İSTANBUL MEDENİYET ÜNİVERSİTESİ
LİSANSÜSTÜ EĞİTİM ENSTİTÜSÜ
ULUSLARARASI İLİŞKİLER ANABİLİM DALI

Küresel Dijital Yönetişim Sorunu: Siber Hukuk Bağlamında İnternet Yönetişimi Forumu (IGF) Örneği

Doktora Tezi

Sevda KORHAN

Mayıs 2024

İSTANBUL MEDENİYET ÜNİVERSİTESİ
LİSANSÜSTÜ EĞİTİM ENSTİTÜSÜ
ULUSLARARASI İLİŞKİLER ANABİLİM DALI

Küresel Dijital Yönetişim Sorunu: Siber Hukuk Bağlamında İnternet Yönetişimi Forumu (IGF) Örneği

Doktora Tezi

Sevda KORHAN

Danışman

Prof. Dr. İsmail ERMAĞAN

Mayıs 2024

TEZ JÜRİSİ ONAYI

Sevda KORHAN tarafından hazırlanan "Küresel Dijital Yönetişim Sorunu: Siber Hukuk Bağlamında İnternet Yönetişimi Forumu (IGF) Örneği" başlıklı bu Doktora Tezi, Uluslararası İlişkiler Anabilim Dalı'nda hazırlanmış ve jürimiz tarafından kabul edilmiştir.

JÜRİ ÜYELERİ **İMZA**

Tez Danışmanı:

Prof. Dr. İsmail ERMAĞAN

İstanbul Medeniyet Üniversitesi

Üyeler:

Doç. Dr. Fatih BAYRAM

İstanbul Medeniyet Üniversitesi

Doç. Dr. Murat TUMAY

İstanbul Medeniyet Üniversitesi

Prof. Dr. Nezir AKYEŞİLMEN

Selçuk Üniversitesi

Prof. Dr. Aşkın İnci SÖKMEN ALACA

İstanbul Arel Üniversitesi

Tez Savunma Tarihi: 07/05/2024

BEYANLAR

Yazım ve Kaynak Gösterme Kılavuzu Beyanı

Danışmanlığımda yazılan bu tezin APA yazım ve kaynak gösterme kılavuzunda belirtilen kurallara uygun olarak yapılandırıldığı ve bu kılavuzun metin içi kaynak gösterme standartlarının bu tezde tutarlı olarak uygulandığı tarafımdan incelenerek teyit edilmiştir.

İmza

Prof. Dr. İsmail ERMAĞAN

Etik İlkelere Sadakat Beyanı

Hazırladığım bu tezin tamamen kendi çalışmam olduğunu, akademik ve etik kuralları gözeterek çalıştığımı ve her alıntıya kaynak gösterdiğimi beyan ederim.

İmza

Sevda KORHAN

ÖZET

Küresel Dijital Yönetişim Sorunu: Siber Hukuk Bağlamında İnternet Yönetişimi Forumu (IGF) Örneği

Korhan, Sevda

Doktora Tezi, Uluslararası İlişkiler Anabilim Dalı

Danışman: Prof. Dr. İsmail ERMAĞAN

Mayıs 2024

Bu tez, küresel internet yönetişimi sorununa odaklanarak, bu alandaki mevcut zorlukları ve potansiyel çözüm yollarını incelemektedir. Temel argüman, küresel bir internet yönetişimi sorununun varlığı ve bu sorunun etkin bir hukuk mekanizmasının eksikliği de dahil olmak üzere, birden fazla sorun alanından kaynaklandığı yönündedir. Bu çerçevede, çoklu sorun alanları arasında hukuk, önemli bir bileşen olarak kabul edilirken, tez aynı zamanda teknik, politik ve sosyal boyutları da kapsamlı bir şekilde inceleyecektir. Mevcut literatürde bu sorunların yönetilemezliği üzerine bir konsensüs olsa da, iyi yönetişim ilkelerinin ve normatif unsurların uygulanmasıyla bu sorunların üstesinden gelinebileceği varsayımından yola çıkılmıştır. Bu bağlamda tez, siber uzayın özgün doğasının getirdiği zorluklar karşısında etkin bir yönetişim ve hukuk mekanizmasının mümkün olup olamayacağını değerlendirir. Bu değerlendirme yapılırken, mevcut uluslararası hukuk sisteminin bu yeni ve kaotik ortama adapte olup olamayacağı sorusu da gündeme gelmektedir. Bu bağlamda bu tez, siber uzayın dinamizmiyle uyumlu bir uluslararası siber hukuk modelinin, etkili bir küresel internet yönetişimi için temel bir gereklilik olduğunu öne sürmektedir. Tezde, İnternet Yönetişimi Forumu (IGF) modeli, küresel internet yönetişimi için uygun bir örnek olarak kabul edilmiştir. Ancak IGF, çok paydaşlı yapısı ve kapsayıcı yaklaşımı ile dikkat çekmekte iken; hukuki bağlayıcılığa sahip olmaması -özellikle etkili kararlar alma noktasında- potansiyelini zayıflatmaktadır. Bu noktada tez, normatif teoriyi küresel internet yönetişimi konusunda bir rehber olarak kullanarak, IGF modelinin mevcut sınırlılıklarını aşmaya odaklanmaktadır. Bu doğrultuda tez, IGF'nin daha etkili bir karar alma mekanizmasına sahip olabilmesi için, hukuki bağlayıcılık önerisinde bulunmaktadır. Bu çerçevede geliştirilen normatif ve hukuki çözüm önerileri, hukuki sınırlılıklar dahilinde yapılırken, modelin çok paydaşlı yapısının korunmasına da özen gösterilmiştir.

Anahtar Kelimeler: İnternet Yönetişimi, Siber Hukuk, IGF, İyi Yönetişim, Normatif Teori

ABSTRACT

The Problem of Global Digital Governance: The Case of the Internet Governance Forum (IGF) in the Context of Cyberlaw

Korhan, Sevda

Ph.D. Thesis, Department of International Relations

Supervisor: Prof. Dr. İsmail ERMAĞAN

May 2024

This thesis focuses on the global internet governance challenge and examines the existing challenges and potential solutions in this area. The main argument is that there is a global internet governance problem and that this problem stems from multiple problem areas, including the lack of an effective legal mechanism. In this framework, while law is recognized as an important component among the multiple problem areas, the thesis will also comprehensively examine the technical, political and social dimensions. While there is a consensus in the existing literature on the unmanageability of these problems, the thesis starts from the assumption that these problems can be overcome through the application of good governance principles and normative elements. In this context, the thesis assesses whether an effective governance and legal mechanism is possible in the face of the challenges posed by the unique nature of cyberspace. This assessment raises the question of whether the existing international legal system can adapt to this new and chaotic environment. In this context, this thesis argues that a model of international cyber law that is compatible with the dynamism of cyberspace is a fundamental requirement for effective global internet governance. In this thesis, the Internet Governance Forum (IGF) model is recognized as an appropriate model for global internet governance. However, while the IGF is noteworthy for its multi-stakeholder structure and inclusive approach, its lack of legally binding nature weakens its potential, especially in terms of effective decision-making. This thesis focuses on overcoming the current limitations of the IGF model by using normative theory as a guide to global internet governance. To this end, the thesis proposes a legally binding mechanism for the IGF to have a more effective decision-making mechanism. While the normative and legal solutions developed in this framework are made within legal limitations, care has been taken to preserve the multi-stakeholder structure of the model.

Keywords: Internet Governance, Cyberlaw, IGF, Good Governance, Normative Theory

ÖNSÖZ

Çalışma boyunca kendisinden sayısız bilgiler edindiğim, önerileriyle tezime büyük katkılar sağlayan kıymetli danışmanım Prof. Dr. İsmail Ermağan'a teşekkürlerimi sunarım. Bana duyduğu güveni her daim dile getirerek beni desteklediği, zorlaştırıcı değil kolaylaştırıcı bir danışman olmayı seçtiği için kendisine minnettarım.

Değerli görüş ve önerileriyle tezime katkıda bulunan jüri üyelerim Doç. Dr. Fatih Bayram, Prof. Dr. Aşkın İnci Sökmen Alaca ve Doç. Dr. Murat Tumay'a ayrıca teşekkürlerimi sunarım.

Tez izleme komite üyem ve kıymetli hocam Prof. Dr. Nezir Akyeşilmen'e özel bir parantez açmak istiyorum. Lisans hayatımdan bu yana hiçbir koşulda desteğini benden esirgemediği, hayatımın her alanında beni yönlendirdiği, teşvik ettiği ve onurlandırdığı için kendisine teşekkürü ve minneti borç bilirim. Hayatıma kattığı değer ve güzelliklerden dolayı sonsuz teşekkürler.

Tezimi yazdığım süre boyunca üzerimden aldığı yükle beni hafiften değerli çalışma arkadaşım Cemil Yardım'a ve anlayışıyla bana çalışma alanı açan değerli hocam Doç. Dr. Yusuf Çınar'a teşekkür ederim.

En büyük teşekkürü, sahip olduğum için her gün şükrettiğim kocaman aileme etmek istiyorum. Beni sevgiyle büyüttükleri için canım annem Vesile Korhan ve canım babam Abdulvahap Korhan'a; bana arkama tüm dünyayı almış kadar güçlü hissettiren abilerim Dr. İbrahim Korhan ve Vecdi Korhan'a ve ablalarım Fidan Güler, Selma Korhan ve Mehtap Akkaya'ya; bana küçük yaşımdan itibaren sorumluluk deneyimini yaşatarak daha güçlü kılan kardeşlerim Murat Korhan, Merve İnan ve Halil Korhan'a binlerce kez teşekkürler.

Son olarak; sevgisi, saygısı, desteği ve bütün sabrıyla yanımda olan İdris Barış'a sonsuz sevgiler ve teşekkürler…

Sevda KORHAN

İstanbul, 2024

İÇİNDEKİLER

TEZ JÜRİSİ ONAYI ..... **i**
BEYANLAR ..... **ii**
ÖZET ..... **iii**
ABSTRACT ..... **iv**
ÖNSÖZ ..... **v**
İÇİNDEKİLER ..... **vi**
KISALTMALAR ..... **ix**
TABLOLAR LİSTESİ ..... **xii**
GRAFİKLER LİSTESİ ..... **xiii**
GİRİŞ **1**
BÖLÜM I: KAVRAMSAL VE KURAMSAL ÇERÇEVE: TANIM, YAKLAŞIMLAR, UNSURLAR, TEORİLER **24**
1.1. Yönetişimi Anlamak: Tarihsel Arka Plan ve Kavramsal Analiz **24**
1.1.1. Yönetişim ve Ortaya Çıkışı 24
1.1.2. Yönetişimin Küreselleşmesi: Küresel Yönetişim 29
1.1.3. Küresel İyi Yönetişim 32
1.2. Küresel Dijital Yönetişim **35**
1.2.1. İnternet ve Ortaya Çıkışı 35
1.2.2. İnternetin Küreselleşmesi: İlk Yönetişim Tartışmaları 37
1.2.3. Küresel İnternet Yönetişimi Tanımı 39
1.2.3.1. Genel Tanım 39
1.2.3.2. Paydaş Odaklı Tanım 43
1.2.3.3. İyi Yönetişim Bağlamında Tanım 50
1.2.4. Dijital Yönetişim Yaklaşımları 52
1.2.4.1. Teknik Yaklaşım 53
1.2.4.2. Politik Yaklaşım 55
1.2.5. Yönetişim Tartışmalarının Uluslararasılaşması 58
1.2.5.1. Uluslararası Konferans ve Zirveler 58
1.2.6. "Kaynak" Yönetişiminden "Tehdit" Yönetişimine Evrim 62
1.2.7. Dijital Yönetişimin Aktörleri **64**
1.2.7.1. Devletler 68
1.2.7.2. Hükümetlerarası Kuruluşlar 71
1.2.7.3. Uluslararası Standardizasyon Kuruluşları 73
1.2.7.4. Özel Sektör 86
1.2.7.5. Sivil Toplum 91
1.2.7.6. Bireyler/Kullanıcılar 95
1.3. Kuramsal Çerçeve: Normatif Bakış Açısını Kuramsallaştırma **97**
1.3.1. Realizm: Güç, Güvenlik ve Çıkar Odaklı Dijital Yönetişim 100
1.3.2. Liberalizm: Özgürlükçü Yaklaşımlar 106
1.3.3. İnşacılık: Dijital Yönetişim İnşa Edilebilir Mi? 109
1.3.4. Eleştirel Bir Teori: Normatif Teori 112

