Gibson, William, **Neuromancer**, SF Masterworks, London: Orion Publishing, 2022.
- Goldsmith Jack ve Tim Wu, **Who Controls the Internet? Illusions of a Borderless World**, New York: Oxford University Press, 2006.
- Gözübüyük, A. Şeref ve Suna Kili, **Türk Anayasa Metinleri: Senedi İttifaktan Günümüze**, Ankara: Türkiye İş Bankası Kültür Yayınları, 1985.
- Griffiths, James, **The Great Firewall of China: How to Build and Control an Alternative Version of the Internet**, 2'nd Edition, London: Zed Books, 2021.
- Grotius, Hugo, **On the Law of War and Peace**, Archibald Colin Campbell (Çev.), Kitchener: Batoche Books, 2001.
- Gül, Yunus Emre, **Savaş Hukuku 2.0: Siber Saldırıları ve Hukuk**, İstanbul: Hukuk Akademisi Eğitim ve Yayıncılık, 2021.
- Güngör Müberra ve Gökhan Evren, **İnternet Sektörü ve Türkiye İncelemeleri**, Ankara: T.C. Telekomünikasyon Kurumu, 2002.
- Hafner, Katie ve John Markoff, **Cyberpunk: Outlaws and Hackers on the Computer Frontier**, New York: Simon & Schuster, 1991.

- Hakala, Janne ve Jazlyn Melnychuk, **Russia's Strategy in Cyberspace**, Riga: NATO Strategic Communications Centre of Excellence, 2021.
- Hart, Herbert Lionel Adolphus, **The Concept of Law**, Third Edition, Oxford: Oxford University Press, 2012.
- Hatipoğlu Aydın, Duygu, **Siber Alan ve Hukuk**, İstanbul: On İki Levha Yayıncılık, 2022.
- Hegel, Georg Wilhelm Friedrich, **Elements of the Philosophy of Right**, Hugh Barr Nisbet (Çev.), Allen W. Wood (Ed.), 18th Printing, Cambridge: Cambridge University Press, 2014.
- Heim, Michael, **The Metaphysics of Virtual Reality**, New York: Oxford University Press, 1993.
- Hillier, Tim, **Principles of Public International Law**, Second Edition, London, Sydney: Cavendish Publishing Limited, 1999.
- Işık, Alper, **İnternet Aktörleri ve Egemenliğin Değişen Boyutları: Digital Services Act ve Türk Mevzuatı Özelinde Bir İnceleme**, İstanbul: On İki Levha Yayıncılık, 2023.
- James, Paul, **Nation Formation: Towards a Theory of Abstract Community**, Cambridge: SAGE Publications, 1996.
- Janis, Mark W., **An Introduction to International Law**, 4th Edition, New York: Aspen Publishers, 2003.
- Karagülmez, Ali, **Bilişim Suçları ve Soruşturma – Kovuşturma Evreleri**, 5. Baskı, Ankara: Seçkin Yayıncılık, 2014.
- Keskin, Funda, **Uluslararası Hukukta Kuvvet Kullanma: Savaş, Karışma ve Birleşmiş Milletler**, Ankara: Mülkiyeliler Birliği Vakfı Yayınları, 1998.
- Kittichaisaree, Kriangsak, **Public International Law of Cyberspace**, Cham: Springer, 2017.
- Koca, Mahmut ve İlhan Üzülmüş, **Türk Ceza Hukuku Genel Hükümler**, 16. Baskı, Ankara: Seçkin Yayıncılık, 2023.
- Krasner, Stephen D., **Sovereignty: Organized Hypocrisy**, Princeton: Princeton University Press, 1999.
- Kukkola, Juha, **Digital Soviet Union: The Russian National Segment of the Internet as a Closed National Network Shaped by Strategic Cultural Ideas**, Series 1, Research Publications No.40, Helsinki: National Defence University, 2020.

- Kuran, Selami, Derya Aydın Okur, Reşat Volkan Günel ve Meltem Sarıbeyoğlu, **Uluslararası Hukuk Temel Metinler**, İkinci Baskı, İstanbul: Türkmen Kitabevi, 2011.
- Kuran, Selami, **Uluslararası Deniz Hukuku**, 6. Baskı, İstanbul: Beta Basım Yayım Dağıtım, 2020.
- Küzeci, Elif, **Sayısal Fil**, İstanbul: İnkılap Kitabevi, 2021.
- Langer, Ullrich, **Divine and Poetic Freedom in the Renaissance: Nominalist Theology and Literature in France and Italy**, Princeton: Princeton University Press, 2014.
- Lefebvre, Henri, **Mekânın Üretimi**, Işık Ergüden (Çev.), 2. Baskı, İstanbul: Sel Yayıncılık, 2014.
- Lessig, Lawrence, **Code and other Laws of Cyberspace**, New York: Basic Books, 1999.
- Lessig, Lawrence, **Code: Version 2.0**, New York: Basic Books, 2006.
- Libicki, Martin C., **Cyberdeterrence and Cyberwarfare**, RAND Corporation, 2009.
- Meray, Seha Lütfü, **Devletler Hukukuna Giriş – Birinci Cilt**, Üçüncü Bası, Ankara: Ankara Üniversitesi Siyasal Bilgiler Fakültesi Yayınları, 1968.
- Mesquita, Anabela ve Chia-Wen Tsai (ed.), **Human Behavior, Psychology, and Social Interaction in the Digital Era**, Hershey: IGI Global, 2015.
- Metallo, Concetta, Maria Ferrara, Alessandra Lazazzara ve Stefano Za (ed.), **Digital Transformation and Human Behavior Innovation for People and Organisations**, Springer, 2021.
- Mitchell, Willam J., **City of Bits: Space, Place, and the Infobahn**, MIT Press, 1995.
- Mueller, Milton L., **Networks and States: The Global Politics of Internet Governance**, The MIT Press, 2010.
- Mueller, Milton L., **Ruling the Root: Internet Governance and the Taming of Cyberspace**, The MIT Press, 2004.
- Murray, Andrew D., **The Regulation of Cyberspace: Control in the Online Environment**, Routledge-Cavendish, 2007.
- Neff, Stephen C., **Justice Among Nations: A History of International Law**, Massachusetts: Harward University Press, 2014.
- O’Neil, Cathy, **Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy**, New York: Crown Publishing, 2016.

- Öktem, Emre, **Uluslararası Teamül Hukuku**, İstanbul: Beta Basım Yayım Dağıtım, 2013.
- Öztekin, Alp, **Teori ve Uygulamada Türk İnternet Hukuku**, Ankara: Seçkin Yayıncılık, 2021.
- Pazarcı, Hüseyin, **Uluslararası Hukuk**, 14. Bası, Ankara: Turhan Kitabevi Yayınları, 2015.
- Peters, Benjamin, **How Not to Network a Nation: The Uneasy History of the Soviet Internet**, Cambridge, MA: MIT Press, 2016.
- Post, David G., **In Search of Jefferson's Moose: Notes on the State of Cyberspace**, New York: Oxford University Press, 2009.
- Ragazzi, Maurizio, **The Concept of International Obligations Erga Omnes**, Oxford: Clarendon Press, 2002.
- Raufoğlu, Tabriz, **Hukuki Yönleri ile Siber Alanda Yetki Sorunu: Evrensel İnternet Yönetimi Buhranı Işığında**, Ankara: Adalet Yayınevi, 2022.
- Reveron, Derek S. ve John E. Savage, **Security in the Cyber Age: An Introduction to Policy and Technology**, Cambridge: Cambridge University Press, 2023.
- Rheingold, Howard, **The Virtual Community: Homesteading on the Electronic Frontier**, Reading, Massachusetts: Addison-Wesley, 1993.
- Rheingold, Howard, **Virtual Reality: The Revolutionary Technology of Computer-Generated Artificial Worlds – and How It Promises and Threatens to Transform Business and Society**, New York: Summit Books, 1991.
- Roscini, Marco, **International Law and the Principle of Non-Intervention: History, Theory, and Interactions with Other Principles**, Oxford: Oxford University Press, 2024.
- Rothwell, Donald R., Stuart Kaye, Afshin Akhtar-Khavari, Ruth Davis ve Imogen Saunders, **International Law: Cases and Materials with Australian Perspectives**, Third Edition, Cambridge: Cambridge University Press, 2018.
- Ryngaert, Cedric, **Jurisdiction in International Law**, Second Edition, Oxford: Oxford University Press, 2015.
- Saalman, Lora, Fei Su ve Larisa Saveleva Dovgal, **Cyber Risk Reduction in China, Russia, the United States and the European Union**, Solna: Stockholm International Peace Research Institute (SIPRI), 2024.
- Sander, Oral, **Siyasi Tarih: İlkçağlardan 1918'e**, 12. Baskı, Ankara: İmge Kitabevi Yayınları, 2003.

- Saunders, Trevor J., **Notes on the Laws of Plato**, Bulletin Supplement (University of London. Institute of Classical Studies), No.28, 1972,
- Schmitt, Carl, **Siyasi İlahiyat: Egemenlik Kuramı Üzerine Dört Bölüm**, Emre Zeybekoğlu (Çev.), 2. Baskı, Ankara: Dost Kitabevi Yayınları, 2005.
- Schmitt, Michael N. (ed.), **Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations**, 2nd Edition, Cambridge: Cambridge University Press, 2017.
- Schwabach, Aaron, **Internet and the Law: Technology, Society, and Compromises**, Santa Barbara, California: ABC-CLIO, 2006.
- Scott, James Brown, **The Catholic Conception of International Law**, New Jersey: The Lawbook Exchange, 2007.
- Shapiro, Carl ve Hai R. Varian, **Information Rules: A Strategic Guide to the Network Economy**, Boston: Harvard Business School Press, 2009.
- Shaw, Joseph M., R. W. Franklin, Harris Kaasa ve Charles W. Buzicky (Ed.), **Readings in Christian Humanism**, Minneapolis: Fortress Press, 2009.
- Shaw, Malcolm, **International Law**, Eighth Edition, Cambridge: Cambridge University Press, 2017.
- Simons, Walter, **The Evolution of International Public Law in Europe since Grotius**, New York: William S Hein & Co, 2004.
- Smith, Merritt Roe ve Leo Marx, **Does Technology Drive History?: The Dilemma of Technological Determinism**, The MIT Press, 1994.
- Sterling, Bruce, **The Hacker Crackdown: Law and Disorder on the Electronic Frontier**, New York, Toronto: Bantam Books, 1992.
- Suluk, Cahit, Rauf Karasu ve Temel Nal, **Fikri Mülkiyet Hukuku**, Ankara: Seçkin Yayıncılık, 2017.
- Şahin, Onur, **Telif Hakları Bakımından Bilgisayar Programları: Araştırma Serbestisi ile Özgür ve Açık Kaynak Kodlu Programlar**, On İki Levha Yayıncılık, 2021.
- Şişek, Ömer, **Suçun Nitelikli Halleri**, Ankara: Seçkin Yayıncılık, 2023.
- Talmon, Stefan, **Recognition of Governments in International Law: With Particular Reference to Governments in Exile**, Oxford, New York: Clarendon Press, 1998.
- Tanyeri, Alp Eren, **Uluslararası Hukukta Özel Hassas Deniz Alanları ve Türk Suları**, Ankara: Seçkin Yayıncılık, 2022.

- Toluner, Sevin, **Milletlerarası Hukuk Dersleri: Devletin Yetkisi**, 4. Bası, İstanbul: Beta Basım Yayım Dağıtım, 1989.
- Touraine, Alain, **Demokrasi Nedir?**, Olcay Kunal (Çev.), İstanbul: Yapı Kredi Yayınları, 1997.
- Töner Şen, Semin, **Siber Uzay ve Uluslararası Hukuk**, İstanbul: On İki Levha Yayıncılık, 2022.
- United Nations High Commissioner for Refugees (UNCHR), **Vatansız Kişilerin Korunması Hakkında El Kitabı: Vatansız Kişilerin Statüsüne Dair 1954 Sözleşmesi Kapsamında**, Cenevre, 2014.
- Vincent, Raymond John, **Nonintervention and International Order**. New Jersey: Princeton University Press, 1974.
- Von Bertalanffy, Ludwig, **General System Theory: Foundations, Development, Applications**, New York: George Braziller, 1969.
- Wallace, Rebecca M. M. ve Olga Martin-Ortega, **International Law**, Eighth Edition, Sweet & Maxwell, 2016.
- Wiener, Norbert, **Cybernetics or Control and Communication in the Animal and the Machine**, Second Edition, Fourth Printing, USA: MIT Press, 1985.
- Wiener, Norbert, **The Human Use of Human Beings: Cybernetics and Society**, London: Free Association Books, 1989.
- Yaran, Cafer Sadık, **Kötülük ve Teodise: Batı ve İslâm Din Felsefesinde “Kötülük Problemi” ve Teistik Çözümler**, Ankara: Vadi Yayınları, 1997.
- Yüksekbaş, Raci Çetin, **Otonom Araçların Haksız Fiil Sorumluluğu**, Ankara: Seçkin Yayıncılık, 2024.
- Zürcher, Erik Jan, **Modernleşen Türkiye’nin Tarihi**, 28. Baskı, İstanbul: İletişim Yayınları, 2013.

Kitap Bölümleri

- Ağaoğulları, Mehmet Ali, “Bodin’dan Hobbes’a Doğru: Jean Bodin”, Mehmet Ali Ağaoğulları (Ed.), **Sokrates'ten Jakobenlere Batı'da Siyasal Düşünceler** içinde. 6. Baskı, İstanbul: İletişim Yayınları, 2015, ss.401-415.
- Ağaoğulları, Mehmet Ali, “Jean-Jacques Rousseau: Halk Kendini Yaratıyor”, Mehmet Ali Ağaoğulları (Ed.), **Sokrates'ten Jakobenlere Batı'da Siyasal Düşünceler** içinde. 6. Baskı, İstanbul: İletişim Yayınları, 2015, ss.569-596.

- Bayram, Ahmet Kemal, “Siyasetin Dili: Kavramlar, Kurumlar”, Davut Dursun ve Mustafa Altunoğlu (Ed.), **Siyaset Bilimi** içinde. Eskişehir: Anadolu Üniversitesi Yayınları, 2012, ss.28-57.
- Benedikt, Michael, “Cyberspace: Some Proposals”, Michael Benedikt (Ed.), **Cyberspace: First Steps** içinde. The MIT Press, 1991, ss.119-224.
- Branscomb, Anne Wells, “Jurisdictional Quandaries for Global Networks”, Linda M. Harasim (Ed.), **Global Networks: Computers and International Communication** içinde. Cambridge: The MIT Press, 1993, ss.83-103.
- Bygrave, Lee A. ve Terje Michaelsen, “Governors of Internet”, Lee A. Bygrave ve Jon Bing (Ed.), **Internet Governance: Infrastructure and Institutions** içinde. New York: Oxford University Press, 2009, ss.92-125.
- Clemente, Dave, “Fundamentals of Cyber Security”, Larry MacFaul (Ed.), **Verification & Implementation – A biennial collection of analysis on international agreements for security and development** içinde. London: VERTIC, 2015, ss.163-179.
- De Pascalis, Francesco, “FinTech Credit Firms: Prospects and Uncertainties”, Iris H-Y Chiu ve Gudula Deipenbrock (ed.), **Routledge Handbook of Financial Technology and Law** içinde. London, New York: Routledge, 2021, ss.119-137.
- Easterbrook, Frank Hoover, “Cyberspace and the Law of the Horse”, Legal Forum Editors, **The University of Chicago Legal Forum** içinde. 1996, ss.207-216.
- Eckersley, Peter, “How Unique Is Your Web Browser?”, Mikhail J. Atallah ve Nicholas J. Hopper (Ed.), **Privacy Enhancing Technologies** içinde. Berlin, Heidelberg, New York: Springer, 2010, ss.1-18.
- Farinho, Domingos Soares ve Ricardo Resende Campos, “Models of Legal Liability for Social Networks: Between Germany and Portugal”, Carlos Blanco de Moraes, Gilmar Ferreira Mendes ve Thomas Vesting (Ed.), **The Rule of Law in Cyberspace** içinde. Cham: Springer, 2022, ss.331-348.
- Fisch, Jörg, “Peoples and Nations”, Bardo Fassbender ve Anne Peters (Ed.), **The Oxford Handbook of the History of International Law** içinde. Oxford: Oxford University Press, 2012, ss.27-48.
- Fuchs, Christian, Kees Boersma, Anders Albrechtslund ve Marisol Sandoval, “Introduction: Internet and Surveillance”, Christian Fuchs, Kees Boersma, Anders Albrechtslund ve Marisol Sandoval (Ed.), **Internet and Surveillance: The Challenges of Web 2.0 and Social Media** içinde. New York, London: Routledge, 2012, ss.1-28.
- Gencer, Bedri, “Keşf-i Kadimin Altı Kapısı”, Şanlıurfa Valiliği, **Uluslararası İslam Bilgeleri Zirvesi: Tebliğler** içinde. İstanbul: Marmara Matbaası, 2017, ss.118-125.