1.3.4.1. Norm 114
1.3.4.2. Düzen 116
1.3.4.3. Hukuk 119
1.3.4.4. Adalet 121
BÖLÜM II: BİR SORUN OLARAK KÜRESEL DİJİTAL YÖNETİŞİM 127
2.1. Sorun Alanlarının Belirlenmesi 127
2.1.1. Teknik Sorun Alanları 129
2.1.1.1. TCP/IP 129
2.1.1.2. DNS 132
2.1.1.3. Kök Bölge 134
2.1.1.4. World Wide Web 137
2.1.1.5. Blok Zinciri (Blokchain) 139
2.1.1.6. Yükselen Sorunlar 142
2.1.2. Politik Sorun Alanları 145
2.1.2.1. Güvenlik Sorunları 145
2.1.2.2. İnsan Hakları Sorunları 156
2.1.3. Diğer Sosyo-Politik Sorunlar 171
2.2. Soyut Tartışma: Siber Uzay Yönetilebilir Mi? 177
2.2.1. Siber Uzayda Yönetişimi Zorlaştıran Unsurlar 179
2.2.1.1. Siber Uzayın Doğası 180
2.2.1.2. Aktör Çeşitliliği 184
2.2.1.3. Teknik Bakış Açısı 187
2.2.1.4. İş Birliği/Çıkar İkilemi 189
2.2.2. Siber İyi Yönetişim Mümkün Mü? 193
BÖLÜM III: SİBER HUKUK BAĞLAMINDA DİJİTAL YÖNETİŞİM 205
3.1. Yükselen Bir Disiplin Olarak Siber Hukuk 205
3.1.1. Kavramsal Sorunsal: Siber Hukuk 208
3.1.2. Siber Hukukun ve Normların Yükselişi 210
3.1.2.1. Küresel Mekanizmalar 210
3.1.2.2. Bölgesel Mekanizmalar 214
3.2. Siber Uzayın Uluslararası Hukuk Bağlamında Değerlendirilmesi 216
3.2.1. Siber Savaş ve Çatışmalar 220
3.2.2. Siber İstihbarat 225
3.2.3. Siber Suçlar 228
3.3. Siber Hukuka Yönelik Yaklaşımlar 230
3.3.1. Uluslararası Hukuk Yaklaşımı 231
3.3.2. Ulusal Hukuk Yaklaşımı 234
3.3.3. Öz-Düzenleme Yaklaşımı 237
3.3.4. Uluslararası Siber Hukuk Yaklaşımı 240
3.4. Uluslararası Siber Hukuk Mümkün Mü? 243
3.4.1. Zorluklar 245
3.4.2. Zorunluluklar 247
3.4.3. Paydaşların Perspektifleri 250
3.4.4. Olasılıklar 253

BÖLÜM IV: YÖNETİŞİM MODELLERİ 263
4.1. İnternet Yönetişimi Modelleri 263
4.1.1. Öz-Yönetim Modeli 266
4.1.2. Ulusal (*Domestic*) Model 269
4.1.3. Çok Paydaşlılık (*Multistakeholder*) Modeli 272
4.1.3.1. Özgürlükçü Yaklaşımlar 275
4.1.3.2. ICANN'in Rolü 277
4.1.3.3. Sorun Alanları 280
4.1.4. Çok Taraflılık (*Multilateral*) Modeli 284
4.1.4.1. Egemenlikçi Yaklaşımlar 286
4.1.4.2. ITU'nun Rolü 288
4.1.5. Alternatif Yaklaşımlar: Rejim Kompleksi Modeli 290
4.2. Önerilen Model: IGF Modeli 293
4.2.1. İnternet Yönetişimi Forumu 293
4.2.1.1. Yapısı 294
4.2.1.2. İşlevleri 296
4.2.1.3. Katkıları 299
4.2.1.4. Toplantıları 303
4.2.2. İnternet Yönetişimi Forumu'nun Sorun Alanları 307
4.2.2.1. Yapısal Sorunlar 307
4.2.2.2. Paydaş Sorunları 309
4.2.3. IGF'ye Hukuki Bağlayıcılık Kazandırılabilir Mi? 315
4.2.3.1. Hukuki Bağlayıcılık: Bir Sorun Mu? 315
4.2.3.2. Hukuki Olasılıklar 321
4.2.3.3. Hukuki ve Normatif Çözüm Önerileri 324
SONUÇ 336
KAYNAKÇA 346

KISALTMALAR

AB	Avrupa Birliği
ABD	Amerika Birleşik Devletleri
AGİT	Avrupa Güvenlik ve İşbirliği Teşkilatı
AI	Yapay Zekâ
AİHM	Avrupa İnsan Hakları Mahkemesi
ALAC	At-Large Danışma Komitesi
APC	Aşamalı İletişim Derneği
ARPA	ABD Savunma Bakanlığı İleri Araştırma Projeleri Ajansı
ARPANET	İleri Araştırma Projeleri Ajansı Ağı
ASEAN	Güneydoğu Asya Uluslar Birliği
ASO	Adres Destekleme Kuruluşu
BİT	Bilgi ve İletişim Teknolojileri
BM	Birleşmiş Milletler
BPF'ler	En İyi Uygulama Forumları
BRICS	Brezilya, Rusya, Hindistan, Çin ve Güney Afrika Cumhuriyeti
ccNSO	Ülke Kodu Adlarını Destekleme Kuruluşu
ccTLD	İnternet Ülke Üst Seviye Alan Adı
CERN	Avrupa Nükleer Araştırma Merkezi
CIR	Kritik İnternet Kaynakları
CISA	Siber Güvenlik ve Altyapı Güvenliği Ajansı
CSB	Sivil Toplum Bürosu
CSCG	Sivil Toplum Koordinasyon Grubu
CSTD	BM Kalkınma için Bilim ve Teknoloji Komisyonu
DNS	Alan Adı Sistemi
DRM	Dijital Haklar Yönetimi
ERCIM	Avrupa Bilişim ve Matematik Araştırma Konsorsiyumu
EuroDIG	İnternet Yönetişiminde Avrupa Diyaloğu
GAC	Devlet Danışma Komitesi
GAIA	Herkes için İnternete Küresel Erişim Araştırma Grubu
GNSO	Genel Adları Destekleme Kuruluşu

gTLD	Genel Üst Seviye Alan Adı
HLSOC	Yüksek Düzeyli Zirve Organizasyon Komitesi
HRPC	İnsan Hakları Protokolü Hususları Araştırma Grubu
HTML	HyperText Markup Language
IAB	İnternet Mimarisi Kurulu
IANA	İnternet Atanmış Numaralar Kurumu
ICANN	İnternet Tahsisli Sayılar ve İsimler Kurumu
ICCB	İnternet Yapılandırma Kontrol Panosu
IESG	İnternet Mühendisliği Yönlendirme Grubu
IETF	İnternet Mühendisliği Görev Gücü
IGC	İnternet Yönetişim Grupları
IGF	İnternet Yönetişimi Forumu
IoT	Nesnelerin İnterneti
IRSG	İnternet Araştırma Yönlendirme Grubu
IRTF	İnternet Araştırma Görev Gücü
ISI	University of Information Sciences Institute
ISO	Uluslararası Standartlar Organizasyonu
ISOC	İnternet Topluluğu
ISS'ler	İnternet Servis Sağlayıcıları
ITR'ler	Uluslararası Telekomünikasyon Yönetmelikleri
ITU	Uluslararası Telekomünikasyon Birliği
JNC	Just Net Coalition
JPA	Ortak Proje Anlaşması
LIR	Yerel İnternet Sicili
MAG	Çok Taraflı Danışma Grubu
MIT/CSAIL	Massachusetts Teknoloji Enstitüsü Bilgisayar Bilimi ve Yapay Zekâ Laboratuvarı
MOU	Mutabakat Muhtırası
NATO	Kuzey Atlantik Antlaşması Örgütü
NCSG	Commercial Non Commercial Payolder Group
NIR	Ulusal İnternet Kayıt Defteri
NMRG	Ağ Yönetimi Araştırma Grubu
NRI'lar	Ulusal ve Bölgesel IGF Girişimleri

NRO	Sayı Kaynak Organizasyonu
NSA	Ulusal Güvenlik Ajansı
NSF	Ulusal Bilim Vakfı
NSI	Network Solutions, Inc.
NTIA	ABD Ulusal Telekomünikasyon ve Bilgi İdaresi
OECD	Ekonomik Kalkınma ve İşbirliği Örgütü
ONI	OpenNet Initiative
PDP	Politika Geliştirme Süreçleri
RALO'lar	Bölgesel At-Large Kuruluşları
RFC'ler	Requests for Comments
RIAA	Amerika Kayıt Endüstrisi Birliği
RIR	Bölgesel İnternet Kayıt Defteri
RIR'lar	Bölgesel İnternet Tescilleri
SEEDIG	İnternet Yönetişiminde Güney Doğu Avrupa Diyaloğu
SGI	Sürdürülebilir Yönetişim Göstergeleri
SSAC	Güvenlik ve İstikrar Danışma Komitesi
SSCB	Sovyet Sosyalist Cumhuriyetler Birliği
STK	Sivil Toplum Kuruluşu
ŞİÖ	Şangay İşbirliği Örgütü
TCP/IP	Transmission Control Protocol/Internet Protokol
TLD	Üst Düzey Alanları
UIP	Unmanaged Internet Protocol
Uİ	Uluslararası İlişkiler
UNCTAD	Birleşmiş Milletler Ticaret ve Kalkınma Konferansı
UNDP	Birleşmiş Milletler Kalkınma Programı
UNESCO	Birleşmiş Milletler Eğitim, Bilim ve Kültür Örgütü
URI	Tekdüzen Kaynak Tanımlayıcıları
W3C	World Wide Web Konsorsiyumu
WGIG	İnternet Yönetişimi Çalışma Grubu
WIPO	Dünya Fikri Mülkiyet Örgütü
WTO	Dünya Ticaret Örgütü
WWW	World Wide Web

TABLOLAR LİSTESİ

Tablo 1. Siber Güvenliğin Tarihsel Evrimi ve Güvenlikleştirme 151
Tablo 2. Siber Uzayın Özellikleri ve Yarattığı Sonuçlar.....181
Tablo 3. IGF'nin Yapısı.....294
Tablo 4. Yıllara Göre IGF Toplantılarının Alt Temaları 305
Tablo 5. Paydaşların Rolüne İlişkin Kuzey-Güney kutuplaşması 308
Tablo 6. IGF'nin Paydaş Sorunlarına Yönelik Zorlukların Kategorizasyonu 310

GRAFİKLER LİSTESİ

Grafik 1. Bölgelere Göre Ocak 2024 İtibariyle Küresel İnternet Erişim Oranı 174
Grafik 2. IGF 2023 Toplantısı Paydaş Gruplarına Göre Katılım Oranları.....311
Grafik 3. IGF 2023 Toplantısı Bölgelere Göre Katılım Oranları.....311

GİRİŞ

> Gelecekte büyük çatışmaların kaynağının toprak anlaşmazlıkları ya da ulusal üstünlük kaygıları değil, bilginin kontrolü ve sahiplenilmesi olacağını öngörebiliriz, zira her şeyin temelinde bu yatmaktadır: kalkınmanın, güvenliğin, savunmanın, eğitimin ve kültürün kendisinin…
>
> UNESCO, 1984.

UNESCO, bu öngörüsünü "bölgesel anlaşmazlıklar ya da ulusal üstünlükten ziyade bilginin kontrolü ve sahipliğinin büyük çatışmaların ana kaynağı olacağı, çünkü bilginin her şey olduğu fikri" üzerine kurmuştur. UNESCO bunu öngördüğünde sene 1984 idi. Takriben beş ila on yıl içinde böylesi bir durumun ortaya çıkacağını tahmin etmişti. Nitekim 1980'lerden itibaren internet, hızla popülerleşti. Bu dönemde, dijital/siber/internet yönetişim(i)[1] teknik bir mesele olarak ele alınmakta ve devletlerin doğrudan katılımıyla sınırlı kalmaktaydı. ARPANET topluluğunun liderleri, internet standartları ve politikaları üzerinde çalışacak kâr amacı gütmeyen kuruluşların kurulması için önemli adımlar attılar. 1980'lerden itibaren ise bu kuruluşlar, internetin araştırma ve geliştirme faaliyetlerinden sorumlu temel aktörler haline geldi.

1990'lara gelindiğinde ise ABD Savunma Bakanlığı, ARPANET'in araştırma kolunu ticarileştirmeye karar verdi. İnternetin ticari alandaki kullanım kısıtlamalarının kaldırılması, 1990'lı yılların başlarında internete olan ilgiyi önemli ölçüde artırdı. Bu dönüşümle birlikte internet standartlarına ek olarak, ticari anlaşmalar da düzenlemeyi etkileyen unsurlar arasına girdi. Ağın büyümesi, iş, eğitim, ekonomi ve güvenlik gibi birçok alanı internet faaliyetleriyle iç içe hale getirdi. Bunun bir sonucu olarak devletler, sivil toplum kuruluşları, düzenleyici ve teknik kurumlar ve özel sektör gibi çok sayıda aktör, alan adları ve adresleriyle ilgili konulara odaklanmaya başladı. Tam da böyle bir dönemde, bugünün literatürünü ziyadesiyle işgal edecek olan o tartışmalı kurum, İnternet Tahsisli Sayılar ve İsimler Kurumu (ICANN), internetin güvenliği ve istikrarının korunması ihtiyacına yanıt olarak oluşturuldu. 21. yüzyılın başlarında ise, internetin küresel toplum için vazgeçilmez bir kaynak haline gelmesi, Uluslararası

[1] Literatürde yaygın olarak internet yönetişimi, siber yönetişim ve dijital yönetişim şeklinde kullanılmaktadır. Çalışmada genel olarak internet yönetişimi ifadesi kullanılacaktır.

Telekomünikasyon Birliği (ITU) tarafından "Bilgi Toplumu" konulu dünya çapında zirvelerin düzenlenmesine yol açtı. Bu zirvelerin de çıktısı, çatışmaların merkezinde yer almaması gerekçesiyle literatürde yeterince önemsenmeyen IGF oldu.

Peki ya bugün? 1984'te dahi "her şey" olan bilgi bugün ne ifade ediyor? Bugün, bilgi sadece her şeyi temsil etmekle kalmıyor, aynı zamanda her yerde. Bilgi, küresel bir fenomen haline geldi, tıpkı yarattığı sorunlar gibi. Bugün, internetin kendisi gibi küresel olan bu sorunlar, sınırları aşan, uluslararası ilişkileri ve iç politikaları şekillendiren yeni bir dinamik oluşturmaktadır. Bilgiye erişim ve bilginin kontrolü üzerine kurulan güç dinamikleri, devletlerin, kurumların ve bireylerin karşı karşıya kaldığı zorluklarda merkezi bir yer tutmaya başladı. Siber güvenlikten veri mahremiyetine, dijital eşitsizliklerden internette ifade özgürlüğüne kadar pek çok konu, önemli tartışma konuları arasında yer almaktadır.

Böylesi küresel olan bir sorun alanı nasıl çözülebilir? Bu soruya yanıt, kuşkusuz küresel iyi yönetişim anlayışıdır. Tek bir devletin hakimiyetinde gelişen, dolayısıyla tek bir devletin kanunlarına tabi, genel itibariyle teknik konulara odaklanan ABD merkezli ICANN gibi kurumlar tarafından oluşturulan kısmi yönetişim modelinin eskiyip işlevselliğini yitirdiği anlaşılmalıdır. Çünkü günümüzde internet, sadece teknik bir mesele olmaktan öteye geçerek ABD'nin kullanım alanını aşmıştır. Bugün internet, devletler, uluslararası kuruluşlar, özel sektör, akademi, sivil toplum ve bireyler gibi her düzeyden aktörlerin tamamını teknik, politik, sosyal ve ekonomik olarak ilgilendiren bir ağ haline gelmiştir. Bu durum, yalnızca ulus devletlerin değil, tüm bu aktörlerin "paydaş" olarak kabul edildiği çok-paydaşlı ve kapsayıcı bir yönetişim modelinin zorunluluğunu ortaya koymaktadır.

Oluşturulacak kapsayıcı modelde, iyi yönetişim unsurlarını merkeze alan normatif bir yaklaşım modelinin benimsenmesi esastır. Fakat günümüzde internet yönetişimi sıklıkla güvenlik odaklı ve çoğunlukla negatif güvenlik anlayışlarıyla ele alınmaktadır. Bu bağlamda normatif bakış açıları, daha adil, özgür, açık ve güvenli bir siber uzayın inşası noktasında önem arz etmektedir. Nitekim güvenlik duvarları örerek bu alanın yönetilemeyeceği, hatta böyle bir yaklaşımın insan haklarını ve iyi yönetişim ilkelerini zedeleyeceği açıkça görülmüştür. Çin'in internet üzerindeki sıkı kontrolleri ve güvenlik duvarlarının yarattığı insan hakları ve insani güvenlik sorunları bu durumun somut bir örneğini teşkil etmiştir. Bu bağlamda etkili bir internet yönetişimi modeli için şeffaflık,

hesap verebilirlik, katılımcılık, hukukun üstünlüğü ve insan haklarına saygı gibi iyi yönetişim ilkelerinin ön plana çıkarılması şarttır. Ancak bu sayede, internetin küresel toplum için sunduğu fırsatlardan en üst düzeyde yararlanılabilirken; potansiyel riskler etkin bir şekilde yönetilebilir hale gelecektir.

Bu alanda potansiyel sorunların çözümü için sunulan önerilerin genel itibariyle teknik ve güvenlik odaklı olduğu, diğer sosyo-politik sorunları göz ardı ettiği görülmektedir. Ancak nihai olarak anlaşılması gereken önemli bir nokta, bu alanın güç ve güvenlik odaklı realist yaklaşımlarla yönetilmeye müsait bir yapıda olmadığıdır. Her şeyden önce, siber alanın doğası buna engel teşkil etmektedir. Güvenlik odaklı yaklaşımların çıkış noktası genellikle bu alanın anarşik olduğu, bu nedenle yönetilmesi gerektiği üzerindedir. Oysa buradaki anarşi, fiziksel alandaki anarşiden çok daha farklı bir formdadır. Siber uzayın karmaşık dinamikleri üzerine yapılan incelemeler, burada da bir tür anarşinin hüküm sürdüğünü ortaya koymakta; fakat bu durumun, fiziksel uluslararası ilişkilerde gözlemlenen anarşiden oldukça farklı olduğu sonucuna varmaktadır. Fiziksel uluslararası ilişkilerde anarşi, uluslararası hukuk, uluslararası örgütler ve diplomasi gibi çeşitli kurumlar aracılığıyla azaltılır ve yönetilebilir hale getirilebilir. Buna karşın, siber uzayda bu tür kurumlar ya çok zayıf, ya mevcut değil, ya da devlet-dışı aktörler tarafından temsil edilmektedir. Bu durum, siber uzayda daha derin bir anarşi düzeyi olan "hiper anarşi"ye işaret etmektedir. Siber uzayın bu özgün yapısı, devletler ve devlet-dışı aktörler arasında yeni ve karmaşık bir ilişkiler ağını meydana getirmektedir. Bu nedenle siber uzayın yönetişimi, geleneksel güvenlik yaklaşımlarından farklı, daha dinamik, esnek ve kapsayıcı bir model gerektirmektedir. Böylesi bir modelin, siber uzayın özgün yapısına yanıt verebilecek kapsayıcılığa sahip olması gerektiği öngörülmektedir.

Burada dikkat çeken diğer bir nokta, yönetişim üzerine yapılan çalışmalarda sıklıkla güvenlik yönetişimine atıfta bulunulmasıdır. Bu durum, genellikle siber tehditlere işaret eder ve bu tehditlerin büyük bir kısmı, alanın kendisinden ve kullanıcılardan kaynaklanan sorunlardan ortaya çıkar. Oysa ki kalan politik ve yönetilemeyen sorunların neredeyse tamamı, burada faaliyet gösteren aktörlerin alanı normatif unsurlardan uzaklaştıran eylemlerde bulunmalarından kaynaklanmaktadır. Bu durum, insan hakları sorunlarından teknik standardizasyon zorluklarına, kalkınma meselelerinden bir hukuk mekanizmasının oluşturulamamasına kadar geniş bir yelpazede sorunlara sebebiyet vermektedir. Bu sorunlar, genellikle aktörlerin işbirliği

unsurlarından kaçınmaları veya egemenlik ve ulusal çıkar algısına dayalı hareket etmeleri gibi nedenlerden türemektedir.

Oysa sorunun kaynağı ne ise, çözümü de orada. Nitekim karşı karşıya kalınan ifade özgürlüğü, gizlilik, kalkınma, dijital bölünme ve erişim gibi sorunların neredeyse tamamı paydaşların şeffaflık ve hesap verebilirlik gibi iyi yönetişim ilkelerine uygun hareket etmeleriyle çözüme kavuşturulabilecek meselelerdir. Burada paydaşların alacağı kararlar ve önlemler önem arz ederken, taahhütte bulundukları ilkelere uygun hareket etmeleri, iyi yönetişimin gerektirdiği güvenilirlik ilkesini etkin kılacaktır.

İşbirliğini teşvik eden yaklaşımların benimsenmesi ve yasal uyum süreçlerini tetikleyecek bir hukuk mekanizmasının kurulması da, bu ilkelerin işlevsel olmasında kritik bir role sahip olacaktır. Ancak bu konuda atılması gereken adımlar belirsizliğini korumakta, bu da "sorun içinde sorun" teşkil etmektedir. Özellikle devletlerin ve özel sektörün farklı çıkarlara, hedeflere ve yasal yapılara sahip olmaları, bu işbirliğini daha karmaşık bir hale getirmektedir. Diğer yandan, mevcut geleneksel uluslararası hukuk mekanizmalarının siber uzayın doğasının gerektirdiği dinamizme yanıt verebilecek mahiyette olmaması, düzenleyici çerçevelerin oluşturulmasını zorlaştırmaktadır.

Uluslararası düzeyde kabul görecek bir yasal çerçevenin eksikliği ihtiyacı sıklıkla gündeme gelse de, siber uzayda etkin bir hukuk mekanizması oluşturulamamaktadır. Bu, pek çok sorun alanından kaynaklansa da, başat sorun, paydaşların çıkar unsurlarını işbirliği unsurlarından daha önemli görmeleridir. Diğer yandan, devletlerin egemenlik ve ulusal çıkarları önceliklendirerek hareket etmeleri, alanın güvenlikleştirilmesine sebebiyet vermekte ve sansür uygulamaları aracılığıyla online özgürlüklerin kısıtlanmasını beraberinde getirmektedir. Bu durum, siber suçlarla mücadele, siber saldırıların önlenmesi, siber savaş ve çatışmalara yönelik norm ve kuralların geliştirmesi gibi konularda ciddi zorluklar yaratmaktadır. Bu nedenle siber uzay için etkin bir hukuk ve yönetişim modeli arayışı halen devam etmektedir.