- Gibney, Matthew J., “Statelessness and Citizenship in Ethical and Political Perspective”, Alice Edwards ve Laura van Waas (Ed.), **Nationality and Statelessness under International Law** içinde. Cambridge: Cambridge University Press, 2014, ss.44-63.
- Giles, Keir ve William Hagestad II, “Divided by a Common Language: Cyber Definitions in Chinese, Russian and English”, K. Podins, J. Stinissen ve M. Maybaum (Eds.), **5th International Conference on Cyber Conflict** içinde. Tallinn: NATO CCDCOE Publications, 2013, ss.413-430.
- Glasner, Sol, “Multinational Corporations and National Sovereignty”, Anne W. Branscomb (Ed.), **Toward a Law of Global Communications Networks** içinde. New York, London: Longman, 1986, ss.335-342.
- Hill, Steven, “NATO and the International Law of Cyber Defence”, Nicholas Tsagourias ve Russell Buchan (ed.), **Research Handbook on International Law and Cyberspace** içinde. Cheltenham: Edward Elgar Publishing, 2021, ss.509-524.
- Kaja, Fatjon, Edoardo D. Martino ve Alessio M. Paces, “FinTech and the Law and Economics of Disintermediation”, Iris H-Y Chiu ve Gudula Deipenbrock (ed.), **Routledge Handbook of Financial Technology and Law** içinde. London, New York: Routledge, 2021, ss.78-95.
- Kohl, Uta, “Jurisdiction in Network Society”, Nicholas Tsagourias ve Russell Buchan (ed.), **Research Handbook on International Law and Cyberspace** içinde. Cheltenham: Edward Elgar Publishing, 2021, ss.69-96.
- Kuczerawy, Aleksandra, “From ‘Notice and Takedown’ to ‘Notice and Stay Down’: Risks and Safeguards for Freedom of Expression”, Giancarlo Frosio (Ed.), **Oxford Handbook of Online Intermediary Liability** içinde. Oxford: Oxford University Press, 2020, ss.525-543.
- Kuehl, Daniel T., “From Cyberspace to Cyberpower: Defining the Problem”, Franklin D. Kramer, Stuart H. Starr ve Larry K. Wentz (Ed.), **Cyberpower and National Security** içinde. Washington: National Defense University Press, Potomac Books, 2009, ss.24-42.
- Lowe, Vaughan, “The Principle of Non-intervention: Use of Force”, Vaughan Lowe ve Colin Warbrick (Ed.), **The United Nations and the Principles of International Law: Essays in Memory of Michael Akehurst** içinde. London, New York: Routledge, 1994, ss.66-84.
- Mairet, Gérard, “Padovalı Marsilius’dan Louis XIV’e Laik Devletin Doğuşu”, Cemal Bali Akal (Ed), **Devlet Kuramı** içinde. 4. Bası, Ankara: Dost Kitabevi Yayınları, 2013, ss.215-244.

- Mendelson, Maurice, “The International Court of Justice and the Sources of International Law”, Vaughan Lowe ve Malgosia Fitzmaurice (Ed.), **Fifty Years of the International Court of Justice: Essays in Honour of Sir Robert Jennings** içinde. Cambridge: Cambridge University Press, 1996, ss.63-89.
- Monkiewicz, Jan ve Paweł Gołąb, “Digital Finance: Systemic Framework”, Lech Gąsiorkiewicz ve Jan Monkiewicz (ed.), **Digital Finance and the Future of the Global Financial System: Disruption and Innovation in Financial Services** içinde. London, New York: Routledge, 2023, ss.13-32.
- Mueller, Milton L. ve Farzaneh Badiei, “Inventing Internet Governance: The Historical Trajectory of the Phenomenon and the Field”, Laura DeNardis, Derrick Cogburn, Nanette S. Levinson ve Francesca Musiani (Ed.), **Researching Internet Governance: Methods, Frameworks, Futures** içinde. Cambridge, Massachusetts: The MIT Press, 2020, ss.59-83.
- Nweke, Livinus Obiora ve Stephen D. Wolthusen, “A Holistic Approach for Enhancing Critical Infrastructure Protection: Research Agenda”, Jemal H. Abawajy, Kim-Kwang Raymond Choo ve Haruna Chiroma (Ed.), **International Conference on Emerging Applications and Technologies for Industry 4.0 (EATI’2020)** içinde. Cham: Springer, 2021, ss.220-228.
- Ørsted, Hans Christian, “First Introduction to General Physics”, (1811), Karen Jelved, Andrew D. Jackson ve Ole Knudsen (Çev.), (Ed.), **Selected Scientific Works of Hans Christian Ørsted** içinde. Princeton: Princeton University Press, 1998, ss.282-309.
- Paasi, Anssi, “Territory”, John Agnew, Katharyne Mitchell ve Gerard Toal (Ed.), **A Companion to Political Geography** içinde. Malden, Oxford, Victoria: Blackwell Publishing, 2003, ss.109-122.
- Roguski, Przemysław, “Layered Sovereignty: Adjusting Traditional Notions of Sovereignty to a Digital Environment”, Tomáš Minárik, Siim Alatalu, Stefano Biondi, Massimiliano Signoretti, İhsan Tolga ve Gábor Visky (Ed.), **11th International Conference on Cyber Conflict: Silent Battle** içinde. Tallinn: NATO CCDCOE Publications, 2019, ss.347-360.
- Roguski, Przemysław, “Violations of Territorial Sovereignty in Cyberspace—an Intrusion-based Approach”, Dennis Broeders ve Bibi van den Berg (Ed.), **Governing Cyberspace: Behavior, Power, and Diplomacy** içinde. London: Rowman & Littlefield, 2020, ss.65-84.
- Rumpf, Helmut, “Çağdaş Devletler Hukukunda Müdahale”, Rona Serozan (Çev.), **Hıfzı Timur’un Anısına Armağan** içinde. İstanbul: İstanbul Üniversitesi Yayınları, 1979, ss.709-727.

- Schafer, Valérie, “The ITU Facing the Emergence of the Internet, 1960s – Early 2000s”, Gabriele Balbi ve Andreas Fickers (Ed.), **History of the International Telecommunication Union (ITU): Transnational Techno-diplomacy from the Telegraph to the Internet** içinde. Berlin, Boston: De Gruyter Oldenbourg, 2020, ss.321-343.
- Stadnik, Ilona, “Russia: An Independent and Sovereign Internet”, Blayne Haggart, Natasha Tusikov ve Jan Aart Scholte (Ed.), **Power and Authority in Internet Governance: Return of the State?** içinde. London, New York: Routledge, 2021, ss.147-167.
- Staker, Christopher, “Jurisdiction”, Malcolm D. Evans (Ed.), **International Law** içinde. Fourth Edition, New York: Oxford University Press, 2014, ss.309-335.
- Stone, Allucquère Rosanne, “Will the Real Body Please Stand Up?”, Michael Benedikt (Ed.), **Cyberspace: First Steps** içinde. The MIT Press, 1991, ss.81-118.
- Şahinaslan, Ender, Önder Şahinaslan ve Selçuk Selimli, “Siber Saldırıların Kritik Altyapılar Üzerindeki Etkileri, Mustafa Akgül, Ufuk Çağlayan, Ethem Derman, Attila Özgüt, Mehmet Topakçı, Ramazan Uyar, Okan Oral, Şahin Akbunar, Turgut Fatih Kasalak, Evren Sezgin, Fırat Yücel, Hakan Akar ve Uğur Ercan (Ed.), **XV. Akademik Bilişim Konferansı Bildirileri** içinde. Antalya: İnternet Teknolojileri Derneği, 2013, ss.128-131.
- Touré, Hamadoun I., “The International Response to Cyberwar”, ITU, **The Quest for Cyber Peace** içinde. ITU, 2011, ss.86-103.
- Tsagourias, Nicholas, “Electoral Cyber Interference, Self-Determination, and the Principle of Non-intervention in Cyberspace”, Dennis Broeders ve Bibi van den Berg (Ed.), **Governing Cyberspace: Behavior, Power, and Diplomacy** içinde. London: Rowman & Littlefield, 2020, ss.45-64.
- Tsagourias, Nicholas, “The Legal Status of Cyberspace: Sovereignty Redux?”, Nicholas Tsagourias ve Russell Buchan (Ed.), **Research Handbook on International Law and Cyberspace** içinde. Cheltenham: Edward Elgar Publishing, 2021, ss.9-31.
- Ulutaş, Güzin, “Siber Güvenlik”, Şeref Sağıroğlu ve Mustafa Alkan (Ed.), **Siber Güvenlik ve Savunma – Farkındalık ve Caydırıcılık** içinde. Ankara: Grafiker Yayınları, 2018, ss.87-101.
- Ülken, Cansu Kaya, “Yabancılık Unsuru İçeren Fikri Haklara İlişkin Uyuşmazlıklarda İlk Sahipliğin Tespiti Sorunu”, Canan Küçükali (Ed.), **Fikri Mülkiyet Hukukunda Güncel Gelişmeler Uluslararası Sempozyumu Tam Metin Bildiri Kitabı** içinde. İstanbul: Filiz Kitabevi, 2023, ss.111-128.

- Vargas-Leon, Patricia, “Tracking Internet Shutdown Practices: Democracies and Hybrid Regimes”, Francesca Musiani, Derrick L. Cogburn, Laura DeNardis ve Nanette S. Levinson (Ed.), **The Turn to Infrastructure in Internet Governance** içinde. New York: Palgrave Macmillan, 2016, ss.167-188.
- Wang, Youjun, Hongqi Zhang, Tianwei Che, Chuanfu Zhang, Yuntian Zhao ve Chao Yang, “An Event-Based Method of Construction of Cyberspace Models”, Zuoyi Liang, Xiaoliang Li (Ed.), **4th International Conference on Mechatronics, Materials, Chemistry and Computer Engineering 2015** içinde. Atlantis Press, 2015, ss.1674-1678.
- Wessel, Ramses A., “European Law and Cyberspace”, Nicholas Tsagourias ve Russell Buchan (ed.), **Research Handbook on International Law and Cyberspace** içinde. Cheltenham: Edward Elgar Publishing, 2021, ss.491-508.
- Winseck, Dwayne, “Is the International Telecommunication Union Still Relevant in ‘the Internet Age?’ Lessons From the 2012 World Conference on International Telecommunications (WCIT)”, Gabriele Balbi ve Andreas Fickers (Ed.), **History of the International Telecommunication Union (ITU): Transnational Techno-diplomacy from the Telegraph to the Internet** içinde. Berlin, Boston: De Gruyter Oldenbourg, 2020, ss.321-343.
- Wu, Tim, “Is Internet Exceptionalism Dead?”, Berin Szoka ve Adam Marcus (Ed.), **The Next Digital Decade: Essays on the Future of the Internet** içinde. Washington, D.C: TechFreedom, 2011, ss.179-188.
- Yalçinkaya, Ayhan, “İlahi Siyaset”, Mehmet Ali Ağaoğulları (Ed.), **Sokrates'ten Jakobenlere Batı'da Siyasal Düşünceler** içinde. 6. Baskı, İstanbul: İletişim Yayınları, 2015, ss.197-234.
- Zekoll, Joachim, “Jurisdiction in Cyberspace”, Günther Handl, Joachim Zekoll ve Peer Zumbansen (ed.), **Beyond Territoriality: Transnational Legal Authority in an Age of Globalization** içinde. Leiden: Martinus Nijhoff Publishers, 2012, ss.341-369.

Sürelî Yayınlar

- Akehurst, Michael, “Jurisdiction in International Law”, **British Year Book of International Law**, Vol.46, (1972-1973), ss.145-257.
- Aksoy, Neşe, “Kant’tan Wittgenstein’a: Mantığın Sınırları”, **Felsefe Arkivi**, Sayı.51, (2019), ss.17-29.
- Aloupi, Niki, “The Right to Non-intervention and Non-interference”, **Cambridge Journal of International and Comparative Law**, Vol.4, Iss.3, (2015), ss.566-587.

- Altınır, Müberra ve Fatma Çakır, “Siber Uzay ve Uluslararası İlişkiler/ Teorisi”, **Cyberpolitik Journal**, Cilt.2, Sayı.4, (2018), ss.183-190.
- Altıntaş Açıkgoz, Elif Hande, “Bulut Bilişim Sisteminde Yer Alan Verilerden Kaynaklanan Uyuşmazlıklarda Milletlerarası Yetkili Mahkemenin Tespiti Meselesi”, **Bilişim Hukuku Dergisi**, Cilt.6, Sayı.1, (2024), ss.80-131.
- Anand, Ram Prakash, “Sovereign Equality of States in International Law – I”, **International Studies**, Vol.8, Iss.3, (1966), ss.213-241.
- Andersen, Tore Rye, “Cyberspace Revisited: A Radial Reading of William Gibson’s “Burning Chrome””, **The Journal of American Culture**, Vol.42, No.2, (2019), ss.121-136.
- Anlar Güneş, Şule, “Maden Kaynaklarının Yönetimi Bağlamında Uluslararası Deniz Yatağı Otoritesinin Rolü”, **Uluslararası İlişkiler**, Cilt.17, Sayı.65, (2020), ss.101-124.
- Aronson, Jay D., “Telecommunications Negotiations in GATT”, **Transnational Data and Communications Report**, Vol.10, No.2, (1987), ss.11-13.
- Asıl, Erdem, “Uluslararası Deniz Hukukuna Hâkim Olan İlkeler Kapsamında Kitle İmha Silahlarının Yayılmasını Engellemeye Yönelik Tedbirlerin Değerlendirilmesi”, **Adalet Dergisi**, Sayı 67, (2021), ss.445-487.
- Atik, Kayhan, “Türklerdeki Kut Anlayışına Karşılaştırmalı Tarih Açısından Bakış”, **Akademik Sosyal Araştırmalar Dergisi**, Yıl.5, Sayı.60, (2017), ss.209-222.
- Aydınlı, Halil İbrahim ve Veysel Ayhan, “Egemenlik Kavramının Tarihsel Gelişimi Perspektifinden İktidarın Sınırlandırılması Tartışması”, **Cumhuriyet Üniversitesi İktisadi ve İdari Bilimler Dergisi**, Cilt.5, Sayı.1, (2004), ss.67-84.
- Banks, William, “Cyber Attribution and State Responsibility”, **International Law Studies**, Vol.97, (2021), ss.1039-1072.
- Barnett, Michael ve Raymond Duvall, “Power in International Politics”, **International Organization**, Vol.50, Iss.1, (2005), ss.39-75.
- Barocas Solon ve Andrew D. Selbst, “Big Data’s Disparate Impact”, **California Law Review**, Vol.104, No.3, (2016), ss.671-732.
- Başkarada, Saša ve Andy Koronios, “Data, Information, Knowledge, Wisdom (DIKW): A Semiotic Theoretical and Empirical Exploration of the Hierarchy and its Quality Dimension”, **Australasian Journal of Information Systems**, Vol.18, No.1, (2013), ss.5-24.
- Beer, Stafford, “What is cybernetics?”, **Kybernetes**, Vol.3, Iss.3/4, (2004), ss.853-863.

- Belik, Mahmut R., “Devletlerin Hak ve Vazifeleri Üzerinde Beyanname Projesi”, **İstanbul Hukuk Mecmuası**, Cilt.18, Sayı.1-2, (1952), ss.59-70.
- Beybur, Mustafa, “Şubesiz Dijital Bankacılık ve Türk Bankacılık Sektörü İçin Öneriler”, **Ankara Hacı Bayram Veli Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi**, Cilt.24, Sayı.1, (2022), ss.286-303.
- Bilder, Richard B., “Perspectives on Sovereignty in the Current Context: An American Viewpoint”, **Canada-United States Law Journal**, Vol.20, (1994), ss.9-17.
- Bowett, Derek William, “Jurisdiction: Changing Patterns of Authority over Activities and Resources”, **British Yearbook of International Law**, Vol.53, Iss.1, (1982), ss.1-26.
- Branscomb, Anne Wells, “Anonymity, Autonomy, and Accountability: Challenges to the First Amendment in Cyberspaces”, **The Yale Law Journal**, Vol.104, No.7, (1995), ss.1639-1679.
- Branscomb, Anne Wells, “Common Law for the Electronic Frontier”, **Scientific American**, Vol.265, No.3, (1991), ss.154-158.
- Breibart, Evan, “The Wood Pulp Case: The Application of European Economic Community Competition Law to Foreign Based Undertakings”, **Georgia Journal of International and Comparative Law**, Vol.19, No.1, (1989), ss.149-173.
- Brierly, James Leslie, “The Lotus Case”, **Law Quarterly Review**, Vol.44, (1928), ss.154-163.
- Bromme Rainer ve Elmar Stahl, “Is a Hypertext a Book or a Space? The Impact of Different Introductory Metaphors on Hypertext Construction”, **Computers & Education**, Vol.44, Iss.3, (2005), ss.115-133.
- Brown, Gary ve Keira Poellet, “The Customary International Law of Cyberspace”, **Strategic Studies Quarterly**, Vol.6, No.3, (2012), ss.126-145.
- Buchanan, James M. ve Yong J. Yoon, “Symmetric Tragedies: Commons and Anticommons”, **The Journal of Law and Economics**, Vol.43, No.1, (2000), ss.1-14.
- Burk, Dan L., “Patents in Cyberspace: Territoriality and Infringement on Global Computer Networks”, **Tulane Law Review**, Vol.68, No.1, (1993), ss.1-67.
- Büyük, Mehmet Emin, “Machiavelli’den Grotius’e Egemenlik Kuramının ve Modern Devletler Hukukunun Gelişimi”, **İstanbul Hukuk Mecmuası**, Cilt.80, Sayı.1, (2022), ss.299-356.