Netice itibariyle, bir platformun yukarıda sayılan iyi yönetişim unsurlarıyla uyum içinde hareket ettiği ve bu alan için gerekli olan yönetişim modelini karşıladığı gözlemlenmiştir: IGF. Bu platform, siber uzayın yönetişiminde işbirliği ve çok paydaşlılığı teşvik eden, ama aynı zamanda güvenlik meselelerine de eğilen, BM çatısı altında "dengeli" bir yaklaşım benimseyerek faaliyet gösteren bir platformdur. 2006 yılında kurulan IGF, şeffaflık, hesap verebilirlik ve kapsayıcılık ilkelerini

benimseyerek, internetin yönetişiminde tüm ilgili paydaşların –devletler, özel sektör, sivil toplum, teknik kuruluşlar ve akademik topluluk– görüşlerini ifade edebilecekleri bir alan sunmaktadır. Forum, çok paydaşlı yapısıyla siber uzayın yönetişiminde farklı bakış açılarının ve ihtiyaçların gündeme gelmesi noktasında katkıda bulunmaktadır. Diğer yandan, uluslararası işbirliği ve yasal uyum konularında kaydettiği ilerlemelerle, bu alandaki en önemli girişimlerden biri olarak kabul edilir. Bu yönüyle IGF, siber uzayın daha adil, güvenli ve açık hale gelmesine yönelik çabaları destekleyen bir model olarak öne çıkmaktadır.

Ancak IGF'nin de karşılaştığı birtakım engeller bulunmaktadır. Zira IGF'nin hukuki bağlayıcılığının olmaması, önemli bir sınırlılık teşkil etmektedir. Bu durum, Forum'un öneri ve politikalarının uygulanmasını zorlaştırırken, etkinliğini ve otoritesini sınırlayan bir faktör olarak öne çıkmaktadır. Bu nedenle, IGF'ye hukuki bağlayıcılık kazandırılması gerektiğine yönelik bir argüman geliştirilmesi fikri gündeme gelmektedir. Böylesi bir argüman geliştirilirken, Uluslararası İlişkilerde norm, hukuk ve düzen anlayışının küresel adalet ve eşitliğin temeli olduğunu kabul eden normatif teori, bu anlamda rehber olarak kullanılabilir. Hukuki bağlayıcılığın kazandırılması sürecinde uluslararası hukuk normları, devletlerin egemenlik hakları, siber uzayın özgün dinamikleri ve çok paydaşlı yapının korunması gibi unsurlar dikkate alınmalıdır. Ayrıca, IGF'ye bağlayıcılık kazandırılmasının uluslararası işbirliğini ve konsensüsü gerektirecek bir süreç olduğu göz önünde bulundurulmalıdır. Dolayısıyla bu süreçte, farklı devletlerin ve devlet dışı aktörlerin çıkarları, beklentileri ve hukuki sistemleri arasında denge kurmak önem arz etmektedir.

Tezin Konusu

Bu çalışma, küresel internet yönetişiminin nasıl gerçekleştirilebileceği ve bu süreçte karşılaşılan zorluklar ile fırsatlar üzerine odaklanmaktadır. Neredeyse her şeyin küreselleştiği bir ortamda internetin ortaya çıkışı ve gelişimi, uluslararası ilişkileri ve iç politikaları derinden etkileyen yeni bir dinamik oluşturmuştur. Bu bağlamda internet üzerinden gerçekleştirilen faaliyetlerin yönetişimi, çok sayıda aktörü kapsayan karmaşık bir meseleye dönüşmüştür. Devletler, uluslararası kuruluşlar, özel sektör, sivil toplum kuruluşları ve bireyler, dijital alanın yönetişiminde önemli roller üstlenmektedir. Bu çok aktörlü yapı, etkili bir yönetişim modelinin geliştirilmesini zorunlu kılmaktadır.

İnternetin küresel ölçekte yönetişimi, teknik sorunların yanı sıra politik, sosyal ve ekonomik meseleleri de içermektedir. Bu kapsamlı sorun alanı, siber güvenlik, veri mahremiyeti, dijital eşitsizlikler, erişim sorunları ve online ifade özgürlüğü gibi konuları kapsamaktadır. Bu sorunların çözümü için uluslararası işbirliği ve çok paydaşlı yönetişim modellerine ihtiyaç duyulsa da, mevcut yönetişim modelleri küresel internet yönetişimi için yeterli olmadığından; daha kapsayıcı, şeffaf ve hesap verebilir bir yönetişim modeline ihtiyaç vardır.

ICANN gibi kurumlar, internetin yönetişiminde önemli roller üstlenmiş olsalar da, bu yapılar yalnızca teknik meselelere odaklanmakta ve geniş bir paydaş yelpazesini kapsamamaktadır. Ayrıca, uluslararası ilişkilerde güç ve güvenlik odaklı yaklaşımlar, siber uzayın yönetişiminde yetersiz kalmaktadır. Siber uzayın doğası ve karmaşık dinamikleri, geleneksel güvenlik yaklaşımlarından farklı, yenilikçi ve kapsayıcı stratejiler gerektirmektedir.

BM çatısı altında faaliyet gösteren ve çok paydaşlı bir yapı sunan bir platform olarak IGF, internetin yönetişiminde tüm ilgili paydaşların görüşlerini ifade edebilecekleri bir alan sağlamaktadır. Ancak IGF'nin hukuki bir bağlayıcılığının olmaması, öneri ve politikalarının uygulanmasını zorlaştırmaktadır. Bu nedenle, IGF'ye hukuki bağlayıcılık kazandırılması, etkin bir yönetişim modeli için önemli bir adım olabilir.

Bu bağlamda bu tez, siber hukuk bağlamında internet yönetişiminin nasıl iyileştirilebileceğini incelemekte ve IGF modelinin potansiyelini ve sınırlılıklarını ele almaktadır. Bu süreçte, uluslararası hukuk normları, devletlerin egemenlik hakları, siber uzayın özgün dinamikleri ve çok paydaşlı yapının korunması gibi faktörler dikkate alınacaktır. Dolayısıyla tezde, IGF bünyesinde etkin bir küresel internet yönetişim modelinin geliştirilmesi ve bu modelin siber hukuk çerçevesinde nasıl uygulanabileceği normatif teorinin argümanlarının rehberliğinde araştırılacaktır.

Tezin Amacı

Bu çalışmada küresel internet yönetişiminin bir "sorun" teşkil ettiğini yukarıda belirtmiştik. Bu sorunun çözülmesi için atılmış olan ve atılmaya devam eden adımların yanı sıra atılması "gereken" adımların hangi sınırlar dahilinde tutulacağını belirlemeye çalışmak, bu çalışmanın esas amacını oluşturmaktadır. Bu bağlamda, iyi yönetişim ilkelerinin ve normatif teorinin önemi özellikle vurgulanmalıdır. Bu saikle tezin amaçları aşağıdaki gibi kategorize edilmiştir:

Sorunun Küresel Mahiyetini Vurgulamak: Bu çalışmanın ilk amacı, internet yönetişiminin neden küresel bir sorun olarak kabul edilmesi gerektiğini vurgulamak ve bu geniş çaplı sorunun farklı boyutlarını net bir şekilde ortaya koymaktır. İnternet yönetişimiyle ilişkili sorunların belirlenmesi süreci, teknik zorluklardan ifade özgürlüğü ve insan haklarına kadar geniş bir yelpazede değerlendirme yapmayı gerektirir. Bu sorunların her biri, farklı coğrafi ve sosyo-ekonomik bağlamlarda farklı şekillerde tezahür edebilir. Bu tez, bu karmaşıklığı sistematik bir şekilde ele alarak, internetin yönetişimiyle ilgili küresel sorun alanlarını açıkça tanımlamayı ve bu sorunların nedenlerini ve potansiyel etkilerini analiz etmeyi amaçlar. İnternet yönetişimi, sadece teknik altyapı ve erişim meselelerini değil, aynı zamanda içerik yönetimi, veri koruma, gizlilik hakları ve siber güvenlik gibi konuları da içerir. Bu konular, ulusal sınırları aşan etkileri ve çeşitli aktörler arasındaki etkileşimi nedeniyle, küresel çözümler gerektirir. Dolayısıyla, bu amacın odak noktası, internet yönetişimiyle ilgili sorunların küresel doğasını anlamak ve bu sorunların çeşitli yönlerini tanımlayarak internet yönetişiminin küresel bir sorun olarak ele alınması gerektiğine dair farkındalığı artırmaktır.

Teknik, Güvenlik ve Devlet Odaklı Bakış Açısına Alternatif Geliştirmek: Çalışmada internet yönetişimi kavramının, tekniği merkeze alan bakış açılarından kurtarılması amaçlanmaktadır. Bu bağlamda devletin değiştirici ve dönüştürücü rolünü kullandığı fakat başat olmadığı, çok aktörlü ama aynı zamanda çok-paydaşlı bir perspektifin hâkim olduğu bir ortamın varlığı, farklı disiplinlerin argümanlarıyla desteklenecektir. Bu çerçevede, çok paydaşlı bir yaklaşım benimsenerek, internet yönetişiminin farklı aktörler tarafından nasıl şekillendirildiği üzerine bir analiz yapılacaktır. Bu analizde, devletler, özel sektör, sivil toplum kuruluşları, akademik topluluk ve diğer ilgili paydaşların internet yönetişimindeki rolleri, etkileşimleri ve çatışma alanları ele alınacaktır.

Siber Uzayın Yönetilebilirliğini Tartışmak: Bu çalışmanın diğer bir temel hedefi, siber uzayın yönetilebilirliğine ve siber iyi yönetişim ilkelerinin uygulanabilirliğine ilişkin sorulara odaklanarak bu soruları iyi yönetişim ilkelerinin pratikteki yansımalarına bakarak yanıtlamaya çalışmaktır. İyi yönetişim; şeffaflık, demokrasi, hesap verebilirlik, katılımcılık, hukukun üstünlüğü, etkililik ve verimlilik, eşitlik ve adalet gibi temel ilkeleri içerdiğinden, siber uzayın etkili ve sorumlu bir şekilde yönetilmesini sağlamada kritik bir role sahiptir. Çalışma, siber uzaydaki mevcut zorlukların, bu iyi yönetişim

ilkelerinin uygulanmasıyla üstesinden gelinebileceğini savunmakta ve siber uzayın yönetilebilir olduğunu göstermeyi amaçlamaktadır. Ancak, siber uzayın yönetişimine ilişkin bu olumlu yaklaşımın yanı sıra, siber uzayın yönetilebilirliğine dair zorluklar da vurgulanacaktır.

Siber Hukukun Olasılıkları Üzerine Tartışmak: Bu çalışmanın hukukla ilgili temel amacı, siber uzayın yönetişiminde mevcut olan ve bir hukuk mekanizmasının eksikliğinden kaynaklanan sorunların üstesinden gelinip gelinemeyeceğini tespit etmektir. Siber hukuk, internet ve dijital teknolojilerle ilgili hukuki meseleleri kapsayan geniş bir alanı ifade eder. Bu alandaki mevcut zorluklardan biri, ulusal ve geleneksel uluslararası hukuk sistemlerinin siber uzayın küresel doğasına uyum sağlamakta yaşadığı güçlüktür. Ayrıca, siber suçlar, veri koruma, gizlilik hakları ve ifade özgürlüğü gibi konularda uluslararası bir konsensüsün olmaması, etkili bir siber hukuk sisteminin oluşturulmasını zorlaştırmaktadır. Bu bağlamda, siber hukukun olasılıkları üzerine derinlemesine düşünmek ve bu alanda iyi yönetişim ilkelerinin nasıl uygulanabileceğini gündeme taşımak esastır.

IGF'ye Hukuki Bağlayıcılık Kazandıracak Çözüm Önerilerinde Bulunmak: Çalışmanın son amacı ise, IGF'nin internet yönetişimi için uygun bir model olduğunu varsaymak ve fakat, onun etkinliğinin artırılması için hukuki bağlayıcılığının kazandırılması gerektiğini vurgulamaktır. Bu bağlamda, IGF'nin mevcut yapısını güçlendirirken karşılaşabileceği hukuki sınırlılıklar dikkate alınarak çözüm önerileri sunulması amaçlanmaktadır. Bu süreçte, yine normatif teori rehber alınarak, IGF'nin işleyişine ve ilkelerine uygun hukuki temellerin nasıl oluşturulabileceği incelenecektir. Bu amaç doğrultusunda normatif teori, siber uzayın yönetişiminde etik değerlere, adalet anlayışına ve insan haklarına dayalı bir yaklaşımı desteklemektedir. Bu yönüyle normatif teori, IGF'nin daha kapsayıcı, adil ve etkili bir yönetişim modeline dönüşmesine rehberlik edebilir. Çözüm önerileri, IGF'nin hukuki bağlayıcılığının nasıl sağlanabileceği, bu sürecin karşılaşabileceği zorluklar ve bu zorlukların nasıl aşılacağı üzerine yoğunlaşacaktır. Ayrıca, çok paydaşlı yapının korunması ve siber uzayda etik ve adaletin teşvik edilmesi gibi unsurlar, bu süreçte öncelikli olarak değerlendirilecektir.

Tezin İçeriği ve Kapsamı

Birinci bölümde, internet yönetişimi üzerine kavramsal kuramsal bir çerçevenin oluşturulmasına odaklanılmıştır. Bu çerçeve içinde internet yönetişiminin tarihçesi, küreselleşmesi ve yönetişim tartışmaları geniş bir perspektiften ele alınmaktadır. Aynı zamanda bu bölümde farklı teorik yaklaşımlar – realizm, liberalizm, inşacılık ve normatif teori – internet yönetişimi bağlamında incelenmektedir. Bu incelemeler, internet yönetişimi ile ilgili geniş bir paydaş analizini de içermekte olup, çeşitli aktörlerin internet yönetişimindeki rolleri, etkileşimleri ve bu aktörler arasındaki dinamikler kapsamlı bir şekilde tartışılmaktadır. Bu bölüm, internet yönetişiminin yalnızca teknik bir mesele olmadığını, aynı zamanda politik, sosyal ve kültürel faktörlerle de şekillenen karmaşık bir yapı olduğunu vurgulamaktadır.

İkinci bölüm, internet yönetişiminin küresel bir sorun olarak neden ele alınması gerektiğini detaylandırmakta ve bu geniş çaplı sorunun çeşitli boyutlarını ortaya koymaktadır. Teknik ve politik sorun alanları ile birlikte, siber uzayın yönetilebilirliği ve siber iyi yönetişimin mümkün olup olmadığı gibi temel sorular ele alınmaktadır. İyi yönetişimin mümkün olup olmadığı sorusu, "Zorluklar", "Zorunluluklar" ve "Olasılıklar" başlıkları altında incelenmiş; burada iyi yönetişimin hem önemli zorluklar barındırdığı, hem de bir zorunluluk teşkil ettiği ve bu zorlukların üstesinden gelinerek gerçekleştirilebileceği olasılığının altı çizilmiştir. Siber uzayda karşılaşılan zorluklar ve bu zorlukların üstesinden gelmek için gereken stratejiler, uluslararası işbirliği ve çok paydaşlı yaklaşımların önemine dikkat çekilerek tartışılmaktadır. Bu bölümde, siber uzayın yönetilebilir olduğuna dair argümanlar geliştirilirken, aynı zamanda bu alanın yönetişimine ilişkin mevcut zorluklar ve bunların çözümü için gereken koşullar üzerine bir değerlendirme yapılmaktadır.

Üçüncü bölüm, siber hukukun evrimi, yaklaşımları ve siber uzayın uluslararası hukuk çerçevesinde nasıl ele alınabileceği üzerine odaklanmaktadır. Siber savaş, siber istihbarat ve siber suçlar gibi konuların, geleneksel uluslararası hukuk çerçevesinde incelenmesi ve uluslararası normlar ve düzenlemelerin bu yeni meydan okumalara nasıl yanıt verebileceğinin tartışılması bu bölümün odak noktalarındandır. Ayrıca, siber hukuka yönelik mevcut yaklaşımlar ve uluslararası düzeyde hukuki uyumun zorlukları ve gereklilikleri üzerine derinlemesine bir analiz sunulmaktadır. Bu bölüm, siber uzayın hukuki düzenlemeleri ve uluslararası hukukun bu alandaki etkisi hakkında kapsamlı bir değerlendirme sağlamaktadır.

Dördüncü bölüm, çeşitli internet yönetişimi modelleri ve özellikle IGF modelinin potansiyelini, mevcut sınırlılıklarını ve hukuki bağlayıcılık kazandırma yollarını ele almaktadır. IGF'nin hukuki statüsünün güçlendirilmesine yönelik zorluklar ve olasılıklar "Hukuki Sınırlılıklar" başlığı altında değerlendirilmekte, normatif teori ışığında stratejik öneriler geliştirilmektedir. Bu bölüm, IGF modeline hukuki bağlayıcılık kazandırırken karşılaşılabilecek hukuki ve pratik sınırlılıklara dair kapsamlı bir analiz sunar ve bu sürecin nasıl yönetilebileceği üzerine odaklanır.

Tezin Araştırma Soruları

Bu çalışmanın araştırma soruları, tezin ana amacını destekleyecek ve küresel internet yönetişimi alanında mevcut sorunların ve potansiyel çözüm yollarının kapsamlı bir analizini sağlayacak şekilde tasarlanmıştır. Sorular, siber uzayın yönetişimi, uluslararası hukukun rolü, siber hukukun olasılıkları ve normatif teori çerçevesinde çözüm önerileri gibi çeşitli boyutları ele alarak, çalışmanın multidisipliner bir yaklaşımla nasıl ilerleyeceğini ortaya koymaktadır. Bu bağlamda çalışmanın temel araştırma soruları şunlardır:

1. "Küresel" anlamda siber iyi yönetişim mümkün müdür? Küresel siber iyi yönetişimi etkili kılan veya engelleyen faktörler nelerdir?
2. Uluslararası hukukun mevcut mekanizmaları, siber uzayın yönetişimi konusunda ne ölçüde etkilidir? Mevcut uluslararası hukuk çerçevesi, siber uzayın dinamiklerini yeterince yansıtabilir mi?
3. Olası bir uluslararası siber hukuk mekanizması, küresel internet yönetişimi sorunlarına çözüm sunabilir mi?
4. IGF modelinin küresel internet yönetişiminde karşılaşılan mevcut sorunları çözmedeki etkinliği nedir ve bu model nasıl iyileştirilebilir?
5. IGF'ye hukuki bağlayıcılık kazandırılması sürecinde karşılaşılması muhtemel zorluklar ve bu zorlukların üstesinden gelinmesi için sunulan çözüm önerileri nelerdir?

Tezin Hipotezleri

1. Siber uzay sınırsız bir alandır fakat bu alandaki sınırsızlık iyi yönetişim ilkeleriyle pozitif bir sınırlılığa kavuşabilir. Bu karmaşık yönetişim manzarası, çeşitli

paydaşların siber uzayı yöneten normları, kuralları ve standartları şekillendirmede kritik bir rol oynadığını göstermektedir.

2. Uluslararası İlişkiler disiplini içerisinde sıklıkla ihmal edilen Normatif teori, küresel internet yönetişimi sorunlarına "en iyi" rehberliği sunacak teoridir. Çünkü bu teori, çok paydaşlı yaklaşımların gerekliliğini, internetin herkes için adil ve eşit bir şekilde erişilebilir olmasının önemini ve güçlü bir hukuki çerçevenin varlığını vurgular.

3. Etkili bir uluslararası siber hukuk mekanizmasının oluşturulmasında birtakım zorluklar olsa da, bu zorunlu hale gelmiştir. Bu doğrultuda, çok paydaşlı işbirliği, esnek ve dinamik yaklaşım, geliştirilmiş diyalog kültürü, siber/dijital diplomasi faaliyetleri, teknoloji tarafsızlığı ve uyumluluk, eğitim ve farkındalık ve hesap verebilirlik gibi unsurların hayata geçirilmesiyle bu olasıdır.

4. IGF'nin önerilerinin bağlayıcılık kazanması, belirli hukuki süreçler ile yapısal değişiklikler aracılığıyla teorik olarak mümkündür.

Tezin Sınırlılıkları

Teknik Sorunların Analizi: Bu tezin ilk sınırlılığı, özellikle politik sorunlara ağırlık verilmesi nedeniyle teknik sorunların görece daha az dikkate alınmış olmasıdır. Küresel internet yönetişimi ve siber hukuk konuları ele alınırken, tez kapsamında politik, hukuki ve sosyo-kültürel faktörler üzerinde yoğunlaşılmış, bu da teknik meselelerin ve çözümlerin derinlemesine incelenmesine sınırlı alan bırakmıştır.

Model Analizi: Bu tez, küresel internet yönetişimi sorununu ve bu alanda siber hukuk bağlamında IGF modelinin potansiyel etkilerini ele almaya odaklanmıştır. Bu nedenle, internet yönetişiminin diğer modelleri daha az incelemeye tabi tutulmuştur.

Teknolojik Gelişmeler: Bu tez, hazırlandığı dönemin teknolojik durumunu ve mevcut tartışmaları temel almaktadır. Ancak, gelecekteki teknolojik gelişmeler ve yenilikler, bu çalışmanın bulgularının ve önerilerinin uygulanabilirliğini etkileyebilir. Dolayısıyla hızlı teknolojik ilerleme, bu tezin bulgularının ve önerilerinin gelecekteki uygulanabilirliğini ve etkinliğini etkileyebileceğinden, sürekli adaptasyon ve yenilik gerektirmektedir.

Normatif Teorinin Kapsamı: Bu tezin genelinde kozmopolit bir bakış açısıyla hareket edilerek evrensel insan hakları ve küresel adalet anlayışı merkeze alınmıştır.

Kozmopolitanizm, tüm bireylerin evrensel değerlere ve haklara sahip olduğunu savunur ve bu hakların küresel düzeyde korunması gerektiğini öne sürer. Bu perspektif, internetin sınırları aşan doğası ve küresel topluluk üzerindeki etkileri göz önünde bulundurularak seçilmiştir. Ancak, bu yaklaşımın kendine özgü bir sınırlılığı vardır: komüniteryen perspektifin dikkate alınmaması. Komüniteryenizm, topluluk değerlerinin ve kültürel özelliklerin bireysel haklardan daha ağırlıklı olabileceğini savunur ve insan haklarının kültürel bağlama göre göreceli olabileceğini öne sürer. Bu perspektiften bakıldığında, küresel internet yönetişimi modelleri, farklı kültürel ve toplumsal ihtiyaçları yeterince yansıtamayabilir.

Tezin Yöntemi

Bu çalışma, küresel internet yönetişimi sorunlarını normatif bir çerçevede değerlendirerek öneriler sunmayı ve siber hukuk kapsamında IGF modelinin hukuki bağlayıcılığa kavuşturulması için öneriler geliştirmeyi amaçlamaktadır. Araştırma, küresel siber yönetişimin karşılaştığı temel sorunları detaylı bir şekilde inceleyecek ve normatif teori çerçevesinde çözüm önerileri sunacaktır. Bu süreçte, siber uzay ve siber hukukun dinamik ve sürekli gelişen doğası göz önünde bulundurulacaktır. Araştırmanın yürütülmesi sırasında, siber yönetişimi etkileyen tüm paydaşların rolleri, aralarındaki anlaşmazlık ve rekabetler neden-sonuç ilişkisi çerçevesinde incelenecek ve bu dinamiklerin yönetişim üzerindeki etkileri analiz edilecektir.

Bu çalışma, nitel araştırma yöntemlerini temel alacaktır. Araştırma, geniş bir literatür taraması yaparak, siber yönetişim ve hukuk üzerine yazılmış bilimsel kitaplar, akademik tezler, hakemli makaleler ve güncel internet kaynaklarını kapsamlı bir şekilde inceleyecektir. Bu süreçte, bilimsel veriler, istatistikler, güncel araştırma bulguları, raporlar ve uluslararası düzeyde kabul gören resmî belgeler temel alınacaktır.