- Chatinakrob, Thanapat, “Interplay of International Law and Cyberspace: State Sovereignty Violation, Extraterritorial Effects, and the Paradigm of Cyber Sovereignty”, **Chinese Journal of International Law**, Vol.23, Iss.1, (2024), ss.25-72.
- Chircop, Luke, “Territorial Sovereignty in Cyberspace after Tallinn Manual 2.0”, **Melbourne Journal of International Law**, Vol.20, Iss.2, (2019), ss.349-377.
- Cohen, Julie E., “Cyberspace as/and Space”, **Columbia Law Review**, Vol.107, No.1, (2007), ss.210-256.
- Corn, Gary P. ve Robert Taylor, “Sovereignty in the Age of Cyber”, **American Journal of International Law Unbound**, Vol.111, (2017), ss.207-212.
- Couture, Stephane ve Sophie Toupin, “What Does the Notion of ‘Sovereignty’ Mean When Referring to the Digital?”, **New Media & Society**, Vol.21, Iss.10, (2019), ss.2305-2322.
- Csonka, Peter, “The Council of Europe's Convention on Cyber-Crime and Other European Initiatives”, **International Review of Penal Law**, Vol.77, (2006), ss.473-501.
- Çakar, Osman, “Hukuk Muhakemeleri Kanundaki Ceza Muhakemesi Hükümleri Özelinde Disiplin Hapsi”, **Türkiye Adalet Akademisi Dergisi**, Yıl.8, Sayı.32, (2017), ss.411-433.
- Çelik, Emin, “Mobil Oyunların Fikri Mülkiyet Hukukunda Korunması”, **Anadolu Üniversitesi Hukuk Fakültesi Dergisi**, Cilt.9, Sayı.1, (2023), ss.139-152.
- Çevik, İpek, “Avrupa Birliği Dijital Hizmetler Yasası’nın Değerlendirmesi”, **Yıldırım Beyazıt Hukuk Dergisi**, Sayı.2, (2023), ss.387-419.
- Dalcalı, Adem, Emre Çelik ve Serdal Arslan, “Mikro ve Mini Hidroelektrik Santralleri için Mikrodenetleyici Tabanlı bir Elektronik Governor Sisteminin Tasarımı”, **Erciyes Üniversitesi Fen Bilimleri Enstitüsü Dergisi**, Cilt.28, Sayı.2, (2012), ss.130-135.
- Day, John D. ve Hubert Zimmermann, “The OSI Reference Model”, **Proceedings of the IEEE**, Vol.71, No.12, (1983), ss.1334-1340.
- De Filippi, Primavera ve Samer Hassan, “Blockchain Technology as a Regulatory Technology From Code is Law to Law is Code”, **First Monday**, Vol.21, No.12, (2016).
- Demchak, Chris and Peter Dombrowski, “Cyber Westphalia: Asserting State Prerogatives in Cyberspace”, **Georgetown Journal of International Affairs**, International Engagement on Cyber III, (2013), ss.29-38.

- Demchak, Chris C. ve Peter Dombrowski, “Rise of a Cybered Westphalian Age”, **Strategic Studies Quarterly**, Vol.5, No.1, (2011), ss.32-61.
- Dewar, Robert, “Cyberspace is a Consensual Hallucination”, **Policy Perspectives**, Vol.6, No.2, (2018), ss.1-4.
- Dilek, Esmâ, Özgür Talih ve Türksel Kaya Bensghir, “Estonya 2007 Siber Saldırılarının İncelenmesi ve Ülkelerin Ulusal Siber Güvenlik Politikalarına Etkileri”, **Bilgi Yönetimi Dergisi**, Cilt.6, Sayı.2, (2023), ss.332-347.
- Doğan, Korcan ve Sacit Arslantekin, “Büyük Veri: Önemi, Yapısı ve Günümüzdeki Durum”, **Ankara Üniversitesi Dil ve Tarih-Coğrafya Fakültesi Dergisi**, Cilt.56, Sayı.1, (2016), ss.15-36.
- Dyson, Esther, George Gilder, George Keyworth ve Alvin Toffler, “Cyberspace and the American Dream: A Magna Carta for the Knowledge Age (Release 1.2, August 22, 1994)”, **The Information Society**, Vol.12, Iss.3, (1996), ss.295-308.
- Elbakyan, Alexandra ve Aras Bozkurt, “A Critical Conversation with Alexandra Elbakyan: Is she the Pirate Queen, Robin Hood, a Scholarly Activist, or a Butterfly Flapping its Wings?”, **Asian Journal of Distance Education**, Vol.16, Iss.1, (2021), ss.111-118.
- Eldem, Tuba, “Uluslararası Siber Güvenlik Normları ve Sorumlu Siber Egemenlik”, **İstanbul Hukuk Mecmuası**, Cilt.79, Sayı.1, (2021), ss.347-378.
- Epstein, Dmitry, Christian Katzenbach ve Francesca Musiani, “Doing Internet Governance: Practices, Controversies, Infrastructures, and Institutions”, **Internet Policy Review**, Vol.5, Iss.3, (2016).
- Erdem, Merve ve Gürkan Özocak, “Siber Güvenliğin Sağlanmasında Uluslararası Hukukun ve Türk Hukukunun Rolü”, **Ankara Üniversitesi Hukuk Fakültesi Dergisi**, Cilt.68, Sayı.1, (2019), ss.127-212.
- Erkiner, Hakkı Hakan, “Grotius Öncesinde İlk Modern Uluslararası Hukuk Düşüncesinin Oluştığı Tarihsel Koşullar ve Erken Klâsik Dönemdeki Öğreti”, **Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi**, Cilt.18, Sayı.1, (2012), ss.51-146.
- Erkiner, Hakkı Hakan, “Uluslararası Hukuk Düşüncesinde Klâsik Öğretinin Kuruluşu: Hugo Grotius ve Postgrotien Yazarlar Samuel Von Pufendorf, Richard Zouche, Cornelius Van Bynkershoek ve Samuel Rachel'e İlişkin İnceleme ve Değerlendirme”, **Marmara Üniversitesi Hukuk Fakültesi Dergisi**, Cilt.18, Sayı.3, (2012), ss.3-142.
- Erkiner, Hakkı Hakan, “Uluslararası Hukukta İsnat Meselesi Bakımından Soykırım İddiaları ve Osmanlı Ermenileri Soykırımı İddiası'nın Değerlendirilmesi”, **Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi**, Cilt.27, Sayı.1, (2021), ss.64-119.

- Ertugay, Fatih, “Potestas ve Populus Arasındaki Mesafe Daralırken Auctoritas'ı Yeniden Ele Almak”, **Muhafazakâr Düşünce Dergisi**, Cilt.8, Sayı.31, (2012), ss.199-222.
- Ertuğrul, Ümmühan Elçin, “Koruma Sorumluluğu: İnsani Müdahaleyi Makyajlamak”, **Gazi Üniversitesi Hukuk Fakültesi Dergisi**, Cilt.20, Sayı.2, (2016), ss.441-470.
- Evans, Gareth, “From Humanitarian Intervention to the Responsibility to Protect”, **Wisconsin International Law Journal**, Vol.24, Iss.3, (2006), ss.703-722.
- Finkelstein, Lawrence S., “What is Global Governance?”, **Global Governance**, Vol.1, No.3, (1995), ss.367-372.
- Franzese, Patrick W., “Sovereignty in Cyberspace: Can It Exist?”, **The Air Force Law Review**, Vol.64, (2009), ss.1-42.
- Goldsmith, Jack L., “Against Cyberanarchy”, **The University of Chicago Law Review**, Vol.65, No.4, (1998), ss.1199-1250.
- Gozzi Jr., Raymond, “The Cyberspace Metaphor”, **ETC: A Review of General Semantics**, Vol.51, No.2, (1994), ss.218-223.
- Griffith, Dodd S., “The Computer Fraud and Abuse Act of 1986: A Measured Response to a Growing Problem”, **Vanderbilt Law Review**, Vol.43, Iss.2, (1990), ss.453-490.
- Gül, Mehmet Tayyib, “Siyasal Yaşamda Yeni Bir Oluşum: Korsan Parti ve İsveç Korsan Partisi Örneği”, **Anadolu Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi**, Cilt.24, Sayı.4, (2023), ss.525-539.
- Güngör, Gülin, “Vatansızlığın Azaltılmasına Dair Birleşmiş Milletler Sözleşmesi’nin Bazı Hükümlerinin 5901 Sayılı Türk Vatandaşlığı Kanunu Üzerindeki Etkisi”, **Ankara Üniversitesi Hukuk Fakültesi Dergisi**, Cilt.63, Sayı.3, (2014), ss.479-508.
- Hadji-Janev, Metodi, “Filling the Opinio Iuris Vacuum on Sovereignty in Cyberspace: A Call for the South-Eastern European States to Act”, **Cybersecurity and Law**, Vol.6, No.2, (2021), ss.151-166.
- Hardy, I. Trotter, “The Proper Legal Regime for 'Cyberspace'”, **University of Pittsburgh Law Review**, Vol.55, Iss.4 (1994), ss.993-1055.
- Hathaway, Oona A., Rebecca Crootof, Philip Levitz, Haley Nix, Aileen Nowlan, William Perdue ve Julia Spiegel, “The Law of Cyber-Attack”, **California Law Review**, Vol.100, No.4 (2012), ss.817-886.
- Heller, Kevin Jon, “In Defense of Pure Sovereignty in Cyberspace”, **International Law Studies**, Vol.97, (2021), ss.1432-1499.

- Henriksen, Anders, “The End of the Road for the UN GGE Process: The Future Regulation of Cyberspace”, **Journal of Cybersecurity**, Vol.5, No.1, (2019), ss.1-9.
- Herzog, Stephen, “Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses”, **Journal of Strategic Security**, Vol.4, No.2, (2011), ss.49-60.
- Hong, Yu ve G. Thomas Goodnight, “How to Think about Cyber Sovereignty: the Case of China”, **Chinese Journal of Communication**, Vol.13, No.1, (2020), ss.8-26.
- Hunter, Dan, “Cyberspace as Place and the Tragedy of the Digital Anticommons”, **California Law Review**, Vol.91, No.2, (2003), ss.439-519.
- Hussien, Seifudein Adem, “On the End of History and the Clash of Civilization: A Dissenter’s View”, **Journal of Muslim Minority Affairs**, Vol.21, No.1, (2001), ss.25-38.
- Johnson, David R. ve David Post, “Law and Borders: The Rise of Law in Cyberspace”, **Stanford Law Review**, Vol.48, No.5, (1996), ss.1367-1402.
- Kadioğlu Kumtepe, Cemre Çise, “Siber Uzayda Kuvvet Kullanma Yasağı ve Yasağın İstisnalarının Geçerliliğinin Tallinn Rehberi Kapsamında Değerlendirilmesi”, **The Turkish Yearbook of International Relations**, Vol.53, (2022), ss.21-40.
- Karauz, Ağâh Kürşat ve Halil Alperen Işık, “Rekabet Kurallarının Yer Bakımından Uygulanması”, **Yıldırım Beyazıt Hukuk Dergisi**, Sayı.1, (2016), ss.283-298.
- Kataria, Deepak, Amarpal Yadav ve Bhupender Pratap Singh, “Wireless Communication Systems: Bluetooth, Infrared, Zig bee, NFC and Wi-Fi Outline”, **International Journal of Innovative Research in Technology**, Vol.1, Iss.6, (2014), ss.585-588.
- Katsh, M. Ethan, “Software Worlds and the First Amendment: Virtual Doorkeepers in Cyberspace”, **University of Chicago Legal Forum**, Vol.1996, Iss.1, (1996), ss.335-360.
- Kavak, Özgür, “‘Siyasî-Fıkhî Ahkâmın’ Fıkıh Usûlü Zemininde Temellendirilmesi: Cüveynî’nin el-Gıyâsî’sinde Kat’iyyât-Zanniyyât Ayrımı ve Modern Yorumları”, **Dîvân Disiplinlerarası Çalışmalar Dergisi**, Cilt.14, Sayı.27, (2009), ss.21-55.
- Kavak, Özgür, “Hal’, İstifa ve İhtilal: İslam Devletlerinde İktidarın El Değiştirmesi Üzerine Bazı Tespitler”, **Dîvân Disiplinlerarası Çalışmalar Dergisi**, Cilt.24, Sayı.47, (2019), ss.141-196.
- Keller, Clara Iglesias, “Exception and Harmonization: Three Theoretical Debates on Internet Regulation”, **Humboldt Institut für Internet und Gesellschaft (HIIG) Discussion Paper Series**, 2020(2), ss.1-21.

- Kello, Lucas, “Cyber legalism: Why It Fails and What to Do About It”, **Journal of Cybersecurity**, Vol.7, Iss.1, (2021), ss.1-15.
- Kelsen, Hans, “The Draft Declaration on Rights and Duties of States: Critical Remarks”, **The American Journal of International Law**, Vol.44, No.2, (1950), ss.259-276.
- Kelsen, Hans, “The Principle of Sovereign Equality of States as a Basis for International Organization”, **The Yale Law Journal**, Vol.53, No.2, (1944), ss.207-220.
- Kerr, Orin S., “The Problem of Perspective in Internet Law”, **Georgetown Law Journal**, Vol.91, Iss.2, (2003), ss.357-405.
- Kılıç, Savaş, “Uzam mı, Uzay mı? Peki Mekân ne?”, **Cogito**, Sayı.59, (2009), ss.48-60.
- Kippenberger, Tony, “How did We get to a World Wide Web?”, **The Antidote**, Vol.4, No.5, (1999), ss.21-22.
- Kirby, Michael, “Legal Aspects of Transborder Data Flow”, **Computer/Law Journal**, Vol.11, Iss.2, (1991), ss.233-246.
- Kiss, Alexandre, “The Common Heritage of Mankind: Utopia or Reality?”, **International Journal**, Vol.40, No.3, (1985), ss.423-441.
- Kleinwächter, Wolfgang, “Beyond ICANN vs ITU?: How WSIS Tries to Enter the New Territory of Internet Governance”, **International Communication Gazette**, Vol.66, Iss.3-4, (2004), ss.233-251.
- Koçhisarlıoğlu, Cengiz ve Özlem Söğütlü Erişgin, “Hayvanların Hukuki Konumu”, **Yaşar Üniversitesi E-Dergisi**, Cilt.8, Sayı.Özel, (2013), ss.1691-1723.
- Korpisaari, Päivi, “From Delfi to Sanchez – When Can an Online Communication Platform be Responsible for Third-Party Comments?: An Analysis of the Practice of the ECtHR and some Reflections on the Digital Services Act”, **The Journal of Media Law**, Vol.14, No.2, (2022), ss.352-377.
- Kostyuk, Nadiya ve Yuri M. Zhukov, “Invisible Digital Front: Can Cyber Attacks Shape Battlefield Events?”, **Journal of Conflict Resolution**, Vol.63, Iss.2, (2019), ss.317-347.
- Kukkola, Juha ve Mari Ristolainen, “Projected Territoriality: A Case Study of the Infrastructure of Russian Digital Borders”, **Journal of Information Warfare**, Vol.17, No.2, (2018), ss.83-100.
- Kulick, Andreas, “Regulating Cyberspace between Grotius, Lotus and Strasbourg”, **Heidelberg Journal of International Law**, Vol.80, Heft.2, (2020), ss.559-569.
- Kurhan, Mürüvvat, “İmparatorluk Tanrısı Amon”, **Belleten**, Cilt.59, Sayı.226, (1995), ss.500-582.

- Kurt, Sümeyra Sena, “Uluslararası Hukukta Diplomatik Koruma”, **Anadolu Üniversitesi Hukuk Fakültesi Dergisi**, Cilt.6, Sayı.2, (2020), ss.467-498.
- Küçükali, Canan, “Bilgisayar Programlarının Fikri Mülkiyet Kapsamında Korunması”, **İstanbul Ticaret Üniversitesi Sosyal Bilimler Dergisi**, Cilt.19, Sayı.37, Covid19-Özel Ek, (2020), ss.104-127.
- Lahmann, Henning, “On the Politics and Ideologies of the Sovereignty Discourse in Cyberspace”, **Duke Journal of Comparative & International Law**, Vol.32, No.1, (2021), ss.61-107.
- Lambach, Daniel, “The Territorialization of Cyberspace”, **International Studies Review**, Vol.22, Iss.3, (2020), ss.1-25.
- Lange, Dieter G.F ve John Byron Sandage, “The Wood Pulp Decision and Its Implications for the Scope of EC Competition Law”, **Common Market Law Review**, Vol.26, Iss.2, (1989), ss.137-165.
- Lemley, Mark A., “Place and Cyberspace”, **California Law Review**, Vol.91, No.2, (2003), ss.521-542.
- Lessig, Lawrence, “The Death of Cyberspace”, **Washington and Lee Law Review**, Vol.57, Iss.2, (2000), ss.337-347.
- Lessig, Lawrence, “The Law of the Horse: What Cyberlaw Might Teach”, **Harvard Law Review**, Vol.113, No.2, (1999), ss.501-549.
- Lessig, Lawrence, “The Path of Cyberlaw”, **The Yale Law Journal**, Vol.104, No.7, (1995), ss.1743-1755.
- Lessig, Lawrence, “The Zones of Cyberspace”, **Stanford Law Review**, Vol.48, No.5, (1996), ss.1403-1411.
- Lewis, James A., “Sovereignty and the Role of Government in Cyberspace”, **The Brown Journal of World Affairs**, Vol.16, No.2, (2010), ss.55-65.
- Lin, Herbert S., “Offensive Cyber Operations and the Use of Force”, **Journal of National Security Law & Policy**, Vol.4, No.1, (2010), ss.63-86.
- Lukasik, Stephen J., “Why the Arpanet Was Built”, **IEEE Annals of the History of Computing**, Vol.33, Iss.3, (2011), ss.4-20.
- Maréchal, Nathalie, “Networked Authoritarianism and the Geopolitics of Information: Understanding Russian Internet Policy”, **Media and Communication**, Vol.5, No.1, (2017), ss.29-41.
- Maxwell, J. Clerk, “On Governors”, **Proceedings of the Royal Society of London**, Vol.16, (1868), ss.270-283.