Araştırmanın ontolojisini oluşturacak nesne alanları, yani analiz birimleri, yönetişim modelleri tarafından öngörülen aktörler -devletler, uluslararası ve hükümetlerarası kuruluşlar, özel sektör, sivil toplum ve bireyler- bağlamında değişkenlik gösterecektir. Bu çeşitlilik, araştırmanın çok boyutlu sorunları ele almasını ve bütüncül bir perspektiften çözümler önermesini sağlayacaktır.

Tezin Katkıları ve Önemi

Bu tez, internet yönetişimi alanında önemli teorik ve pratik katkılar sunarak, bu alandaki akademik çalışmalara, politika yapım süreçlerine ve çok paydaşlı işbirliği

çabalarına yeni bir bakış açısı getirmektedir. Aşağıda sıralanan katkılar, internetin küresel yönetişimiyle ilgili daha derinlemesine anlayışların geliştirilmesine ve bu alanda karşılaşılan zorlukların üstesinden gelinmesine yönelik önemli adımlar atılmasını sağlamaktadır:

Yeni Bir Perspektif: Mevcut literatürde genellikle teknik meselelere verilen ağırlığın aksine, politik meselelerin ve paydaşların etkileşiminin öneminin altı çizilmekte ve internet yönetişimi kavramına daha kapsamlı bir perspektiften yaklaşılması amaçlanmaktadır. İnternet yönetişimi ile ilgili birçok tartışmaya konu olması gereken bu sorunlar gündemin gerisinde kalmaktadır. Dolayısıyla internetin "yüzeyindeki" bu konular genellikle verilerin korunması, ifade özgürlüğü, egemen devletlerin genel kuralları empoze etme kabiliyetleri ve internetin ulus aşırı doğası gibi yönleri içermektedir. Bu konulara ağırlık veren bir yaklaşımın, internet yönetişimi tartışmalarını zenginleştireceği ve disiplinler arası bir anlayışı teşvik edeceği öngörülmekte; bu sayede internetin küresel yönetişimiyle ilgili daha derinlemesine bir anlayışın ve çözümlerin geliştirilmesine katkıda bulunulacağı düşünülmektedir.

Geniş Bir Paydaş Analizi: Tez, internet yönetişimi süreçlerinde aktörlerin rollerini ve etkileşimlerini kapsamlı bir şekilde inceleyerek, geniş bir paydaş analizi sunar. Bu analiz, internet yönetişimindeki çeşitli aktörlerin perspektiflerini ve katkılarını anlamak açısından önemli bir kaynak oluştururken; çok paydaşlı işbirliğinin önemine atıfta bulunmaktadır.

Normatif ve Hukuki Bir Katkı: Çalışma, literatürdeki diğer çalışmalara ek olarak siber yönetişimin normatif ve hukuki boyutu konusunda katkı sağlamayı amaçlamaktadır. Elbette daha önce siber alanın normatif boyutu ile ilgili çalışmalar yok değildir. Fakat bunlar genellikle normatifi bir teori olarak değil, olması gereken unsurlar üzerinden değerlendirmiştir. Bunun yanında, hukuki boyutla ilgili yapılan çalışmaların çoğu hukukun yönetişim boyutunu belli konularla sınırlandırmıştır. Aynı zamanda siber yönetişim ile ilgili yapılan çalışmalarda internet kaynaklarının yönetişimine dair teknik konular daha geniş ele alınmış, kapsamlı bir hukuk çerçevesi sunulamamıştır. Bu bilgiden hareketle bu çalışma, yönetişim kavramının hem "politik" hem "hukuki" hem de "normatif" boyutuna Uluslararası İlişkiler disiplini ve Uluslararası Hukuk'un öngördüğü argümanlar üzerinden yaklaşarak, disipline katkı sağlamayı amaçlaması açısından önem arz etmektedir.

Hukuki Bağlayıcılık Üzerine Çözüm Önerileri: IGF'nin hukuki statüsünün güçlendirilmesi gerekliliği üzerine odaklanan tez, bu alandaki önemli bir eksikliği ele alır. Normatif teoriden yola çıkarak, IGF'nin hukuki bağlayıcılığını artırma yolları üzerine somut öneriler sunar ve küresel internet yönetişiminin etkinliğini artırmayı hedefler. IGF'nin mevcut durumunda bir hukuki bağlayıcılığının olmaması, öneri ve politikalarının uygulanmasını zorlaştırmakta ve etkinliğini sınırlamaktadır. Bu nedenle, IGF modeline hukuki bağlayıcılık kazandırılması ve bu modelin normatif teori çerçevesinde geliştirilmesi, siber uzayın yönetişiminde önemli bir adım olacaktır.

Tezin İlgili Literatürdeki Yeri

Küresel internet yönetişimi, teknolojinin sürekli evrimi ve küreselleşmenin derinleşmesiyle birlikte hukuki, teknik, politik ve sosyal olmak üzere dört ana boyutta çeşitli zorluklar sunan bir alan haline gelmiştir. Bu karmaşık ve dinamik alan, çok çeşitli aktörlerin katılımıyla şekillenmektedir ve sosyal medya platformlarından devletlere, uluslararası kuruluşlardan sivil toplum örgütlerine kadar geniş bir yelpazeyi kapsamaktadır. Sansür ve içerik düzenlemesi, e-ticarette telif haklarının korunması, gizlilik ve gözetim politikaları, iletişim hizmetlerinin düzenlenmesi, teknik standartların oluşturulması gibi çeşitli konularda düzenlemeler yapılmaktadır. Bunlar internetin ilk yaygınlaşmaya başladığı zamanlardan bu yana devamlılığını sürdüren düzenlemeler olarak adlandırılabilir. Ancak internet kullanımının küresel anlamda yarattığı politik sorunlar da mevcuttur. Yalnızca devletlerin değil, bireyler de dahil olmak üzere bütün aktörlerin maruz kaldığı siber suçlar ve saldırılar, politik sorunların başında gelmektedir. Bu çalışmada da internet yönetişiminin ilgilendiği politik sorunlar, bunun yarattığı sonuçlar ve buna yönelik geliştirilebilecek yönetişim mekanizmaları ele alınacağı için, teknik boyuttan ziyade politik boyut -bu çalışma açısından- daha birincil kabul edilecektir.

Literatürdeki ortak görüş, internet yönetişimi üzerine tartışmaların 1990'lardan itibaren ortaya çıkmaya başladığına yöneliktir (Mueller, 2004; Rakner & Menocal & Fritz, 2007; Dahlgren, 2005). Choucri (2012), 2000'li yılların ortalarından bu yana önemli ekonomik, sosyal ve politik meselelerin, bilgi ve iletişim teknolojilerine bağlı bir hale geldiğini ve siber uzay konularının artık alçak politika (*low politics*) alanından yüksek politika (*high politics*) alanına doğru evrildiğini belirtmiştir. DeNardis (2014), dijital yönetişim üzerindeki çatışmaların yirmi birinci yüzyılda politik ve ekonomik gücün ortaya çıktığı yeni alanlar haline geldiğine işaret ederken; Price (2014), küresel internet

yönetişimini "yarı olimpik bir spor" olarak tanımlayarak internet yönetişimi üzerinden devletler arasındaki küresel rekabetin yoğunluğunu vurgulamaktadır.

Mueller (2010), *Networks and States: The Global Politics of Internet Governance* adlı çalışmasında internet yönetişiminin yeni ve ilgi çekici yönetişim sorunları ortaya çıkardığını ve küresel siyaset ile yeni transnasyonel kurumların oluşumuna yol açtığını belirtir. Mueller, ağ yönetişimi teorilerinden yararlanarak, ICANN'in oluşumundan WSIS'e, IGF'nin kurulmasına ve ulusal düzeyde internet kontrolü ve güvenlik endişelerine kadar internet yönetişiminin geniş bir özetini sunar. Bu çalışma, internet yönetişiminin küresel siyasetteki rolünü ve transnasyonel kurumların iletişim-bilgi politikasının küresel yönetişimini teşvik etmedeki potansiyel önemine vurgu yapmıştır.

Benzer şekilde Choucri (2012), küresel internet yönetişiminin tartışmalı küresel siyaset alanlarından biri haline geldiğinin altını çizdiği çalışmasında, internetin küresel siyasette kabul görmesiyle birlikte internet yönetişiminin kurumsal, altyapısal, politik, ekonomik ve yasal dinamiklerinin dikkat çekmeye başladığını ifade etmiştir. Goldsmith ve Wu, 2006 tarihli *Who Controls the Internet?* adlı kitaplarında internet üzerine yapılan birçok tartışmanın uluslararası ilişkilerin klasik sorunları arasına girdiğini savunarak internetin küresel ölçekte yönetileceğini açıkça belirtmiş ve kabul etmişlerdir.

İnternet yönetişiminin tanımı konusunda halen akademik bir fikir birliği sağlanamadığı için, kavramın tanımlanmasını amaçlayan çalışmalar da yapılmaktadır. Bu anlamda internet yönetişiminin tanımını yapmak veya genişletmek oldukça önemlidir. Hofmann'a (2007) göre internet yönetişimi, "değişim halinde olan düzenleyici bir fikir" iken; Castells'e (2001) göre ise bu kavram, ağdaki iletişim ve koordinasyon işlevini sağlamaya yönelik prosedürleri kapsamaktadır. Castells bu tanımı devlet ve internet arasındaki ilişkiden bağımsız olarak yapsa da, devletlerin internet yönetişiminde önemli bir rol oynadığını ve bu konunun dışında bırakılamayacağını kabul etmektedir.

Mueller (2010) yönetişimi "kapsayıcı bir siyasi otoritenin yokluğunda birbirine bağlı aktörlerin koordinasyonu ve düzenlenmesi" olarak ifade eder. Ona göre, uluslararası ilişkilerde küresel yönetişim yönlendirme ve şekillendirme açısından fayda sağlarken, daha az hiyerarşik ve daha az otoriter bir ortam da sunmaktadır. İnternet yönetişimini de bu doğrultuda değerlendiren Mueller, internet yönetişimini uluslararası ilişkilerdeki

gibi politikaları yansıtacak şekilde koordine eden, yöneten ve şekillendiren bir süreç olarak tanımlamaktadır.

1998 yılında, ABD'nin inisiyatifiyle, küresel alan adları ve IP adreslerinin yönetimini üstlenmek üzere çok paydaşlı, kâr amacı gütmeyen bir özel şirket olan ICANN'in kurulmasıyla internet yönetişimine dair çalışmalar daha da artmaya başlamıştır. ICANN'in kurulmasıyla birlikte internet yönetişiminde çok paydaşlı bir tutum sergilendiği iddia edilse de, bu sisteme sık sık müdahale edilmiş ve halen edilmektedir. Dolayısıyla ICANN'in özellikle meşruiyet ve hesap verebilirlik gibi konular söz konusu olduğunda ABD ile diğer devletler arasında ciddi bir rekabet meselesi haline geldiği Castells (2001), Mueller (2002;2010) ve Hofmann'ın (2007) çalışmalarına konu olmuştur. Kalinauskas ve Barčys (2013), ICANN'in internet yönetişimindeki rolü ve ulusal yönetim kurumları ile olan etkileşimi hakkında problemli konuları incelemektedir. Bu çalışma, ICANN'in mevcut uluslararası hukuki durumunun çeşitli paydaşlar arasında tartışmalara yol açtığını ve bu konuda bir uzlaşıya varılmasını kolaylaştıracak analitik bir yaklaşım sunmayı amaçlamaktadır.