- Mégret, Frédéric, “Are There ‘Inherently Sovereign Functions’ in International Law?”, **American Journal of International Law**, Vol.115, No.3, (2021), ss.452-492.
- Menthe, Darrel C., “Jurisdiction in Cyberspace: A Theory of International Spaces”, **Michigan Telecommunications and Technology Law Review**, Vol.4, Iss.1, (1998), ss.69-103.
- Milik, Piotr, “International Legal Regulations in the Area of Cybersecurity”, **Cybersecurity and Law**, Vol.1, No.1, (2019), ss.115-141.
- Miller, Anthony Paul, “Teleinformatics, Transborder Data Flows and the Emerging Struggle for Information: An Introduction to the Arrival of the New Information Age”, **Columbia Journal of Law and Social Problems**, Vol.20, No.1, (1986), ss.89-144.
- Mueller, Milton L., “Against Sovereignty in Cyberspace”, **International Studies Review**, Vol.22, Iss.4, (2020), ss.779-801.
- Netanel, Neil W., “Cyberspace Self-Governance: A Skeptical View From Liberal Democratic Theory”, **California Law Review**, Vol.88, No.2, (2000), ss.395-498.
- Ning, Huansheng, Xiaozhen Ye, Mohammed Amine Bouras, Dawei Wei ve Mahmoud Daneshmand, “General Cyberspace: Cyberspace and Cyber-Enabled Spaces”, **IEEE Internet of Things Journal**, Vol.5, No.3, (2018), ss.1843-1856.
- Nocetti, Julien, “Contest and Conquest: Russia and Global Internet Governance”, **International Affairs**, Vol.91, Iss.1, (2015), ss.111-130.
- Olson, Kathleen K., “Cyberspace as Place and the Limits of Metaphor”, **Convergence – The International Journal of Research into New Media Technologies**, Vol.11, No.1, (2005), ss.10-18.
- Orji, Uchenna Jerome, “The African Union Convention on Cybersecurity: A Regional Response Towards Cyber Stability?”, **Masaryk University Journal of Law and Technology**, Vol.12, No.2, (2018), ss.91-129.
- Önok, Murat, “Avrupa Konseyi Siber Suç Sözleşmesi Işığında Siber Suçlarla Mücadelede Uluslararası İşbirliği”, **Marmara Üniversitesi Hukuk Araştırmaları Dergisi – Prof. Dr. Nur Centel’e Armağan**, Cilt.19, Sayı.2, (2013), ss.1229-1270.
- Özen, Mustafa, “Non Bis in Idem (Aynı Fiilden Dolayı İki Kez Yargılama Olmaz) İlkesi, **Gazi Üniversitesi Hukuk Fakültesi Dergisi**, Cilt.14, Sayı.1, (2010), ss.389-417.
- Özman, Mehmet Aydoğan, “Devletlerin Egemenliği ve Milletlerarası Teşekküller”, **Ankara Üniversitesi Hukuk Fakültesi Dergisi**, Cilt.21, Sayı.1, (1964), ss.53-121.

- Özpolat, Haşim, “Tanrının Siyasetinden Siyasetin Tanrısına Egemenlik Kuramının Dönüşümü”, **Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi**, Cilt.23, Sayı.2, (2017), ss.143-166.
- Öztürk, Yasin, “Uluslararası Hukukta Devletlerin Egemen Eşitliği Kavramının Jus Cogens Niteliği”, **Erciyes Üniversitesi Sosyal Bilimler Enstitüsü Dergisi**, Cilt.31, Sayı.42, (2017), ss.37-53.
- Özyazıcı, Kurtuluş, “Beyazperdede Radyolu Filmler”, **TRT Akademi**, Cilt.5, Sayı.9, (2020), ss.418-435.
- Pattenden, Philip, “The Byzantine Early Warning System”, **Byzantion**, Vol.53, No.1, (1983), ss.258-299.
- Perritt Jr., Henry H., “The Internet as a Threat to Sovereignty? Thoughts on the Internet's Role in Strengthening National and Global Governance”, **Indiana Journal of Global Legal Studies**, Vol.5, Iss.2, (1998), ss.423-442.
- Perritt Jr., Henry H., “The Internet is Changing International Law”, **Chicago-Kent Law Review**, Vol.73, Iss.4, (1998), ss.997-1054.
- Polański, Paul Przemysław, “Cyberspace: A New Branch of International Customary Law?”, **Computer Law & Security Review**, Vol.33, Iss.3, (2017), ss.371-381.
- Post, David G., “Governing Cyberspace: Law”, **Santa Clara High Technology Law Journal**, Vol.24, Iss.4, (2008), ss.883-914.
- Rada, Roy, “Writing and Reading Hypertext: An Overview”, **Journal of the American Society for Information Science**, Vol.40, Iss.3, (1989), ss.164-171.
- Rahman, Mohammad Osiur, Nour Mohammad ve Mohammad Mahabubur Rahman, “Towards Understanding Personal Jurisdiction in Cyberspace: An Overview of American Try-Out for Internet Cases”, **International Journal of Law and Management**, Vol.50, No.3, (2008), ss.105-120.
- Raymond, Mark ve Laura DeNardis, “Multistakeholderism: Anatomy of an Inchoate global Institution”, **International Theory**, Vol.7, Iss.3, (2015), ss.572-616.
- Reidenberg, Joel R., “Lex Informatica: The Formulation of Information Policy Rules through Technology”, **Texas Law Review**, Vol.76, No.3, (1998), ss.553-593.
- Ruddy, Francis Stephen, “Res Nullius and Occupation in Roman and International Law”, **University of Missouri-Kansas City Law Review**, Vol.36, No.2, (1968), ss.274-287.
- Rusch, Jonathan J., “Cyberspace and the ‘Devil’s Hatband’”, **Seattle University Law Review**, Vol.24, Iss.2, (2000), ss.577-598.

- Ryan, Daniel J., Maeve Dion, Eneken Tikk ve Julie J. C. H. Ryan, “International Cyberlaw: A Normative Approach”, **Georgetown Journal of International Law**, Vol.42, No.4, (2011), ss.1161-1199.
- Salihpaşaoğlu, Yaşar ve Özgem Tuğçe Gümüş Boyacı, “Bir Modern Devlet ve Egemenlik Miti: Westphalia Barışı”, **Erciyes Üniversitesi Hukuk Fakültesi Dergisi**, Cilt.15, Sayı.1, (2020), ss.191-224.
- Samie, Najeeb, “The Doctrine of "Effects" and the Extraterritorial Application of Antitrust Laws”, **University of Miami Inter-American Law Review**, Vol.14, Iss.1, (1982), ss.23-59.
- San, Coşkun, “Toplumbilimsel Yöntem Açısından Durkheim ve Weber”, **Sosyoloji Dergisi**, Dizi.3, Sayı.21, (2010), ss.17-39.
- Savelyev, Alexander, “Russia's New Personal Data Localization Regulations: A Step Forward or a Self-Imposed Sanction?”, **Computer Law & Security Review**, Vol.32, Iss.1, (2016), ss.128-145.
- Schiavetta, Susan ve Konstantinos Komaitis, “ICANN's Role in Controlling Information on the Internet”, **International Review of Law, Computers & Technology**, Vol.17, No.3, (2003), ss.267-284.
- Schmitt, Michael N. ve Liis Vihul, “Respect for Sovereignty in Cyberspace”, **Texas Law Review**, Vol.95, Iss.7, (2017), ss.1639-1670.
- Schmitt, Michael N. ve Liis Vihul, “Sovereignty in Cyberspace: Lex Lata Vel Non?”, **American Journal of International Law Unbound**, Vol.111, (2017), ss.213-128.
- Scott, Susan V. ve Markos Zachariadis, “Origins and development of SWIFT, 1973–2009”, **Business History**, Vol.54, No.3, (2012), ss.462-482.
- Sevim, Hüseyin, “Uluslararası İlişkilerde Küreselleşme Olgusu ve Ulus-Devlet Kavramını Yeniden Düşünmek”, **Uluslararası İlişkiler Dergisi**, Cilt.3, Sayı.9, (2006), ss.89-124.
- Sevinç, Hüseyin, “Antik Yunan’da Siyasal Yapı ve Aristo ile Platon Özelinde Siyasal Düşünüş”, **Ekonomi İşletme Siyaset ve Uluslararası İlişkiler Dergisi**, Cilt.7, Sayı.2, (2021), ss.209-223.
- Shah, Shvetank, Andrew Horne ve Jaime Capellá, “Good Data Won’t Guarantee Good Decisions”, **Harvard Business Review**, Vol.90, Iss.4, (2012), ss.23-25.
- Shapiro, Andrew L., “The Disappearance of Cyberspace and the Rise of Code”, **Seton Hall Constitutional Law Journal**, Vol.8, No.3, (1998), ss.703-724.

- Sierzputowski, Bartłomiej, “The Data Embassy Under Public International Law”, **International and Comparative Law Quarterly**, Vol.68, Iss.1, (2019), ss.225-242.
- Sieyes, Emmanuel, “Tiers Etat Nedir”, Süheyp Derbil (Çev.), **Ankara Üniversitesi Hukuk Fakültesi Dergisi**, Cilt.8, Sayı.1, (1951), ss.126-207.
- Soldatov, Andrei ve Irina Borogan, “Russia's Surveillance State”, **World Policy Journal**, Vol.30, No.3, (2013), ss.23-30.
- Solove, Daniel J., “Privacy Self-Management and the Consent Dilemma”, **Harvard Law Review**, Vol.126, Iss.7, (2013), ss.1880-1903.
- Sommer, Joseph H., “Against Cyberlaw”, **Berkeley Technology Law Journal**, Vol.15, No.3, (2000), ss.1145-1232.
- Soysal, Tamer, “İnternet Servis Sağlayıcılarının Hukuki Sorumlulukları”, **Türkiye Barolar Birliği Dergisi**, Sayı.61, (2005), ss.304-339.
- Stein, Allan R., “The Unexceptional Problem of Jurisdiction in Cyberspace”, **The International Lawyer**, Vol.32, No.4, (1998), ss.1167-1191.
- Strate, Lance, “The Varieties of Cyberspace: Problems in Definition and Delimitation”, **Western Journal of Communication**, Vol.63, No.3, (1999), ss.382-412.
- Suganami, Hidemi, “Understanding Sovereignty Through Kelsen/Schmitt”, **Review of International Studies**, Vol.33, No.3, (2007), ss.511-530.
- Sui, Daniel Z., “Tobler's First Law of Geography: A Big Idea for a Small World?”, **Annals of the Association of American Geographers**, Vol.94, No.2, (2004), ss.269-277.
- Sunstein, Cass R., “The First Amendment in Cyberspace”, **The Yale Law Journal**, Vol.104, No.7, (1995), ss.1757-1804.
- Surlu, Aydan Ömür, “Leon Duguit’nin Devlet ve Hukuk Anlayışı”, **Erzincan Binali Yıldırım Üniversitesi Hukuk Fakültesi Dergisi**, Cilt.13, Sayı.3-4, (2009), ss.107-132.
- Tabansky, Lior, “Basic Concepts in Cyber Warfare”, **Military and Strategic Affairs**, Vol.3, No.1, (2011), ss.75-92.
- Tan, Oğuzhan, “İslam Hukuk Literatüründe Bir Müşterek Metin İnşâsı Örneği Olarak Şerhu’s Siyeri’l-Kebîr”, **Turkish Studies**, Vol.13, Iss.17, (2018), ss.289-300
- Taşdemir, Özgür, Ümit Vefa Özbay ve Burhanettin Onur Kireçtepe, “Robotların Hukuki ve Cezai Sorumluluğu Üzerine Bir Deneme”, **Ankara Üniversitesi Hukuk Fakültesi Dergisi**, Cilt.69, Sayı.2, (2020), ss.793-834.

- Ten Oever, Niels, “‘This is not How We Imagined It’: Technological Affordances, Economic Drivers, and the Internet Architecture Imaginary”, **New Media & Society**, Vol.23, Iss.2, (2021), ss.344-362.
- Terentieva, Luidmila, “The Issue of State Sovereignty in Cyberspace”, **Legal Issues in the Digital Age**, Vol.2, No.2, (2021), ss.49-67.
- Tüzgen, Abdurrahman Hamza, “Tasarımlara İlişkin Yabancılık Unsuru Taşıyan Uyuşmazlıklarda Uygulanacak Hukuk”, **Ticaret ve Fikri Mülkiyet Hukuku Dergisi**, Cilt.9, Sayı.2, (2023), ss.307-325.
- Uerpman-Witzack, Robert, “Principles of International Internet Law”, **German Law Journal**, Vol.11, Iss.11, (2010), ss.1245-1263.
- Urban, Jennifer M. ve Laura Quilter, “Efficient Process or Chilling Effects - Takedown Notices under Section 512 of the Digital Millennium Copyright Act”, **Santa Clara High Technology Law Journal**, Vol.22, Iss.4, (2006), ss.621-693.
- Ülkeryıldız, Evren ve Nilay Özcan Uslu, “Hakikat Sonrası Bilincin Siber-Mekân Üzerinden Üretimi: Ağdaşın Kamusal Mekânı”, **Eskişehir Osmangazi Üniversitesi Sosyal Bilimler Dergisi**, Cilt.22, Sayı.1, (2021), ss.293-303.
- Wallace Jr., Don, “Extraterritorial Jurisdiction”, **Law and Policy in International Business**, Vol.15, No.4, (1983), ss.1099-1108.
- Watt, Horatia Muir, “Yahoo! Cyber-Collision of Cultures: Who Regulates?”, **Michigan Journal of International Law**, Vol.24, Iss.3, (2003), ss.673-696.
- Waytz, Adam, Carey K. Morewedge, Nicholas Epley, George Monteleone, Jia-Hong Gao ve John T. Cacioppo, “Making Sense by Making Sentient: Effectance Motivation Increases Anthropomorphism”, **Journal of Personality and Social Psychology**, Vol.99, No.3, (2010), ss.410-435.
- Weber, Rolf H., “‘Rose is a Rose is a Rose is a Rose’ – What about Code and Law?”, **Computer Law & Security Review**, Vol.34, Iss.4, (2018), ss.701-706.
- Weber, Valentin, Maria Pericàs Riera ve Emma Laumann, “Mapping the World’s Critical Infrastructure Sectors”, **DGAP Policy Brief**, No.35, (2023), ss.1-9.
- Wheatley, Steven, “Election Hacking, the Rule of Sovereignty, and Deductive Reasoning in Customary International Law”, **Leiden Journal of International Law**, Vol.36, No.3, (2023), ss.675-698.
- Wheatley, Steven, “Foreign Interference in Elections under the Non-intervention Principle: We Need to Talk about ‘Coercion’”, **Duke Journal of Comparative & International Law**, Vol.31, No.1, (2020), ss.161-197.

- Wicaksono, Muhammad Rifky, Kusuma Raditya, Laurensia Andrini ve Muhammad Hawin, “Implementing the Extraterritoriality Principle to Strengthen Competition Law Enforcement in Indonesia in the Aec Era: A Comparative Study”, **Indonesia Law Review**, Vol.9, No.1, (2019), ss.27-50.
- Wu, Timothy S., “Cyberspace Sovereignty? – The Internet and the International System”, **Harvard Journal of Law and Technology**, Vol.10, No.3, (1997), ss.647-666.
- Yayla, Mehmet, “Uluslararası Hukukta Siber Saldırlara Karşı Kuvvet Kullanma”, **Türkiye Barolar Birliği Dergisi**, Sayı.107, (2013), ss.199-220.
- Yen, Alfred C., “Western Frontier or Feudal Society?: Metaphors and Perceptions of Cyberspace”, **Berkeley Technology Law Journal**, Vol.17, No.4 (2002), ss.1207-1263.
- Yıldırım, Ercüment, “Türklerdeki Kut Anlayışı ile Mezopotamya'daki Kralın Kutsallığı İnancının Karşılaştırılması”, **Atatürk Üniversitesi Türkiyat Araştırmaları Enstitüsü Dergisi**, Sayı.70, (2021), ss.325-342.
- Yıldız, Yeşim, “Terör Örgütü Üyeliği Sebebiyle Vatandaşlıktan Çıkarmanın Uluslararası Hukuk Açısından Değerlendirilmesi”, **Sakarya Üniversitesi Hukuk Fakültesi Dergisi**, Cilt.9, Sayı.2, (2011), ss.311-340.
- Yılmaz, Onur, “Küreselleşme Sürecinde Dönüşen Güvenlik Algısı ve Siber Güvenlik”, **Cyberpolitik Journal**, Cilt.2, Sayı.4, (2018), ss.22-43.
- Yücel, Özlem, “Halkların Ekonomik (İktisadi) Self Determinasyon Hakkı ve Afrika’daki Halklar”, **Adam Akademi Sosyal Bilimler Dergisi**, Cilt.4, Sayı.1, (2014), ss.89-100.
- Zeng, Jinghan, Tim Stevens ve Yaru Chen, “China’s Solution to Global Cyber Governance: Unpacking the Domestic Discourse of ‘Internet Sovereignty’”, **Politics & Policy**, Vol.45, No.3, (2017), ss.432-464.
- Zhu, Xianwei, Wei Liu, Zihao Liu ve Zeyu Gu, “Data Recommendation Algorithm of Network Security Event Based on Knowledge Graph”, **Chinese Journal of Network and Information Security**, Vol.9, No.6, (2023), ss.116-126.
- Zins, Chaim, “Conceptual Approaches for Defining Data, Information, and Knowledge”, **Journal of the Association for Information Science and Technology**, Vol.58, Iss.4, (2007), ss.479-493.

Ansiklopedi ve Sözlük Maddeleri

- A **Dictionary of Law**, “sic utere tuo ut alienum non laedas”, Eighth Edition, Oxford: Oxford University Press, 2015.

- Alpyağıl, Recep (Hzl.), “Espace”, **Büyük Felsefe Lugatı**, Cilt I, İstanbul: İz Yayıncılık, 2021.
- Atalay, Besim, “Alan”, **Divanü Lügat-it-Türk Tercümesi**, Ankara: Türk Tarih Kurumu Yayınları, 1985.
- Britannica, “Bulletin-board system”, <https://www.britannica.com/technology/bulletin-board-system> (31.12.2024).
- Bussell, Jennifer, “cyberspace”, Britannica, <https://www.britannica.com/topic/cyberspace> (31.12.2024).
- Butterfield, Andrew, Gerard Ekembe Ngondi ve Anne Kerr, “cyberspace”, **A Dictionary of Computer Science**, 7th Edition, Oxford University Press, 2016.
- CyberPeace Institute, “Cyberspace”, Glossary of Cyber Terms, <https://cyberpeaceinstitute.org/glossary/> (31.12.2024).
- DOD Dictionary of Military and Related Terms, “Cyberspace”, Washington, DC: The Joint Chiefs of Staff, dated April 12, 2001, and amended through November 9, 2006.
- DOD Dictionary of Military and Related Terms, “Cyberspace”, Washington DC: The Joint Chiefs of Staff, March 2017.
- Eskin, Şerif (Hzl.), “Espace”, **Resimli Kâmûs-ı Fransevî**, Cilt II, Ankara: Türkiye Bilimler Akademisi, 2018.
- Glosbe, “Cyberspace”, <https://en.glosbe.com/en/fa/cyberspace> (31.12.2024).
- Güncel Türkçe Sözlük**, “alan”, Türk Dil Kurumu, <https://sozluk.gov.tr> (31.12.2024).
- Güncel Türkçe Sözlük**, “İdare”, Türk Dil Kurumu, <https://sozluk.gov.tr> (31.12.2024).
- Güncel Türkçe Sözlük**, “Yönetişim”, Türk Dil Kurumu, <https://sozluk.gov.tr> (31.12.2024).
- Harman, Ömer Faruk, “Fıravun”, **Türkiye Diyanet Vakfı İslam Ansiklopedisi**, Cilt.13, İstanbul: Türkiye Diyanet Vakfı Yayınları, 1996.
- Kunig, Philip, “Prohibition of Intervention”, **Max Planck Encyclopedia of Public International Law**, Oxford University Press, 2015.
- Larousse, “cybermonde”, <https://www.larousse.fr/dictionnaires/francais/cybermonde> (31.12.2024).
- Merriam Webster Dictionary, “Jurisdiction”, Word History, <https://www.merriam-webster.com/dictionary/jurisdiction#word-history> (31.12.2024).

Pohlmann, Norbert, “cyber-raum”, Institut für Internet-Sicherheit, <https://norbert-pohlmann.com/glossar-cyber-sicherheit/cyber-raum/> (31.12.2024).

Siberay Sözlük, “Siber Vatan”, <https://www.siberay.com/kurumlar/Siberay.com/SIBERAY-Sozluk.pdf> (31.12.2024).

U.S. Department of Commerce / The National Institute of Standards and Technology Computer Security Resource Center, “Cryptocurrency”, Glossary, <https://csrc.nist.gov/glossary/term/cryptocurrency> (31.12.2024).

UNESCO, “Cyberspace”, Internet Governance Glossary, <https://en.unesco.org/glossaries/igg> (31.12.2024).

Yaman, Ahmet, “es-Siyerü’l-kebîr”, **Türkiye Diyanet Vakfı İslam Ansiklopedisi**, Cilt.37, İstanbul: Türkiye Diyanet Vakfı Yayınları, 2009.

Tezler

Bolat, Can, “Siber Saldırılarına Karşı Meşru Müdafaa Hakkının Uluslararası Hukuk Açısından İncelenmesi”, (**Doktora Tezi**, İstanbul Üniversitesi Sosyal Bilimler Enstitüsü, 2020).

Böyük, Şaban, “Bulanık Mantık Yöntemi ile Jeneratörlerde Devir Kontrolü ve Yük Paylaşımı için Elektronik Governör Tasarımı ve Uygulaması”, (**Yüksek Lisans Tezi**, Marmara Üniversitesi Fen Bilimleri Enstitüsü Mekatronik Anabilim Dalı, 2011).

Çiçekçi, Melih Furkan, “Genel Hukuk Teorisi ve Zorlama Kavramı”, (**Yüksek Lisans Tezi**, Bursa Uludağ Üniversitesi Sosyal Bilimler Enstitüsü, 2024).

Emrağ, Sırma Korkut, “Bilgisayar Programlarının Fikri Mülkiyet Hukuku Kapsamında Korunması”, (**Yüksek Lisans Tezi**, İstanbul Bilgi Üniversitesi, Lisansüstü Programlar Enstitüsü, 2024).

Kaptanoğlu, Bülent, “Bilgisayar Teknolojilerinin Gelişmesi ile Ortaya Çıkan Siber Mekan Kavramı ve Mimarlığa Olan Etkileri”, (**Yayınlanmamış Yüksek Lisans Tezi**, Yıldız Teknik Üniversitesi, Fen Bilimleri Enstitüsü, 2000).

Korhan, Sevda, “Siber Uzayda Uluslararası İlişkilerin Değişen Parametreleri”, (**Yüksek Lisans Tezi**, Selçuk Üniversitesi Sosyal Bilimler Enstitüsü, 2018).

Uluslararası Antlaşmalar

Ay ve Diğer Gök Cisimleri Dâhil, Uzayın Keşif ve Kullanılmasında Devletlerin Faaliyetlerini Yöneten İlkeler Hakkında Antlaşma (*Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and Other Celestial Bodies*), UNTS, Vol.610, No.8843, 1970.

Bilgi Teknolojisi Suçlarıyla Mücadele Hakkında Arap Sözleşmesi (*Arab Convention on Combating Information Technology Offences*), <https://www.asianlaws.org/gcld/cyberlawdb/GCC/Arab%20Convention%20on%20Combating%20Information%20Technology%20Offences.pdf> (31.12.2024).

Birleşmiş Milletler Şartı (*United Nations Charter*), <https://www.un.org/en/about-us/un-charter/full-text> (31.12.2024).

Devletlerin Ay'da ve Diğer Gök Cisimlerindeki Faaliyetlerini Düzenleyen Anlaşma (*Agreement Governing the Activities of States on the Moon and Other Celestial Bodies*), UNTS, Vol.1363, No.23002, 1992.

Dış Uzaya Fırlatılan Cisimlerin Tescili Sözleşmesi (*Convention on Registration of Objects Launched into Outer Space*), UNTS, Vol.1023, No.15020, 1976.

DTÖ-WIPO İş Birliği Anlaşması (*WTO-WIPO Cooperation Agreement*), https://www.wto.org/english/tratop_e/trips_e/wtowip_e.htm (31.12.2024).

Edebiyat ve Sanat Eserlerinin Korunmasına İlişkin Bern Sözleşmesi (*Berne Convention for the Protection of Literary and Artistic Works*), <https://www.wipo.int/wipolex/en/text/283693> (31.12.2024).

Fikri Mülkiyet Haklarının Ticaretle İlişkili Yönleri Hakkı Anlaşma (*Agreement on Trade-Related Aspects of Intellectual Property Rights*), https://www.wto.org/english/docs_e/legal_e/27-trips_01_e.htm (31.12.2024).

İnsan Haklarının ve Temel Özgürlüklerin Korunması Sözleşmesi (*Convention for the Protection of Human Rights and Fundamental Freedoms*), UNTS, Vol.213, No.2889, 1955.

Medeni ve Siyasi Haklar Sözleşmesi (*International Covenant on Civil and Political Rights*), UNTS, Vol.999, No.14668, 1976.

Sanal Ortamda İşlenen (Siber) Suçlar Sözleşmesi (*Convention on Cybercrime*) "Convention on Cybercrime", UNTS, Vol.2296, No.40916, 2006.

- Sanal Ortamda İşlenen Suçlar Sözleşmesine Ek, Bilgisayar Sistemleri Aracılığıyla İşlenen Irkçı ve Yabancı Düşmanı Nitelikteki Eylemlerin Suç Sayılmasına İlişkin Protokol (*Additional Protocol to the Convention on Cybercrime, Concerning the Criminalisation of Acts of a Racist and Xenophobic Nature Committed through Computer Systems*), UNTS, Vol.2466, No.40916, 2006.
- Sanal Ortamda İşlenen Suçlar Sözleşmesine İkinci Ek, Gelişmiş İş Birliği ve Elektronik Delillerin İfşasına İlişkin Protokol (*Second Additional Protocol to the Convention on Cybercrime on Enhanced Co-Operation and Disclosure of Electronic Evidence*), CETS No. 224.
- Siber Güvenlik ve Kişisel Verilerin Korunması Hakkında Afrika Birliği Sözleşmesi (*African Union Convention on Cyber Security and Personal Data Protection*), <https://au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection> (31.12.2024).
- Terörizme Karşı Şangay İşbirliği Örgütü Konvansiyonu (*Convention of the Shanghai Cooperation Organization Against Terrorism*), UNTS, Vol.2815, No.49374, 2012.
- Türkmenistan Hükümeti ile Rusya Federasyonu Hükümeti arasında Uluslararası Bilgi Güvenliğinin Sağlanmasında İşbirliği Anlaşması (*Agreement between the Government of Turkmenistan and the Government of the Russian Federation on Cooperation in Ensuring International Information Security*), UNTS, Registration No.56871, 2021.
- Uluslararası Telekomünikasyon Örgütü Kuruluş Yasası ve Sözleşmesi (*Constitution and Convention of the International Telecommunication Union*), UNTS, Vol.1825, No.31251, 1998.
- Uzay Cisimlerinin Verdiği Zararlardan Dolayı Uluslararası Sorumluluk Hakkında Sözleşme (*Convention on International Liability for Damage Caused by Space Objects*), UNTS, Vol.961, No.13810, 1975.
- Vatansız Kişilerin Statüsüne İlişkin Sözleşme (*Convention Relating to the Status of Stateless Persons*), UNTS, Vol.360, No.5158, 1960.
- Vatansızlığın Azaltılmasına İlişkin Sözleşme (*Convention on the Reduction of Statelessness*), UNTS, Vol.989, No.14458, 1983.
- Viyana Antlaşmalar Hukuku Sözleşmesi (*Vienna Convention on the Law of Treaties*), UNTS, Vol.1155, No.18232, 1987.
- Westfalya Barış Antlaşması (*Acta Pacis Westphalicae*), http://www.pax-westphalica.de/ipmipo/pdf/o_1732en-treatys.pdf (31.12.2024)
- WIPO Telif Antlaşması (*WIPO Copyright Treaty*), <https://www.wipo.int/wipolex/en/text/295166> (31.12.2024).

Avrupa Birliđi Düzenlemeleri

Avrupa Ağ ve Bilgi Güvenliđi Ajansı Kurucu Tüzüğü (*Regulation Establishing the European Network and Information Security Agency*), <http://data.europa.eu/eli/reg/2004/460/oj> (31.12.2024).

Birliđin Kurum, Kuruluş, Ofis ve Ajanslarında Yüksek Düzeyde Ortak Siber Güvenlik Tedbirlerini Belirleyen Tüzük (*Regulation Laying Down Measures for a High Common Level of Cybersecurity at the Institutions, Bodies, Offices and Agencies of the Union*), <http://data.europa.eu/eli/reg/2023/2841/oj> (31.12.2024).

Dijital Hizmetler Yasası (*Digital Services Act*), <http://data.europa.eu/eli/reg/2022/2065/oj> (31.12.2024).

Dijital Piyasalar Yasası (*Digital Markets Act*), <http://data.europa.eu/eli/reg/2022/1925/oj> (31.12.2024).

Elektronik Ticaret Direktifi (*Directive on Electronic Commerce*), <http://data.europa.eu/eli/dir/2000/31/oj> (31.12.2024).

Genel Veri Koruma Tüzüğü (*General Data Protection Regulation*), <http://data.europa.eu/eli/reg/2016/679/oj> (31.12.2024).

Kripto Varlık Piyasaları Tüzüğü (*The Markets in Crypto-Assets Regulation*), <http://data.europa.eu/eli/reg/2023/1114/2024-01-09> (31.12.2024).

Kritik Varlıkların Dayanıklılığı Hakkında Direktif (*Directive on the Resilience of Critical Entities*), <http://data.europa.eu/eli/dir/2022/2557/oj> (31.12.2024),

Siber Dayanıklılık Yasası, (*Cyber Resilience Act*), <https://data.consilium.europa.eu/doc/document/PE-100-2023-REV-1/en/pdf> (31.12.2024).

Siber Güvenlik Yasası (*Cybersecurity Act*), <http://data.europa.eu/eli/reg/2019/881/oj> (31.12.2024).

Terörist İçeriğın Çevrimiçi Yayılmasının Önlenmesine ilişkin Tüzük (*Regulation on Addressing the Dissemination of Terrorist Content Online*), <http://data.europa.eu/eli/reg/2021/784/oj> (31.12.2024).

Yapay Zekâ Yasası (*Artificial Intelligence Act*), <http://data.europa.eu/eli/reg/2024/1689/oj> (31.12.2024).

Ulusal Hukuk Düzenlemeleri

ABD, Amerikalıları Yabancı Hasım Kontrolündeki Uygulamalardan Koruma Yasası (*Protecting Americans from Foreign Adversary Controlled Applications Act*), 118th Congress, H.R.7521.

ABD, Çocukların Çevrimiçi Mahremiyetinin Korunması Yasası (*Children's Online Privacy Protection Act*), 15 U.S. Code, §§6501-6506.

ABD, Çocukların İnternette Korunması Yasası (*Children's Internet Protection Act*), 47 CFR 54.520.

ABD, DARPA Kurucu Direktifi (*Department of Defence Advanced Research Projects Agency*), US Department of Defence, **Directive 5105.15**, 07.02.1958.

ABD, Devletlerin ve Mağdurların Çevrimiçi Seks Ticaretiyle Mücadele Etmesine İzin Yasası (*Allow States and Victims to Fight Online Sex Trafficking Act*) ve Seks Tacirlerini Müsaadeyi Durdurma Yasası (*Stop Enabling Sex Traffickers Act*) (FOSTA-SESTA), 132 Stat. 1253 – Public Law No.115-164, 11.04.2018.

ABD, Dijital Binyıl Telif Hakkı Yasası (*Digital Millennium Copyright Act*), 17 U.S. Code, §512.

ABD, FISA Değişiklikleri (*FISA Amendments*), 129 Stat. 268 – Public Law No.114-23, 06.02.2015.

ABD, İç Güvenlik Başkanlık Direktifi 7, (*Homeland Security Presidential Directive 7*).

ABD, Kolluk Kuvvetleri için İletişim Yardımı Yasası (*Communications Assistance for Law Enforcement Act*), Public Law 103-414.

ABD, Kritik Altyapı Siber Güvenliğinin Geliştirilmesi, Yürütme Emri, (*Improving Critical Infrastructure Cybersecurity, Executive Order*), 12.02.2013.

ABD, Müttefik Olmayan Yabancı Ülkelerden Hassas Malzemelerin Edinilmesi: Yasaklama (*Acquisition of Sensitive Materials from Non-allied Foreign Nations: Prohibition*), 10 U.S. Code §4872.

ABD, Sakıncalı İçeriklerin Özel Olarak Engellenmesi ve Filtrelenmesine Yönelik Koruma, (*Protection for Private Blocking and Screening of Offensive Material*), 47 U.S. Code, §230.

Avusturalya, Avustralya Ceza Kanunu 1995 (*Criminal Code Act 1995*), (Cth).

Birleşik Krallık, Çevrimiçi Güvenlik Yasası 2023 (*Online Safety Act 2023*), Chapter.50.

Birleşik Krallık, Terörizm Yasası 2000 (*Terrorism Act 2000*), Chapter.11.