ICANN üzerine çalışmalar yapan Mueller (2006), bu kurum üzerinde inşa edilmeye çalışılan muhafazakâr rejimin internetin teknolojik yaşam döngüsüne zarar verdiğini iddia etmiştir. Bu doğrultuda devletlerin ICANN'e dair problemleri çözmek adına ekonomik teşvikleri arttırmaları gerektiğini vurgulamıştır. Kleinwæchter (2003), ICANN içinde devletler, endüstriyel firmalar ve sivil toplum tarafından oluşturulan üçlü sistemi incelediği çalışmasında, internetin ne kendi kendini yöneten ne de yalnızca devletler tarafından yönetilen bir sistem olmadığını vurgulamıştır. Ona göre "ortak düzenleme sistemi" tüm taraflar için hem istikrarlı hem de esnek bir politika çerçevesi sağlayacaktır.

DeNardis (2014), internet yönetişimi çatışmalarının 21. yüzyılda siyasi ve ekonomik gücün yeni bir alanı olarak ortaya çıkışını ele alır. İnternet yönetişimi teknolojilerinin ifade özgürlüğü, bireysel mahremiyet, ulusal güvenlik ve küresel ticaret gibi kamu yararı alanları üzerinde giderek artan bir etkisi olduğunu ve bu teknolojilerin dağıtık yapısının egemen ulus devletlerden özel düzenlere ve yeni küresel kurumlara doğru bir güç kayması yarattığını vurgular. DeNardis'in çalışması, Suriye'deki internet kesintileri, ABD hükümeti ile Google arasındaki çatışmalar, BM'nin internet üzerindeki etkisi, NSA izleme skandalları, siber güvenlik endişeleri ve sosyal medya şirketlerinin

gizlilik politikaları gibi çeşitli küresel tartışmalara değinerek, internet yönetişiminin karmaşık ve genellikle kamuoyunun dikkatinden uzakta kalan teknolojik ve kurumsal zorluklarını inceler. DeNardis, bu bağlamda, internetin teknik mimarisi ve yeni küresel kurumlar aracılığıyla nasıl yönetildiğini detaylandırarak, ekonomik ve ifade özgürlüğü üzerindeki etkilerini tartışan yeni internet yönetişimi meselelerini ortaya koymuştur.

Xiaoju (2015), siber uzayın beşinci çatışma alanı olarak kabul edilmesinin önemini vurgulayarak, internet yönetişiminin hala gelişmekte olan bir model olduğunu ve bu modelin siber uzayın temel niteliklerine dayanarak şekillendirilmesi gerektiğini savunmaktadır. Bu doğrultuda, deniz ve havanın yönetişim mekanizmalarından örnekler vererek, siber uzayın hem yerel hem de küresel bir ortak alan olduğunu ve bu nedenle uluslararası yönetişimin, ulusal egemenlik ilkesiyle sınırlı olması gerektiğini öne sürmüştür Xiaoju, aynı zamanda, yerel alanda ülkelerin münhasır egemenliğine ve kişisel ve bölgesel yargı yetkisine vurgu yaparken, küresel ortak alanda ülkeler arası işbirliğinin önemini ve bu işbirliğinin BM gibi mekanizmalar aracılığıyla nasıl desteklenebileceğini tartışmıştır.

Çalışmaların önemli bir kısmı, bu alanda devletin rolünü de tartışmıştır. Devletin internet yönetişimine dahil olması hem gerekli hem de kaçınılmazdır. Ancak siber alan için daha iyi bir ortam oluşturmak, özgürlük, demokrasi ve ekonomik kalkınmanın gelişimi için çaba sarf etmeyi gerektirir. Bu da devletlerin bu alanda güçlerini sınırlamaları, şeffaflıklarını arttırmaları ve diğer paydaşlarla koordinasyon içinde olmalarıyla mümkündür. Zira bilgi güvenliği alanındaki mevcut ve potansiyel tehditler, 21. yüzyılın en ciddi zorlukları arasındadır. Bugün devletlerin siber savaş yeteneklerini geliştirmeye çalıştıklarının bilinen bir durum olması nedeniyle, siber tehditlerin uluslararası barış ve ulusal güvenlik açısından risk oluşturacak kadar büyük olduğu düşünülmektedir (Bodeau vd., 2010). 15 Ocak 2020 tarihinde yayımlanan Küresel Riskler Raporu'nda, teknolojik sistemlere yönelik ciddi tehditleri ortadan kaldırmak için dünya liderleri, şirketler ve siyasete yön verenler arasında işbirliği yapılmasına her zamankinden daha fazla ihtiyaç duyulduğu öne sürülmüştür. Bu yılki raporda, diğer sorunların yanında teknoloji yönetişimindeki boşlukların etkilerine de odaklanıldığı açıkça belirtilmiştir (The Global Risks Report, 2020). Ancak Akyeşilmen'e (2018a) göre siber uzayı bir işbirliği değil, bir çatışma ve güç politikası platformu haline getirme gayesi güden bazı hırslı paydaşlar, siber yönetişim kavramını hırsları uğruna anlam kaybına uğratmayı göze almışlardır.

İnternet yönetişiminin tanımı hala oldukça tartışmalı olsa da, bu alanda yapılan çalışmalarda genel olarak devletlerin siber uzay meselelerine dahil olmaları gerektiği konusunda bir konsensüs mevcut iken, diğer taraftan bu alanda güçlerini sınırlamaları gerektiği vurgulanmaktadır. Bu noktada öne çıkan çalışmalardan ilki, John Perry Barlow'un 1996 yılında kaleme aldığı *A Declaration of the Independence of Cyberspace* adlı deklarasyondur. Deklarasyonda Barlow, devletlerin siber uzayı yasal süreçler yoluyla yönetme girişimlerini eleştirmiş ve siber alanın "tiranlardan" bağımsız olduğunu iddia etmiştir. Bu ünlü deklarasyon, hem teknoloji uzmanları hem de akademisyenler tarafından desteklenmiştir. Barlow, devletlere ve devlet kurumlarına seslenerek; "Mülkiyet, ifade, kimlik, hareket ve bağlamla ilgili yasal kavramlarınız burada geçerli değildir" ifadesini kullanmıştır. Negroponte (2004) ise, Barlow'a benzer ancak ondan daha idealist bir öneri sunarak, siber yönetişimin mevcut yapısının sağlıklı olmadığını ve bunu çözmenin yolunun interneti herkese ait bağımsız bir ulus olarak ele almaktan geçtiğini vurgulamıştır. Hatta interneti "BM üyesi" yapmak fikrini dahi ortaya atmıştır.

Bygrave ve Michaelsen (2009), yönetişim kavramının devletlerden çok daha fazlasını kapsadığını vurgulamışlardır. Benzer şekilde Levinson ve Marzouki'nin (2015) ortak çalışması da, internet yönetişiminin küresel boyutunu ve uluslararası kuruluşların bu alandaki rollerini ele almıştır. Bu çalışma, internet yönetişiminin çok yönlü ve karmaşık yapısını, çeşitli aktörlerin etkileşimini ve küresel internet yönetişimi ekosisteminde yaşanan değişimleri incelemiştir. Özellikle internet yönetişimi konusunda uluslararası kuruluşların genellikle göz ardı edilen rollerini vurgulamış ve bu alandaki çok paydaşlı yaklaşımların yükselişini analiz etmiştir.

Keller (2015) ise, özel sektörün küresel internet yönetişiminin yürütülmesi için daha uygun ve "ilkeli" olduğunu savunmuştur. Ona göre devlet düzeyinde ideolojik bölünmeler mevcut iken; özel sektörde işbirliği ve fikir birliği anlayışı mevcuttur. Buna örnek olarak, Çin'in en büyük online perakendecisi Alibaba'nın New York Borsası'ndaki halka arz edilmesinde iki ana hissedarının ABD menşeili şirket Yahoo ve Japonya menşeili Softbank olması durumunu göstermiştir.

Grewlich'e göre (2005) de "yönetişim" teriminin popülaritesi, uluslararası sistemin bir geçiş döneminde olmasıyla açıklanabilir. Ulus devlet küresel anlamda pozisyonunu korumasına rağmen uluslararası kuruluşlar ve özel sektör gibi devlet-dışı aktörlerin

yükselen trendiyle karşı karşıya kalmaktadır. Bu bağlamda Grewlich, "yönetişim" terimini devlet-dışı aktörlerin karma faaliyetlerine olanak tanıyan bir süreç olarak değerlendirmektedir. DeNardis (2014) de, çok sayıda aktörün internet tasarımında yer aldığına işaret ettiği çalışmasında internet yönetişiminin birincil görevinin ne olduğuna da değinmiştir. Ona göre interneti çalışır durumda tutmak için gerekli teknolojilerin tasarımı ve yönetimi, sağlam bir politika yürütmekten geçmektedir. Lessig (1999a) ise, internetin ne devlet ne de özel sektör tarafından değil, katkıda bulunanlar ve kullanıcılar tarafından yönetilmesi gerektiğini iddia etmiştir. Bu bağlamda Netanel (2000), sınırsız bir siber uzayın çoğunluğun azınlığı çiğneyebileceği bir ortam yaratacağına dikkat çekerek, bu durumun sivil topluma birçok yönden zarar vereceğini vurgulamıştır.

Bununla birlikte, en azından şimdilik devlet aktörünün siber uzayın yönetişimi konusunda baskın olduğunu iddia eden uzmanlar da mevcuttur (Yan, 2019). Drezner (2004), özel aktörlerin egemen olduğu kendi kendini yöneten bir siber uzayı savunan literatüre karşı çıkmakta ve küresel anlamda siber yönetişim için devletlerin hala birincil aktörler olduğunu iddia etmektedir. Sunstein (2001), internet kullanıcıları ve şirketler için devletin önemini vurgulamakta ve internet için özgür ortamı yaratacak olanın yine devlet olduğunu savunmaktadır. Chouchri'ye (2014) göre siber uzayın yaygınlığı ve küresel erişimi, onun özel sektör tarafından yönetilmesini gerektirmiştir. Siber alanı oluşturan fiziksel altyapının çoğu, vatandaşlar veya şirketlerin özel mülkiyetidir ancak protokolleri tanımlayan standartların belirlenmesinde devlet kurumları önemli bir rol oynamaktadır. Altyapının büyük bir kısmı özel sektöre ait olmakla birlikte, ulus-devletler kendi egemenliklerini, siber alanın yetki alanlarına giren fiziksel unsurları üzerinde kullanmaktadırlar.

Diğer yandan, bu çalışmanın üzerinde durduğu düzenleyici bir mekanizmanın olmaması durumunun yol açtığı anarşi seviyesine dikkat çeken çalışmalar da mevcuttur. *In Internet Governance: A Regulative Idea in Flux* adlı kitabında Hofmann (2007), küresel anlamda düzenleyici bir mekanizmanın olmamasını "düzenleyici boşluk" olarak nitelendirmiştir. Yönetişimi de bu boşluğu doldurmanın meşru, açık uçlu ve kolektif bir yolu olarak tanımlamıştır. Qian ve Zhang (2020) ise, küresel bir siber güvenlik işbirliği sisteminin inşasının önemini vurguladıkları çalışmalarında, siber tehditlere karşı devletlerararası ortak mücadeleyi ve siber uzayın etkili yönetişimini savunmuşlardır. Yazarlar, insanların karşılıklı bağımlılığını, çıkarların entegrasyonunu

ve siber uzayda devletlerarası etkileşimi, küresel siber güvenlik için işbirliği sistemi oluşturmanın temel iç mantığı olarak sunmuşlardır.

Kulesza (2012), internet yönetişimiyle ilgili uluslararası hukuki meseleleri ele aldığı çalışmasında internetin sorunlarına uluslararası bir çözüm önermiştir. Bu çalışma, internet yönetişimi için bir Uluslararası Çerçeve Sözleşmesi önererek, böylesi bir sözleşmenin uluslararası işbirliğinin başlangıç noktası olarak hizmet edebileceğini savunmuştur. Serrano (2019) tarafından yapılan bir incelemede ise, internetin uluslararası düzenlemesinin kapsamlı bir görünümü sunulmuş ve internetle etkileşim içinde olan veya internet üzerinden gerçekleşen faaliyetlere uygulanan uluslararası hukuk alanları belirlenmiştir. Bu çalışma, internetin küresel doğasını dikkate alarak, uluslararası hukukun bu yeni ortama uygulanmasının hem mümkün hem de gerekli olduğunu savunmuştur.