- Çin Halk Cumhuriyeti Siber Güvenlik Yasası (*Cybersecurity Law of the People's Republic of China*), <https://digichina.stanford.edu/work/translation-cybersecurity-law-of-the-peoples-republic-of-china-effective-june-1-2017/> (31.12.2024); <https://www.chinajusticeobserver.com/law/x/cybersecurity-law-of-china-20161107> (31.12.2024).
- Çin Halk Cumhuriyeti, Çevrimiçi Bilgi İçeriği Ekosisteminin Yönetişimine İlişkin Hükümler, Çin Siber Uzay İdaresi, 5 Numaralı Emir (*Provisions on the Governance of the Online Information Content Ecosystem, Order of the Cyberspace Administration of China No.5*), <https://wilmap.stanford.edu/entries/provisions-governance-online-information-content-ecosystem> (31.12.2024).
- Çin Halk Cumhuriyeti, Çin Halk Cumhuriyeti Kişisel Bilgi Koruma Yasası (*Personal Information Protection Law of the People's Republic of China*), http://en.npc.gov.cn.cdurl.cn/2021-12/29/c_694559.htm (31.12.2024).
- Çin Halk Cumhuriyeti, Çin Halk Cumhuriyeti Kriptografi Yasası (*Cryptography Law of the People's Republic of China*), <https://appinchina.co/government-documents/cryptography-law-of-the-peoples-republic-of-china/> (31.12.2024).
- Çin Halk Cumhuriyeti, Kamu Güvenlik Kurumları Tarafından İnternet Güvenliği Gözetim ve Denetimine İlişkin Yönetmelik (*Regulations on Internet Security Supervision and Inspection by Public Security Bodies*), <https://digichina.stanford.edu/work/regulations-on-internet-security-supervision-and-inspection-by-public-security-bodies/> (31.12.2024).
- Rusya Federasyonu, Bilgi, Bilgi Teknolojileri ve Bilginin Korunması Hakkında Federal Yasa (*Federal Law On Information, Information Technologies and Protection of Information*), The Russian Federation Federal law No. 149-FZ of 14 July 2006. <https://eais.rkn.gov.ru/docs.eng/149.pdf> (31.12.2024).
- Rusya Federasyonu, Operasyonel Arama Faaliyetleri Federal Yasası (*Federal Law on Operational-Search Activities*), Federal Law No.144-FZ of 12 August 1995, https://www.wto.org/english/thewto_e/acc_e/rus_e/wtaccrus58_leg_373.pdf (31.12.2024).
- Rusya Federasyonu, Rusya Federasyonu Bilgi Güvenliği Doktrini (*Doctrine of Information Security of the Russian Federation*), No. 646 of December 5, 2016.
- T.C., 4110 sayılı 5846 Sayılı Fikir ve Sanat Eserleri Kanununun Bazı Maddelerinin Değiştirilmesine İlişkin Kanun, R. G., 12.06.1995, Sayı.22311.
- T.C., 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun, R. G., 04.05.2007, Sayı.26530.
- T.C., 5809 sayılı Elektronik Haberleşme Kanunu, R. G., 10.11.2008, Sayı.27050.

- T.C., 5846 Sayılı Fikir ve Sanat Eserleri Kanunu, R. G., 13.12.1951, Sayı.7981.
- T.C., 6361 sayılı Finansal Kiralama, Faktoring, Finansman ve Tasarruf Finansman Şirketleri Kanunu, R. G., 21.11.2012, Sayı.28496.
- T.C., 6532 sayılı Devlet İstihbarat Hizmetleri ve Millî İstihbarat Teşkilâtı Kanununda Değişiklik Yapılmasına Dair Kanun, R. G., 26.04.2014, Sayı.28983.
- T.C., 6563 sayılı Elektronik Ticaretin Düzenlenmesi Hakkında Kanun, R. G., 05.11.2014, Sayı.29166.
- T.C., 6698 sayılı Kişisel Verilerin Korunması Kanunu, R. G., 24.03.2016, Sayı.29677.
- T.C., 7253 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanunda Değişiklik Yapılmasına Dair Kanun (Sosyal Medya Yasası), R. G., 31.07.2020, Sayı.31202.
- T.C., 7518 sayılı Sermaye Piyasası Kanununda Değişiklik Yapılmasına Dair Kanun, R. G., 02.07.2024, Sayı.32590.
- T.C., Elektronik Haberleşme Sektörüne İlişkin Yetkilendirme Yönetmeliği, R. G., 28.05.2009, Sayı.27241.
- T.C., İnternet Toplu Kullanım Sağlayıcıları Hakkında Yönetmelik, R. G., 11.04.2017, Sayı.30035.
- T.C., Motorlu Araçlar ve Römorkları ile Bunlar İçin Tasarlanan Aksam, Sistem ve Ayrı Teknik Ünitelerin Genel Güvenliği ve Korunmasız Karayolu Kullanıcılarının ve Yolcuların Korunması ile İlgili Tip Onayı Yönetmeliği, R. G., 14.05.2020, Sayı.31127.
- T.C., Ödemelerde Kripto Varlıkların Kullanılmamasına Dair Yönetmelik, R. G., 16.04.2021, Sayı.31456.
- T.C., Telekomünikasyon Kurumu Tarafından Erişim Sağlayıcılara ve Yer Sağlayıcılara Faaliyet Belgesi Verilmesine İlişkin Usul ve Esaslar Hakkında Yönetmelik, R. G., 24.10.2007, Sayı.26680.
- T.C., Uluslararası Telekomünikasyon Birliği (ITU) Kuruluş Yasası ve Sözleşmesinde Değişiklik Yapan Kyoto ve Minneapolis Tam Yetkili Konferansları Sonuç Belgelerinin Beyanlarla ve Çekincelerle Onaylanması Hakkında Karar, R. G., 24.10.2008, Sayı.27034, Karar Sayısı.2008/14157.

Yargı Kararları

ABD, Intel Corporation v. European Commission, Judgment of the Court (Grand Chamber), Case C-413/14 P., 06.09.2017.

ABD, U.S. Justice Department v. International Business Machines Corporation, US Court of Appeals for the Second Circuit, 687 F.2d 591, 13.08.1982.

ABD, United States v. Aluminum Company of America, U.S. Court of Appeals for the Second Circuit, 148 F.2d 416, 12.03.1945.

ABD, United States v. General Electric Company, U.S. District Court for the District of New Jersey, 82 F. Supp. 753, 04.04.1949.

ABD, United States v. Watchmakers of Switzerland Information Center, U.S. District Court for the Southern District of New York, 25 F.R.D. 203, 3 Fed. R. Serv. 2d 648, 02.03.1960.

AİHM, Perrin v. The United Kingdom, **Decision**, European Court of Human Rights, No.5446/03, 18.10.2005.

BM, Island of Palmas Case (Netherlands, USA), **Reports of the International Arbitral Awards**, Vol.II, 04.04.1928.

T.C., T.C. Anayasa Mahkemesi, E.2020/76, K.2023/172, 11/10/2023.

T.C., Yargıtay 18. Ceza Dairesi, E.2018/5669, K.2019/10900, 19.06.2019.

T.C., Yargıtay 4. Ceza Dairesi, E.2021/30178, K.2021/27676, 25.11.2021.

UAD, Corfu Channel Case, Merits, **Judgment**, ICJ Reports, 1949.

UAD, Military and Paramilitary Activities in and Against Nicaragua (Nicaragua v. United States of America), Merits, **Judgment**, ICJ Reports, 1986.

UAD, Reparation for Injuries Suffered in the Service of the United Nations, **Advisory Opinion**, ICJ Reports, 1949.

UAD, Western Sahara, **Advisory Opinion**, ICJ Reports, 1975.

Birleşmiş Milletler Karar ve Belgeleri

UN/General Assembly, A Universal Declaration of Human Rights, **A/RES/217(III)**, 10.12.1948.

- UN/General Assembly, Countering the Use of Information and Communications Technologies for Criminal Purposes, **A/RES/74/247**, 20.01.2020.
- UN/General Assembly, Declaration of Principles Governing the Sea-Bed and the Ocean Floor, and the Subsoil Thereof, beyond the Limits of National Jurisdiction, **A/RES/2749(XXV)**, 17.12.1970.
- UN/General Assembly, Declaration on Principles of International Law concerning Friendly Relations and Cooperation among States in accordance with the Charter of the United Nations, **A/RES/2625(XXV)**, 24.10.1970.
- UN/General Assembly, Declaration on the Inadmissibility of Intervention in the Domestic Affairs of States and the Protection of Their Independence and Sovereignty, **A/RES/20/2131(XX)**, 21.12.1965.
- UN/General Assembly, Developments in the Field of Information and Telecommunications in the Context of International Security, **A/RES/73/27**, 05.12.2018.
- UN/General Assembly, Developments in the Field of Information and Telecommunications in the Context of International Security, **A/RES/75/240**, 31.12.2020.
- UN/General Assembly, Developments in the Field of Information and Telecommunications in the Context of International Security, **A/59/116/Add.1**, 28.12.2004,
- UN/General Assembly, Developments in the field of information and telecommunications in the context of international security, **A/RES/53/70**, 04.01.1999.
- UN/General Assembly, Draft Declaration on Rights and Duties of States, **A/RES/596(VI)**, 05.02.1952.
- UN/General Assembly, Letter dated 23 September 1998 from the Permanent Representative of the Russian Federation to the United Nations addressed to the Secretary-General, **A/C.1/53/3**, 30.09.1998.
- UN/General Assembly, Letter dated 9 January 2015 from the Permanent Representatives of China, Kazakhstan, Kyrgyzstan, the Russian Federation, Tajikistan and Uzbekistan to the United Nations addressed to the Secretary-General, **A/69/723**, 13.01.2015.
- UN/General Assembly, Official compendium of voluntary national contributions on the subject of how international law applies to the use of information and communications technologies by States submitted by participating governmental experts in the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security established pursuant to General Assembly resolution, **A/76/136**, 13.07.2021.

- UN/General Assembly, Overview of Existing Instruments, Recommendations and Other Documents on Countering the Use of Information and Communications Technologies for Criminal Purposes, **A/AC.291/CRP.10**, 20.04.2022.
- UN/General Assembly, Permanent Sovereignty over Natural Resources, **A/RES/1803(XVII)**, 14.12.1962.
- UN/General Assembly, Report of the Open-ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security, **A/75/816**, 18.03.2021.
- UN/General Assembly, Report of the Open-ended Working Group on Security of and in the Use of Information and Communications Technologies 2021-2025, **A/77/275**, 08.08.2022.
- UN/General Assembly, Report of the Open-ended Working Group on Security of and in the Use of Information and Communications Technologies 2021-2025, **A/78/265**, 01.08.2023.
- UN/General Assembly, Report of the Open-ended Working Group on Security of and in the Use of Information and Communications Technologies 2021-2025, **A/79/214**, 22.07.2024.
- UN/General Assembly, Reservation exclusively for peaceful purposes of the sea-bed and the ocean floor, and the subsoil thereof, underlying the high seas beyond the limits of present national jurisdiction and the use of their resources in the interests of mankind, and convening of a conference on the law of the sea, **A/RES/2750 (XXV)**, 17.12.1970.
- UN/General Assembly, Responsibility of States for Internationally Wrongful Acts, **A/RES/56/83**, 28.01.2002.
- UN/General Assembly, The Right to Privacy in the Digital Age, **A/RES/68/167**, 21.01.2014.
- UN/Open-ended Working Group on Information and Communication Technologies, China's Positions on International Rules-making in Cyberspace, Working Papers, 01.12.2021; <https://documents.unoda.org/wp-content/uploads/2021/12/Chinese-Position-Paper-on-International-Rules-making-in-Cyberspace-ENG.pdf> (31.12.2024).
- UN/Open-ended Working Group on Information and Communication Technologies, China's Positions on International Rules-making in Cyberspace, Working Papers, 01.12.2021; <https://documents.unoda.org/wp-content/uploads/2021/12/Chinese-Position-Paper-on-International-Rules-making-in-Cyberspace-CHN.pdf> (31.12.2024).

UN/Open-ended Working Group on Information and Communication Technologies, Concept paper on establishing a permanent Open-Ended Working Group by Russian Federation (co-sponsors: Belarus, Burundi, Cuba, DPRK, Eritrea, Myanmar, Nicaragua, Syrian Arab Republic, Sudan, Venezuela, Zimbabwe), Working Papers, 15.12.2023. [https://docs-library.unoda.org/Open-Ended-Working-Group-on-Information-and-Communication-Technologies-\(2021\)/ENG-Concept-paper-on-a-Permanent-Decision-making-OEWG.pdf](https://docs-library.unoda.org/Open-Ended-Working-Group-on-Information-and-Communication-Technologies-(2021)/ENG-Concept-paper-on-a-Permanent-Decision-making-OEWG.pdf) (31.12.2024).

UN/Open-ended Working Group on Information and Communication Technologies, Working Paper: Towards a Regular Institutional Dialogue on International ICT Security by UNIDIR (United Nations Institute for Disarmament Research), Working Papers, 28.06.2024, [https://docs-library.unoda.org/Open-Ended-Working-Group-on-Information-and-Communication-Technologies-\(2021\)/UNIDIR-TOWARDS-A-REGULAR-INSTITUTIONAL-DIALOGUE-ON-INTERNATIONAL-ICT-SECURITY-3.pdf](https://docs-library.unoda.org/Open-Ended-Working-Group-on-Information-and-Communication-Technologies-(2021)/UNIDIR-TOWARDS-A-REGULAR-INSTITUTIONAL-DIALOGUE-ON-INTERNATIONAL-ICT-SECURITY-3.pdf) (31.12.2024).

UN/Open-ended Working Group on Information and Communication Technologies, China's Positions on International Rules-making in Cyberspace, Working Papers, 01.12.2021, <https://documents.unoda.org/wp-content/uploads/2021/12/Chinese-Position-Paper-on-International-Rules-making-in-Cyberspace-ENG.pdf> (31.12.2024).

UN/Open-ended Working Group on Information and Communication Technologies, Concept Paper on a Permanent Decision-Making Open-Ended Working Group on Security of and in the Use of Information and Communications Technologies, Working Papers, 08.03.2024, [https://docs-library.unoda.org/Open-Ended-Working-Group-on-Information-and-Communication-Technologies-\(2021\)/ENG-Concept-paper-on-a-Permanent-Decision-making-OEWG.pdf](https://docs-library.unoda.org/Open-Ended-Working-Group-on-Information-and-Communication-Technologies-(2021)/ENG-Concept-paper-on-a-Permanent-Decision-making-OEWG.pdf) (31.12.2024).

UN/Open-ended Working Group on Information and Communication Technologies, Joint Position of the Republic of Belarus, the Republic of Cuba, the Islamic Republic of Iran, Republic of Nicaragua, the Russian Federation, the Syrian Arab Republic and the Bolivarian Republic of Venezuela on the Draft Annual Progress Report of the Open-ended Working Group on Security of and in the Use of ICTs 2021-2025, Working Papers, 25.07.2022, <https://documents.unoda.org/wp-content/uploads/2022/07/Draft-Joint-Position-on-the-OEWG-draft-report-Final.pdf> (31.12.2024).

- UN/Open-ended Working Group on Information and Communication Technologies, Updated Concept of the Convention of the United Nations Ensuring International Information Security submitted by Russian Federation (Cosponsors: Belarus, DPRK, Nicaragua, Syria, Venezuela), Working Papers, 29.06.2023, [https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_ \(2021\)/ENG_Concept_of_convention_on_ensuring_international_information_security.pdf](https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_ (2021)/ENG_Concept_of_convention_on_ensuring_international_information_security.pdf) (31.12.2024).
- UN/Open-ended Working Group on Information and Communication Technologies, Statement by the Representative of the Russian Federation at the Online Discussion of the Second “Pre-draft” of the Final Report of the UN Open-ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security, 15.06.2020, <https://front.un-arm.org/wp-content/uploads/2020/09/oewg-informal-virtual-meetings-statement-by-the-russian-federation-15-june-2020.pdf> (31.12.2024).
- UN/Open-ended Working Group on Information and Communication Technologies, Statement on Existing and Potential Threats by Turkey, Statements, 29.03.2022, <https://documents.unoda.org/wp-content/uploads/2022/03/Turkey-Statement-OEWG-29-March-2022.pdf> (31.12.2024).
- UN/Open-ended Working Group on Information and Communication Technologies, General Statement of Views by Turkey, Statements, 14.12.2021, <https://documents.unoda.org/wp-content/uploads/2021/12/STATEMENT-BY-TURKEY-OEWG-2021-2025-002.pdf> (31.12.2024).
- UN/Open-ended Working Group on Information and Communication Technologies, Statement by Turkey: Informal Meeting of the Open-ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security, ZD Statement, 19.02.2021, https://front.un-arm.org/wp-content/uploads/2021/02/Turkey-statement_OEWG-informal-meeting_February-2021.pdf (31.12.2024).
- UN/Open-ended Working Group on Information and Communication Technologies, Working Paper on application of international humanitarian law to the use of ICTs in situations of armed conflict submitted by Group of States, Working Papers, 01.03.2024, [https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_ \(2021\)/OEWG_Working_Paper_IHL_ICT_Operations.pdf](https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_ (2021)/OEWG_Working_Paper_IHL_ICT_Operations.pdf) (31.12.2024).
- UN/Open-ended Working Group on Information and Communication Technologies, Position Paper on the Application of International Law in Cyberspace by Ireland, Working Papers, 07.07.2023, [https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_ \(2021\)/Ireland_-_National_Position_Paper.pdf](https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_ (2021)/Ireland_-_National_Position_Paper.pdf) (31.12.2024).

UN/Open-ended Working Group on Information and Communication Technologies, Non-paper "on spyware and its use by US intelligence services" by Russian Federation, Non-papers, 10.07.2024, [https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_ \(2021\)/Spyware_and_its_use_by_US_intelligence_services_ENG_0.pdf](https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_ (2021)/Spyware_and_its_use_by_US_intelligence_services_ENG_0.pdf) (31.12.2024).

Raporlar, Standartlar ve Sair Belgeler

Bilgi Teknolojileri ve İletişim Kurumu, **Türkiye Elektronik Haberleşme Sektörü Üç Aylık Pazar Verileri Raporu**, 2024 Yılı 1. Çeyrek.

Clark, David D., “Characterizing Cyberspace: Past, Present and Future”, **ECIR Working Paper No.2010-3**, MIT Political Science Department, 2010.

COE/Cybercrime Program Office (C-PROC), **The Global State of Cybercrime Legislation 2013 – 2019: A cursory Overview**, Update as at 30 June 2019 Prepared by the Cybercrime Programme Office of the Council of Europe, Version 4 July 2019 / Public, Bucharest, Romania.

Dingwerth, Klaus, “From International Politics to Global Governance? The Case of Nature Conservation”, **GARNET Working Paper No. 46/08**, Institute for Intercultural and International Studies, University of Bremen, 2008.

Goldsmith, Jack ve Alex Loomis, “‘Defend Forward’ and Sovereignty”, **Hoover Working Group on National Security, Technology, and Law**, Aegis Series Paper No.2102, 29.04.2021.

Halog, Jason, Paul Margat ve Michael Stadermann, “Legal Considerations on the Protection of Subsea Cables in the International and National Legislative Framework”, **3rd European Workshop on Maritime Systems, Resilience and Security 2023 (MARESEC 23)**, Bremen: Institut für den Schutz maritimer Infrastrukturen, 04.10.2023.

Hitchens, Theresa ve Nilsu Gören, “International Cybersecurity Information Sharing Agreements”, **Study Report**, Center for International & Security Studies, University of Maryland, 2017.

International Development Law Organization (IDLO) ve UNCHR, **Addressing Statelessness through the Rule of Law**, 2022.

International Law Association, Committee on Submarine Cables and Pipelines, Submarine Cables and Pipelines under International Law, **Interim Report 2020**.

ISO/IEC, Information Technology – Open Systems Interconnection – Basic Reference Model: The Basic Model, **ISO/IEC 7498-1:1993(E)**.

ISO/IEC, Information technology — Security techniques — Guidelines for cybersecurity, International Standard, **ISO/IEC 2703:2012(E)**.

ITU, **The ITU National Cybersecurity Strategy Guide**, 2011.

Joint Publication (JP) 3–12, Cyberspace Operations, Washington, DC: The Joint Chiefs of Staff, March 2017.

Korzak, Elaine, “Russia’s Cyber Policy Efforts in the United Nations”, **Tallinn Paper No.11**, NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE), 2021.

Ku, Julian, “How China’s Views on the Law of Jus ad Bellum Will Shape Its Legal Approach to Cyberwarfare”, **Hoover Working Group on National Security, Technology, and Law**, Aegis Series Paper No.1707, (17.08.2017).

Leroux, Christophe ve Roberto Labruto (Ed.), **Suggestion for a Green Paper on Legal Issues in Robotics**, The European Robotics Coordination Action, Grant Agreement Number: 248552, 2012.

Raynova, Denitsa, “Towards a Common Understanding of the Non-Intervention Principle”, **European Leadership Network Post-Workshop Report**, 2017.

Rollins, John W., Susan V. Lawrence, Dianne E. Rennack ve Catherine A. Theohary, **U.S.-China Cyber Agreement**, Library of Congress, Congressional Research Service (CRS) Insight, IN10376, 16.10.2015.

T.C. Ulaştırma Denizcilik ve Haberleşme Bakanlığı, **2016-2019 Ulusal Siber Güvenlik Stratejisi**.

T.C. Ulaştırma ve Altyapı Bakanlığı, **Ulusal Siber Güvenlik Stratejisi ve Eylem Planı (2020-2023)**.

T.C. Ulaştırma ve Altyapı Bakanlığı, **Ulusal Siber Güvenlik Stratejisi ve Eylem Planı (2024-2028)**.

TBMM, **Kişisel Verilerin Korunması Kanunu Tasarısı (1/541) ve Adalet Komisyonu Raporu**, Sıra No.117, Yasama Dönemi.26, Yasama Yılı.1.

TBMM, **Sanal Ortamda İşlenen Suçlar Sözleşmesinin Onaylanmasının Uygun Bulunduğuna Dair Kanun Tasarısı ve Dışişleri Komisyonu Raporu**, (1/676), Yasama Dönemi.24, Yasama Yılı.3, Sıra Sayısı.380.

UNESCO/Executive Board, “Preliminary Study on the Technical and Legal Aspects Relating to the Desirability of a Standard-Setting Instrument on the Ethics of Artificial Intelligence”, **206 EX/42**, 21.03.2019.

United Nations Security Council / Counter-Terrorism Committee Executive Directorate (CTED), “Physical Protection of Critical Infrastructure Against Terrorist Attacks”, **CTED Trends Report**, 2017.

United States / Office of the Director of National Intelligence, **A Guide to Cyber Attribution**, 14.09.2018.

United States Department of Commerce / National Telecommunications and Information Administration, “Statement of Policy on the Management of Internet Names and Addresses”, Docket Number:980212036-8146-02, 05.06.1998.

United States Department of Commerce / National Telecommunications and Information Administration, “Memorandum of Understanding Between the U.S. Department of Commerce and the Internet Corporation for Assigned Names and Numbers”, 25.11.1998.

United States, White House, **National Cybersecurity Strategy**, Washington, 01.03.2023.

Web Sayfaları

Adonis, Abid A., “International Law on Cyber Security in the Age of Digital Sovereignty”, E-International Relations, 14.03.2020, <https://www.e-ir.info/2020/03/14/international-law-on-cyber-security-in-the-age-of-digital-sovereignty/> (31.12.2024).

AlArabiya News, “Saudi Aramco Says Cyber Attack Targeted Kingdom’s Economy”, 09.12.2012, <https://english.alarabiya.net/articles/2012/12/09/254162> (31.12.2024).

American Civil Liberties Union, “Surveillance Under the USA/PATRIOT Act”, <https://www.aclu.org/documents/surveillance-under-usapatriot-act> (31.12.2024).

Anadolu Ajansı, “Instagram’a Uygulanan Erişim Engeli Kaldırıldı”, 11.08.2024, <https://www.aa.com.tr/tr/info/infografik/40694> (31.12.2024).

Article 19, “Türkiye: Uçtan Uca Şifreleme Korunmalı”, 20.04.2023, <https://www.article19.org/tr/resources/turkey-protect-end-to-end-encrypted-services/> (31.12.2024).

Associated Press, “Snowden Receives Russian Passport, takes Citizenship Oath”, 02.12.2022, <https://apnews.com/article/putin-europe-united-states-moscow-edward-snowden-48d05f2699466f1c5c9b5d04f57d553b> (31.12.2024).

- Atlantic Council, “Central Bank Digital Currency Tracker”, <https://www.atlanticcouncil.org/cbdctracker/> (31.12.2024).
- Barlow, John Perry, “A Declaration of the Independence of Cyberspace”, Electronic Frontier Foundation, <https://www.eff.org/tr/cyberspace-independence> (31.12.2024).
- Barlow, John Perry, “Jack In, Young Pioneer!”, 11.08.1994, <https://www.eff.org/tr/pages/jack-young-pioneer> (31.12.2024).
- Brodin, Jon, “Ukraine asks ICANN to Revoke Russian Domains and Shut Down DNS Root Servers”, Ars Technica, 02.03.2022, <https://arstechnica.com/tech-policy/2022/03/ukraine-wants-russia-cut-off-from-core-internet-systems-experts-say-its-a-bad-idea/> (31.12.2024).
- BTK, “Denetleme”, 15.12.2017, <https://www.btk.gov.tr/denetleme> (31.12.2024).
- BTK, “Finans Sektörü Siber Kalkan 2022 Tatbikatı Başladı”, 20.10.2022, <https://www.btk.gov.tr/haberler/finans-sektoru-siber-kalkan-2022-tatbikati-basladi> (31.12.2024).
- BTK, “İnternet İhbar Başvurusu”, <https://www.turkiye.gov.tr/btk-internet-ihbar-basvurusu> (31.12.2024).
- BTK, “Ulusal Siber Kalkan 2021 Tatbikatı Başladı”, 12.10.2021, <https://www.btk.gov.tr/haberler/ulusal-siber-kalkan-2021-tatbikati-basladi> (31.12.2024).
- BTK, “Ulusal Siber Kalkan 2022 Başladı”, 11.10.2022, <https://www.btk.gov.tr/haberler/siber-kalkan-2022-basladi> (31.12.2024).
- CCDCOE, “About Us”, <https://ccdcoe.org/about-us/> (31.12.2024).
- CCDCOE, “North Atlantic Treaty Organisation”, <https://ccdcoe.org/organisations/nato/> (31.12.2024).
- CCDCOE, “Sovereignty”, <https://cyberlaw.ccdcoe.org/wiki/Sovereignty> (31.12.2024).
- CCDCOE, “The Tallinn Manual”, <https://ccdcoe.org/research/tallinn-manual/> (31.12.2024).
- Centre National de la Recherche Scientifique, Chemise 483, Carton 36, http://www.ampere.cnrs.fr/ice/ice_book_detail.php?lang=fr&type=img&bdd=koyre_ampere&table=ampere_mats&bookId=483&typeofbookId=1&num=0&&nump=204 (31.12.2024).
- Cerf, Vint, “IETF and the Internet Society”, Internet Society, 18.07.1995, <https://www.internetsociety.org/internet/history-of-the-internet/ietf-internet-society/> (31.12.2024).

- Cerf, Vinton G., “Keep the Internet Open”, The New York Times, 24.05.2012, <https://www.nytimes.com/2012/05/25/opinion/keep-the-internet-open.html> (31.12.2024).
- CERN, “Tim Berners-Lee's Proposal”, <http://info.cern.ch/Proposal.html> (31.12.2024).
- Chee, Foo Yun ve Benoit Van Overstraeten, “Google's \$2.7 Bln EU Antitrust Fine Should be Upheld, Court Adviser Says”, Reuters, 12.01.2024, <https://www.reuters.com/technology/eu-court-should-back-googles-27-bln-eu-antitrust-fine-court-adviser-says-2024-01-11/> (31.12.2024).
- China Daily, “SCO Heads of State Council Meets in Yekaterinburg”, 20.07.2009, https://www.chinadaily.com.cn/china/peacemission2009/2009-07/20/content_8449520.htm (31.12.2024).
- China/Ministry of Foreign Affairs, “Joint Communiqué of Meeting of the Council of the Heads of the Member States of the Shanghai Cooperation Organisation”, 17.06.2009, https://www.fmprc.gov.cn/eng/wjdt_665385/2649_665393/200907/t20090710_679273.html (31.12.2024).
- China/Ministry of Foreign Affairs, “Yekaterinburg Declaration of the Heads of the Member States of the Shanghai Cooperation Organisation”, 17.06.2009, https://www.mfa.gov.cn/mfa_eng/wjdt_665385/2649_665393/200906/t20090626_679272.html (31.12.2024).
- COE, “Chart of Signatures and Ratifications of Treaty 185”, <https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treatyNum=185> (31.12.2024).
- COE, “Reservations and Declarations for Treaty No.185 – Convention on Cybercrime (ETS No. 185)”, <https://www.coe.int/en/web/conventions/full-list?module=declarations-by-treaty&numSte=185&codeNature=0> (31.12.2024).
- Committee on Science US House of Representatives Subcommittee on Basic Research Subcommittee on Technology Hearing Charter, “The Domain Name System: Where do We Go from Here?”, 31.03.1998, https://commdocs.house.gov/committees/science/hsy090140.000/hsy090140_0_HTM (31.12.2024).
- Communications Assistance for Law Enforcement Act, <https://www.govinfo.gov/app/details/COMPS-937/> (31.12.2024).
- CORDIS, “Conclusions of Information Society and Development Conference”, <https://cordis.europa.eu/article/id/6191-conclusions-of-information-society-and-development-conference> (31.12.2024).
- Creative Commons, “Who We are”, <https://creativecommons.org/mission/> (31.12.2024).

- Cuba's Representative Office Abroad, "71 UNGA: Cuba at the Final Session of Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security", 23.06.2017, <https://misiones.cubaminrex.cu/en/un/statements/71-unga-cuba-final-session-group-governmental-experts-developments-field-information> (31.12.2024).
- Cybersecurity and Infrastructure Security Agency, "Critical Infrastructure Security and Resilience", <https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience> (31.12.2024).
- Cyberspace Administration of China, "Cyberspace Administration of China Launches the Initiative on China-Africa Jointly Building a Community with a Shared Future in Cyberspace", 25.08.2021, https://www.cac.gov.cn/2021-08/25/c_1631480920680924.htm (31.12.2024).
- Çallı, Muhammed Enes, "Starlink to comply with court orders to block X in Brazil", Anadolu Ajansı, 04.09.2024, <https://www.aa.com.tr/en/world/starlink-to-comply-with-court-orders-to-block-x-in-brazil/3320971> (31.12.2024)
- Data Guidance, "Jurisdictions, United States (USA) Federal", <https://www.dataguidance.com/jurisdictions/united-states-federal> (31.12.2024).
- Devon City Council, "Fire Beacons; Warning Signals Across the Countryside", <https://devoncc.sharepoint.com/sites/PublicDocs/Environment/Historic/Forms/AllItems.aspx?id=%2Fsites%2FPublicDocs%2FEnvironment%2FHistoric%2FSchools%2FFire%20Beacons%2Epdf&parent=%2Fsites%2FPublicDocs%2FEnvironment%2FHistoric%2FSchools&p=true&ga=1> (31.12.2024).
- Ekşi Sözlük, "PayPal Açılsın Kampanyası", [https://eksisozluk.com/paypal-acilsin-kampanyasi--7056151\(31.12.2024\)](https://eksisozluk.com/paypal-acilsin-kampanyasi--7056151(31.12.2024)).
- ENISA, "EU Cybersecurity Certification", <https://certification.enisa.europa.eu> (31.12.2024).
- EU Artificial Intelligence Act, "Up-to-date Developments and Analyses of the EU AI Act", <https://artificialintelligenceact.eu> (31.12.2024).
- Euronews ve Associated Press, "Elon Musk's X to be Reinstated in Brazil after Complying with Court", 09.10.2024, <https://www.euronews.com/next/2024/10/09/elon-musks-x-to-be-reinstated-in-brazil-after-complying-with-court> (31.12.2024).
- European Commission ve ENISA, "Cyber Resilience Act Requirements Standards Mapping, Joint Research Centre & ENISA Joint Analysis", 2024, <https://www.enisa.europa.eu/publications/cyber-resilience-act-requirements-standards-mapping> (31.12.2024).

- European Commission, “Antitrust: Commission fines Google €4.34 Billion for Illegal Practices Regarding Android Mobile Devices to Strengthen Dominance of Google's Search Engine”, 18.07.2018, https://ec.europa.eu/commission/presscorner/detail/en/IP_18_4581 (31.12.2024).
- European Commission, “One Common Charging Solution for All”, https://single-market-economy.ec.europa.eu/sectors/electrical-and-electronic-engineering-industries-eei/radio-equipment-directive-red/one-common-charging-solution-all_en (31.12.2024).
- Faulconbridge, Guy, “Developing World Leaders Show New Power at Summits”, Reuters, 16.06.2009, <https://www.reuters.com/article/idUSTRE55F02F/> (31.12.2024).
- Finley, Klint, “The Internet Finally Belongs to Everyone: ICANN might not be Perfect. But It just might be the Future”, The Wired, 03.10.2016, <https://www.wired.com/2016/10/internet-finally-belongs-everyone/> (31.12.2024).
- Finley, Klint, “The Internet Finally Belongs to Everyone: ICANN might not be Perfect. But It just might be the Future”, The Wired, 03.10.2016, <https://www.wired.com/2016/10/internet-finally-belongs-everyone/> (31.12.2024).
- Foreign & Commonwealth Office ve William Hague, “Security and Freedom in the Cyber Age – Seeking the Rules of the Road”, 04.02.2011, <https://www.gov.uk/government/speeches/security-and-freedom-in-the-cyber-age-seeking-the-rules-of-the-road> (31.12.2024).
- Free Software Foundation, “About”, <https://www.fsf.org/about> (31.12.2024).
- Greenwald, Glenn ve Ewen MacAskill, “NSA Prism Program Taps in to User Data of Apple, Google and Others”, The Guardian, 07.06.2013, <https://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data> (31.12.2024).
- Gross, Grant, “New ICANN Agreement Runs Into Criticism”, PC World, 01.10.2009, <https://www.pcworld.com/article/519864/article-5164.html> (31.12.2024).
- Hakmeh, Joyce ve Allison Peters, “A New UN Cybercrime Treaty? The Way Forward for Supporters of an Open, Free, and Secure Internet”, Council on Foreign Relations, 13.01.2020, <https://www.cfr.org/blog/new-un-cybercrime-treaty-way-forward-supporters-open-free-and-secure-internet> (31.12.2024).
- Harford, Tim, “Big Data: Are We Making a Big Mistake?”, Financial Times, 28.03.2014, <https://www.ft.com/content/21a6e7d8-b479-11e3-a09a-00144feabdc0> (31.12.2024).

Hauben, Ronda, “From the ARPANET to the Internet”, 23.06.1998, http://www.columbia.edu/~rh120/other/tcpdigest_paper.txt (31.12.2024).

<https://artificialintelligenceact.eu> (31.12.2024).

ICANN, “Articles of Incorporation of Internet Corporation for Assigned Names and Numbers”, <https://www.icann.org/resources/pages/articles-2012-02-25-en> (31.12.2024).

ICANN, “Bylaws”, <https://www.icann.org/resources/pages/governance/bylaws-en> (31.12.2024).

ICANN, “IANA Fonksiyonları: Giriş”, <https://www.icann.org/en/system/files/files/functions-basics-08apr14-tr.pdf> (31.12.2024).

ICANN, “List of Approved Dispute Resolution Service Providers”, <https://www.icann.org/resources/pages/providers-6d-2012-02-25-en> (31.12.2024).

ICANN, “USC/ICANN Transition Agreement”, 24.12.1998, <https://www.icann.org/resources/unthemed-pages/usc-icann-transition-2012-02-25-en> (31.12.2024).

ICANN, Correspondence, 02.03.2022, <https://www.icann.org/en/system/files/correspondence/marby-to-fedorov-02mar22-en.pdf> (31.12.2024).

IEEE, “History of IEEE”, <https://www.ieee.org/about/ieee-history.html> (31.12.2024).

IETF, “A Mission Statement for the IETF”, <https://www.ietf.org/rfc/rfc3935.txt> (31.12.2024).

IETF, “Common Requirements for Carrier-Grade NATs (CGNs)”, RFC 6888, 2013, <https://datatracker.ietf.org/doc/html/rfc6888> (31.12.2024).

IETF, “Structure of the IETF”, https://www.ietf.org/media/documents/IETF_Structure_-_February_2022.png (31.12.2024).

Instagram, “Kolluk Kuvvetlerine Yönelik Bilgiler”, <https://help.instagram.com/494561080557017> (31.12.2024).

International Association of Internet Hotlines Providers (INHOPE), <https://www.inhope.org> (31.12.2024).

Internet Watch Foundation, “About Us”, <https://www.iwf.org.uk/about-us/> (31.12.2024).

- INTERPOL, “International Child Sexual Exploitation Database”, <https://www.interpol.int/Crimes/Crimes-against-children/International-Child-Sexual-Exploitation-database> (31.12.2024).
- ITU, “Constitution and Convention”, <http://handle.itu.int/11.1004/020.2000/s.020> (31.12.2024).
- ITU, “Facts and Figures 2023”, <https://www.itu.int/itu-d/reports/statistics/2023/10/10/ff23-internet-use/> (31.12.2024).
- ITU, “Overview of ITU's History (3)”, <https://www.itu.int/en/history/Pages/ITUHistory-page-3.aspx> (31.12.2024).
- ITU, “Publications”, <https://www.itu.int/hub/pubs> (31.12.2024).
- ITU, “WCIT-12 Signatories of the Final Acts”, <https://www.itu.int/osg/wcit-12/highlights/signatories.html> (31.12.2024).
- ITU, “World Conference on International Telecommunications (WCIT-12)”, <https://www.itu.int/en/wcit-12> (31.12.2024).
- ITU, “World Telecommunication Development Conferences”, <https://www.itu.int/en/ITU-D/Conferences/WTDC> (31.12.2024).
- ITU/ITU-D, “Cyber Shield 2019”, <https://www.itu.int/en/ITU-D/Regional-Presence/Europe/Pages/Events/2019/CyberShield/Cyber-Shield-2019.aspx> (31.12.2024).
- ITU/ITU-D, “International Cyber Shield Exercise 2014, 15 – 16 May 2014, Istanbul, Turkey”, <https://www.itu.int/en/ITU-D/Regional-Presence/Europe/Pages/International-Cyber-Shield-Exercise.aspx> (31.12.2024).
- Kabar, “Duşanbe’deki BDT Devlet Başkanları Zirvesinde 12 Anlaşma İmzalandı”, 28.09.2018, <https://tr.kabar.kg/news/du-anbedeki-bdt-devlet-ba-kanlar-zirvesinde-12-belge-imzaland/> (31.12.2024).
- Kapor, Mitchell ve John Perry Barlow, “Across the Electronic Frontier”, 10.07.1990, <https://www.eff.org/tr/pages/across-electronic-frontier> (31.12.2024).
- Lambrecht, Anja ve Catherine Tucker, “The 4 Mistakes Most Managers Make with Analytics”, Harvard Business Review, 12.07.2016, <https://hbr.org/2016/07/the-4-mistakes-most-managers-make-with-analytics> (31.12.2024).
- Lederman, Josh, “Intelligence Chief Blasts NSA Leaks, Declassifies some Details about Phone Program Limits”, Associated Press, 06.06.2013, <https://web.archive.org/web/20151222130621/http://news.yahoo.com/intelligence-chief-blasts-nsa-leaks-declassifies-details-phone-025804881.html> (31.12.2024).

- Lillemose, Jacob ve Mathias Kryger, “The (Re)invention of Cyberspace, Kunstkritikk”, 24.08.2015, <https://kunstkritikk.com/the-reinvention-of-cyberspace/> (31.12.2024).
- Macron, Emmanuel, “IGF 2018 Speech”, IGF, 12.11.2018, <https://www.intgovforum.org/en/content/igf-2018-speech-by-french-president-emmanuel-macron> (31.12.2024).
- Maheshwari, Sapna, David McCabe ve Annie Karni, “House Passes Bill to Force TikTok Sale From Chinese Owner or Ban the App”, The New York Times, 13.03.2024, <https://www.nytimes.com/2024/03/13/technology/tiktok-ban-house-vote.html> (31.12.2024).
- McCarthy, Kieren, “Bush Administration Annexes Internet: Extraordinary Statement”, The Register, 01.06.2005, https://www.theregister.com/2005/07/01/bush_net_policy/ (31.12.2024).
- Merkel, Angela, “Opening Speech the 14th Annual Meeting of the Internet Governance Forum in Berlin”, Bundesregierung, 26.11.2019, <https://www.bundesregierung.de/breg-en/service/archive/speech-by-federal-chancellor-dr-angela-merkel-opening-the-14th-annual-meeting-of-the-internet-governance-forum-in-berlin-on-26-november-2019-1701494> (31.12.2024).
- Moyle, J. B. (Çev.), “The Institutes of Justinian, Fifth Edition, 1913”, Gutenberg, <https://www.gutenberg.org/files/5983/5983-h/5983-h.htm> (31.12.2024).
- Mueller, Milton, “ICANN's New MoU: Old Wine in a New Bottle”, Internet Governance, 30.09.2006, <https://www.internetgovernance.org/2006/09/30/icanns-new-mou-old-wine-in-a-new-bottle/> (31.12.2024).
- National Computer Incident Response and Coordination Center, <https://cert.gov.ru/en/> (31.12.2024).
- National Informatics Centre, “Rules and Procedures-Central”, <https://eprocure.gov.in/cppp/rulesandprocs> (31.12.2024).
- NATO, “Prague Summit Declaration”, 21.11.2002, https://www.nato.int/cps/en/natohq/official_texts_19552.htm (31.12.2024).
- NATO, “Warsaw Summit Communiqué”, 09.07.2016, https://www.nato.int/cps/en/natohq/official_texts_133169.htm (31.12.2024).
- NJ, “How Many Websites Are There in the World?”, Sitefy, 04.10.2024 <https://sitefy.com/how-many-websites-are-there> (31.12.2024).
- Nojeim, Greg, “FISA Court Opinion Outlines FBI Abuse of Key Intelligence Surveillance Authority”, Center for Democracy & Technology, 04.09.2020, <https://cdt.org/insights/fisa-court-opinion-outlines-fbi-abuse-of-key-intelligence-surveillance-authority/> (31.12.2024).

- NSF, “A Brief History of NSF and the Internet”, https://www.nsf.gov/news/news_summ.jsp?cntn_id=103050 (31.12.2024).
- Oğuztüzün, Halit, “Berimsel bir Deneme”, https://users.metu.edu.tr/bozsahin/berimsel_bir_deneme-ho.html (31.12.2024).
- Open Letter to UN General Assembly: Proposed International Convention on Cybercrime Poses a Threat to Human Rights Online, https://www.apc.org/sites/default/files/Open_letter_re_UNGA_cybercrime_resolution_0.pdf (31.12.2024).
- Paik, Amy ve Jennifer Counter, “International Law Doesn’t Adequately Protect Undersea Cables: That Must Change”, Atlantic Council, 25.01.2024, <https://www.atlanticcouncil.org/content-series/hybrid-warfare-project/international-law-doesnt-adequately-protect-undersea-cables-that-must-change/> (31.12.2024).
- Pelt, Mason, “‘Big Data’ is an Overused Buzzword and This Twitter Bot Proves It”, SiliconANGLE, 26.10.2015, <https://siliconangle.com/2015/10/26/big-data-is-an-over-used-buzzword-and-this-twitter-bot-proves-it/> (31.12.2024).
- ProCompliance, “PayPal ve KVKK Değişikliği – PayPal Türkiye’ye Geri Dönüyor (Mu?)”, 15.03.2024, <https://www.procompliance.net/paypal-ve-kvkk-degisikligi-paypal-turkiyeye-geri-donuyor-mu/> (31.12.2024).
- Randers, Katie, “Fact-checking John Oliver's Interview with Edward Snowden about NSA Surveillance”, Politifact, 09.04.2015, <https://www.politifact.com/factchecks/2015/apr/09/edward-snowden/fact-checking-john-olivers-interview-edward-snowde/> (31.12.2024).
- Reddit, r/Turkey, “Paypalın Yasaklı Olması Kadar Saçma Bir Şey Yok”, https://www.reddit.com/r/Turkey/comments/pbf0v7/paypalın_yasaklı_olması_kadar_saçma_bir_şey_yok/ (31.12.2024).
- Richter, Andrei, “Sovereign Internet Law Adopted”, IRIS Merlin, 01.06.2019, <https://merlin.obs.coe.int/article/8603> (31.12.2024).
- Root Server Technical Operations Association, <https://root-servers.org> (31.12.2024).
- Schmitt, Michael ve Liis Vihul, “International Cyber Law Politicized: The UN GGE’s Failure to Advance Cyber Norms”, Just Security, 30.06.2017, <https://www.justsecurity.org/42768/international-cyber-law-politicized-gges-failure-advance-cyber-norms/> (31.12.2024).
- Schmitt, Michael, “Canada Takes on International Law in Cyberspace”, EJIL:Talk!, 14.07.2022, <https://www.ejiltalk.org/canada-takes-on-international-law-in-cyberspace/> (31.12.2024).

- Siber Vatan, “Kalkınma Ajansları Siber Vatan Programı”, <https://www.sibervatan.org/kalkinma-ajanslari-sibervatan-programi> (31.12.2024).
- Siteefy, “How Many Websites Are There in the World?”, 04.10.2024, <https://siteefy.com/how-many-websites-are-there> (31.12.2024).
- Sputnik Türkiye, “Kılıçdaroğlu: İktidara Gelir Gelmez PayPal Yasasını Kaldıracağız”, 13.10.2022, <https://anlatilaninotesi.com.tr/20221013/kilicdaroglu-iktidara-gelir-gelmez-paypal-yasagini-kaldiracagiz-1062286099.html> (31.12.2024).
- Starlink, <https://www.starlink.com> (31.12.2024).
- Şeker, Ata Ufuk, “Avrupa Parlamentosu ‘Yapay Zeka Yasası’nı onayladı”, Anadolu Ajansı, 13.03.2024, <https://www.aa.com.tr/tr/dunya/avrupa-parlamentosu-yapay-zeka-yasasini-onayladi/3163480> (31.12.2024).
- T. C. Cumhurbaşkanlığı, “Özgün Teknolojilerimizi, Yazılımlarımızı Geliştirmeden Geleceğimize Güvenle Bakamayız”, 21.03.2022, <https://www.tccb.gov.tr/haberler/410/136171/-ozgun-teknolojilerimizi-yazilimlarimizi-gelistirmeden-gelecegimize-guvenle-bakamayiz-> (31.12.2024).
- T.C. Adalet Bakanlığı Dış İlişkiler ve Avrupa Birliği Genel Müdürlüğü, “İnternet Ortamında İşlenen Suçlarda Uluslararası Ceza İstinabe İşlemleri”, <https://diabgm.adalet.gov.tr/Home/SayfaDetay/internet-ortaminda-islenen-suclarda-uluslararasi-ceza-istinabe-islemleri14022020041756> (31.12.2024).
- T.C. Cumhurbaşkanlığı Dijital Dönüşüm Ofisi, “Kamu Bulut Bilişim Stratejisi”, <https://cbddo.gov.tr/bulut-bilisim-stratejisi/> (31.12.2024).
- T.C. Cumhurbaşkanlığı Dijital Dönüşüm Ofisi, “Siber Güvenlik Dairesi Başkanlığı”, <https://cbddo.gov.tr/hizmet-birimlerimiz/siber-guvenlik-dairesi-baskanligi/> (31.12.2024).
- T.C. Cumhurbaşkanlığı İletişim Başkanlığı, “Siber Vatan Koruyucuları Sertifikalarını Aldı”, 30.07.2024, https://www.iletisim.gov.tr/turkce/yerel_basin/detay/siber-vatan-koruyuculari-sertifikalarini-aldi (31.12.2024).
- T.C. Cumhurbaşkanlığı, “Türkiye’yi, Bilgi ve İletişim Teknolojilerinde Dünyanın En Önde Gelen Ülkeleri Arasına Sokacağız”, 10.02.2020, <https://www.tccb.gov.tr/haberler/410/116592/-turkiye-yi-bilgi-ve-iletisim-teknolojilerinde-dunyanin-en-onde-gelen-ulkeleri-arasina-sokacagiz-> (31.12.2024).
- T.C. Merkez Bankası, “Elektronik Fon Transfer Sistemi – Elektronik Menkul Kıymet Transfer Sistemi – Fonların Anlık ve Sürekli Transferi (FAST) Sistemi”, <https://www.tcmb.gov.tr/wps/wcm/connect/TR/TCMB+TR/Main+Menu/Teme1+Faaliyetler/Odeme+Sistemleri/Turkiyedeki+Odeme+Sistemleri/Elektronik+Fon+Transfer+%28EFT%29+Sistemi> (31.12.2024).

- T.C. Tallin Büyükelçiliği, <https://tallin-be.mfa.gov.tr/Mission> (31.12.2024).
- T.C. Ulaştırma ve Altyapı Bakanlığı Haberleşme Genel Müdürlüğü, “Siber Güvenlik”, <https://hgm.uab.gov.tr/siber-guvenlik> (31.12.2024).
- The Community Research and Development Information Service (CORDIS), “Information Society and Development”, <https://cordis.europa.eu/event/id/5905-information-society-and-development> (31.12.2024).
- The European Cyber Resilience Act (CRA), <https://www.european-cyber-resilience-act.com> (31.12.2024).
- The Internet Map, <http://internet-map.net>, (31.12.2024).
- The PirateBay, <https://thepiratebay.org> (31.12.2024).
- The Shanghai Cooperation Organisation, “Documents, 2009”, <https://eng.sectesco.org/documents/?year=2009> (31.12.2024).
- TR Ağ Bilgi Sistemi, <https://www.trabis.gov.tr> (31.12.2024).
- Tribe, Laurence H., “The Constitution in Cyberspace: Law and Liberty Beyond the Electronic Frontier”, Electronic Privacy Information Center, 1991, https://archive.epic.org/free_speech/tribe.html (31.12.2024).
- TRT Haber, “Cumhurbaşkanı Erdoğan'dan 'Siber Vatan' Mesajı”, 15.01.2021, <https://www.trthaber.com/haber/gundem/cumhurbaskani-erdogandan-siber-vatan-mesaji-547553.html> (31.12.2024).
- TRT Haber, “Sosyal Medya Platformu X, Türkiye’de Temsilcilik Açtı”, 22.05.2024, <https://www.trthaber.com/haber/gundem/sosyal-medya-platformu-x-turkiyede-temsilcilik-acti-859255.html> (31.12.2024).
- Tutak, Serhan, “Bakan Uraloğlu, Instagram'a Getirilen Erişim Engeline İlişkin Son Durumu Değerlendirdi”, Anadolu Ajansı, 06.08.2024, <https://www.aa.com.tr/tr/bilim-teknoloji/bakan-uraloglu-instagram-a-getirilen-erisim-engeline-iliskin-son-durumu-degerlendirdi/3296674> (31.12.2024).
- Türkiye Katılım Bankaları Birliği, “Katılım Bankacılığı Dijital Araştırma Raporu 2021”, <https://tkbb.org.tr/faaliyetler/yayinlar/dijital-arastirma-raporu> (31.12.2024).
- U.S. Department of Justice / Office of Public Affairs, “U.S. Charges Five Chinese Military Hackers for Cyber Espionage Against U.S. Corporations and a Labor Organization for Commercial Advantage”, 19.05.2014, <https://www.justice.gov/opa/pr/us-charges-five-chinese-military-hackers-cyber-espionage-against-us-corporations-and-labor> (31.12.2024).

- U.S. Department of State, Bureau of Cyberspace and Digital Policy, “Key Topics”, <https://www.state.gov/key-topics-bureau-of-cyberspace-and-digital-policy/> (31.12.2024).
- United States Foreign Intelligence Surveillance Court, “Memorandum Opinion and Order”, 06.12.2019, https://www.intelligence.gov/assets/documents/702%20Documents/declassified/2019_702_Cert_FISC_Opinion_06Dec19_OCR.pdf (31.12.2024).
- United States House of Representatives/Judiciary Committee, “USA Freedom Act”, <https://judiciary.house.gov/usa-freedom-act> (31.12.2024).
- USOM, “İhbar”, <https://www.usom.gov.tr/ihbar> (31.12.2024).
- W3C, “Cascading Style Sheets Home Page”, <https://www.w3.org/Style/CSS> (31.12.2024).
- W3C, “Extensible Markup Language (XML)”, <https://www.w3.org/XML> (31.12.2024).
- W3C, “Our Mission”, <https://www.w3.org/mission/> (31.12.2024).
- Wu, Huizhong ve Johnson Lai, “Taiwan Suspects Chinese Ships Cut Islands’ Internet Cables”, Associated Press, 18.04.2023, <https://apnews.com/article/matsu-taiwan-internet-cables-cut-china-65f10f5f73a346fa788436366d7a7c70> (31.12.2024).
- X, “Hukuki Talep SSS”, <https://help.x.com/tr/rules-and-policies/x-legal-faqs> (31.12.2024).