Kowack'ın (1997) çalışması, internetin ekonomik ve sosyal modellerinin, geleneksel yönetişim mekanizmalarına meydan okuyan ve daha kapsayıcı ve katılımcı bir yönetişim modeli talep eden bir küresel sivil toplumun ortaya çıkmasına yardımcı olduğunu savunmaktadır. Kowack'a göre bu yeni ortam, geleneksel sınırları aşan bir katılım ve etkileşim imkânı sunmaktadır. Carr (2015) tarafından yapılan analizde ise, katılımcı bakış açısının zorlukları ele alınmıştır. Carr, çok paydaşlı internet yönetişim modelinin meşruiyet ve hesap verebilirlik gibi konularda karşılaştığı zorlukları tartıştığı çalışmasında, bu modelin yönetişimi demokratikleştirmesi beklenirken; mevcut güç dinamiklerini pekiştirebilecek bir mekanizma olarak işlev görebileceğinin altını çizmiştir.

Öte yandan, çalışmada önerilen model olan IGF modelinin de bazı çalışmalara konu olduğu görülmektedir. Yapılan çalışmalarda özellikle IGF'nin konumuna yönelik pozitif bir vurgu göze çarpmaktadır. Creech vd. (2009) ve Cogburn'nun (2017) çalışmalarına göre IGF, internet yönetişimi konusunda diğer platform ve kuruluşlardan daha başarılı çok paydaşlı bir katılım sergilemektedir. IGF, çeşitli paydaş gruplarını bir araya getirerek ve internet yönetişimiyle ilgili kritik konularda diyalog ve işbirliğini teşvik ederek önemli başarılar elde etmiştir. Bu yaklaşım sayesinde, tekil kuruluşların veya bir sektörün tek başına ulaşamayacağı sonuçlara ulaşılmıştır. Epstein (2013) de, IGF'nin, çeşitli politik ilgi ve değerlerin bir arada var olabilmesine olanak tanıyan yeni yönetişim kurumlarının oluşumunda nasıl bir dönüm noktası teşkil ettiğini

incelemektedir. Bu forum, meşruiyet ve otorite kavramlarının, karmaşık bilgi sistemlerinin politika müzakereleri için yeniden tanımlandığı bir örnek olarak gösterilmiştir.

Türkçe literatüre gelindiği zaman ise, genel olarak internet yönetişimine yönelik özellikle son on yılda gelişen bir literatürün varlığı göze çarpmaktadır. Ancak yapılan çalışmaların neredeyse yüzde doksanının yönetişimin politik boyutundan çok teknik boyutuna odaklandığı söylenebilir. Öte yandan yapılan çalışmaların büyük çoğunluğu Kamu Yönetimi veya Bilişim Hukuku bağlamında çalışmalar olup, internet yönetişimini kapsamlı bir şekilde ele alan bir Uluslararası İlişkiler çalışmasına rastlanmamıştır. Yönetişim kavramı daha çok "e-devlet" çerçevesinde değerlendirilerek hukuki ve politik anlamda var olan kavramsal boşluk doldurulamamıştır.

Türkçe literatürde ilk olarak değinilecek çalışmalardan biri, her ne kadar ana konusu internet yönetişimi olmasa da, bu çalışmanın yaklaşımına en yakın çalışma olması gerekçesiyle Akyeşilmen'in kaleme aldığı *Disiplinlerarası Bir Yaklaşımla Siber Politika & Siber Güvenlik* adlı kitap olmuştur. Kitap, kapsamlı bir siber politika ve güvenlik çalışması olarak karşımıza çıkmaktadır. Politik unsurların siber uzaydaki etkileri üzerine analizlerin yapıldığı çalışmada, teknik ve politik siber yönetişim, siber hukuk ve IGF modeli de tartışılmıştır. Akyeşilmen, siber yönetişimi siber uzayın anarşik, karmaşık, küresel ve çok aktörlü yapısı nedeniyle bir "oksimoron hikayesi" olarak betimleme yoluna gitmiştir.

Çağdaş İnternet Yönetimi adlı raporunda Akdeniz (2004), siber yönetişimde çok-katmanlı bir yaklaşımın kaçınılmaz olduğunu savunmuştur. Türkiye örneğinden yola çıkan Akdeniz, ulusal alanda yapılan düzenlemelerin tek başına yeterli olmadığını, bunun yanında BM, Avrupa Konseyi, OECD, G8 gibi ulusüstü ve uluslararası kurumların politika geliştirmede belirleyici olması gerektiğinin altını çizmiştir. Burada *self-regulation* ve *co-regulation* kavramlarının önemine vurgu yapan Akdeniz, devlet düzenlemeleri ve yasalaştırmaya ek olarak, sivil toplum kuruluşlarının çalışmaları, sektörün ve toplumun rolü gibi olguların da sürece dahil edildiği, ifade özgürlüğü ve gizlilik gibi kişisel hakları tartışılmaz değerler olarak kabul edildiği "normatif" bir düzenin gerekliliğine dikkat çekmiştir. Bu noktada referans kaynağı olarak Avrupa İnsan Hakları Sözleşmesi, İnsan Hakları Evrensel Beyannamesi, BM Siyasi ve Medeni Haklar Sözleşmesi ve AB Temel Haklar Bildirgesi gibi insan haklarının temel

metinlerini göstermiştir. Bu temel belgelerin mahremiyeti ve ifade özgürlüğünü açıkça koruması, özellikle internetin doğasına da uygun düşmektedir. Bu çalışmada da insan haklarını esas alan bu metinlerin küresel yönetişim bağlamında hukuki süreçleri ne şekilde etkiledikleri irdeleneceğinden, Akdeniz'in hazırladığı bu rapor çalışmaya referans olması açısından önem arz etmektedir.

Haksever (2018) tarafından yapılan *İnternet ve Çok-Paydaşlı Yönetişimi* adlı tez çalışmasında, bilişim hukuku yöntemi ışığında; internetin teknik, teknolojik ve politik gelişimi; yönetişim, paydaş ve çok-paydaşlılık kavramları bağlamında açıklanmaya çalışılmıştır. İnternet ve çok-paydaşlı yönetişimin bugünkü halini almasını sağlayan neden-sonuç ilişkilerinin ortaya konulmaya çalışıldığı çalışmada politika konuları ikincil planda kalmış, teknik boyutun daha ağırlıklı işlendiği görülmüştür. Bununla birlikte çalışma, bir Bilişim Hukuku çalışması olması gerekçesiyle Uluslararası Hukuk alanına giren konuların irdelenmesi noktasında bir boşluk bırakmıştır.

Doğan ve Ustakara (2013) tarafından yazılan *Kamuda Bir Yapılanma Dönüşümü Olarak E-Devlet ve E-Yönetişim İlişkisi Üzerine* adlı makalede, bilgi teknolojilerinin devlet yapılanması üzerinde yarattığı etki, e-devlet ekseninde değerlendirilerek, yönetişim kavramı bu bağlamda açıklanmaya çalışılmıştır. Özer (2017) tarafından yazılan *Yönetişimden Dijital Yönetişime: Paradigma Değişiminin Teknolojik Boyutu* adlı makalede de yine benzer şekilde e-dönüşüm projesi, e-devlet ve e-demokrasi gibi uygulamalara öncelik verildiği görülmüştür. Parlak ve Doğan (2019) tarafından kaleme alınan *E-Yönetişim: Kavramsal/Kurumsal Çerçeve, Ülke İncelemeleri ve Türkiye'ye Yansımaları* adlı kitapta, dünyada e-yönetişim modelini uygulayan farklı devletlerin deneyimlerine yer verilmiştir. Özetle Türkiye'de e-yönetişimin uygulanabilirliği, farklı kamu kurumlarındaki uygulama deneyimleri ve e-devlet gibi konulara ağırlık verilmiştir.

Görüldüğü üzere genel olarak internet yönetişimi üzerine yapılan çalışmalarda benzer eğilimler söz konusudur. Çalışmaların büyük çoğunluğunda ilk olarak kavramın tanımı ve yapısı gibi bu alandaki temel konulara odaklanılmaktadır. İkincisi, politik meseleleri ele alan çalışmaların büyük çoğunluğu daha çok tehdit unsurlarına odaklanarak "güvenliği" merkeze alan bir bakış açısını benimsemişlerdir. Üçüncü olarak ise, kamu politikası konuları tartışmaya açılarak; bunların özgürlük, demokrasi, sosyoekonomik kalkınma ve uluslararası ticaret ile ilişkisinin internet yönetişimi üzerindeki sonuçları

incelenmiştir. Ancak bilhassa bir internet yönetişiminin küresel vurgusu, iyi yönetişim ilkelerinin uygulanmasının gerekliliği, normatif argümanların öne sürüldüğü yahut etkili bir hukuk mekanizmasının olasılıkları üzerine inşa edilmiş yekpare geniş kapsamlı bir çalışma olmadığı gözlenmiştir. Özellikle IGF'nin hukuki bağlayıcılığının olmadığına ve bunun kararları üzerinde olumsuz etkiler yarattığına vurgu yapan çalışmalar olsa da (Lahmann vd., 2017; Cogburn, 2017) IGF'ye hukuki bağlayıcılık kazandırılması için önerilerin geliştirildiği spesifik bir çalışmaya rastlanmamıştır.

BÖLÜM I: KAVRAMSAL VE KURAMSAL ÇERÇEVE: TANIM, YAKLAŞIMLAR, UNSURLAR, TEORİLER

Çalışmanın bu bölümünde, küresel dijital yönetişimin kavramsal ve kuramsal çerçevesi kapsamlı bir şekilde ele alınacaktır. Küresel dijital yönetişim tartışmalarının ne zaman ortaya çıktığı, üzerinde uzlaşmaya varılmış bir tanımı olup olmadığı ilk incelenecek konular arasındadır. Bunun yanında, dijital alanın kritik kaynaklarının veya teknik ve politik unsurlarının neler olduğu, bunların yönetişim sürecini ne ölçüde etkilediği irdelenecektir. Daha sonrasında yönetişim sürecinde etkili olan aktörlerin/paydaşların rolleri ve konumları kapsamlı bir biçimde aktarılacaktır. Son olarak, çalışmanın kuramsal çerçevesini belirleyecek olan "normatif teorinin" daha iyi anlaşılması için Uluslararası İlişkiler (Uİ) disiplininin ana akım teorilerinin küresel internet yönetişimine yönelik yaklaşımları ele alınacaktır.

1.1.Yönetişimi Anlamak: Tarihsel Arka Plan ve Kavramsal Analiz

1.1.1. Yönetişim ve Ortaya Çıkışı

Yönetişim kavramının gelişiminin incelenmesi, çalışmanın ileriki bölümlerinin anlaşılması açısından önem arz etmektedir. Dolayısıyla yönetişim kavramının anlaşılması hem tarihsel arka planın hem de kavramsal çerçevenin kapsamlı bir incelemesini gerektirir. Yönetişim kavramı her ne kadar yeni yeni popülerleşmeye başlamış olsa da esasen bu kavram insanlık tarihi kadar eskidir (Weiss, 2000, s. 795). Tarih boyunca küresel yönetişim, insanlığın politik, ekonomik ve sosyal zorluklarla başa çıkmak için geliştirdiği çeşitli sistemler ve kurumlar aracılığıyla kendini göstermiştir. Küresel yönetişimin evrimi, insanlık tarihi boyunca farklı dönemlerde ve farklı biçimlerde ortaya çıkmıştır. Bu durum genellikle mevcut politik, ekonomik ve teknolojik koşulların bir yansımasıdır.

Tarih öncesi dönemlerden itibaren, küresel yönetişimin temel taşlarını oluşturan birçok öncü fikir ortaya çıkmıştır. Dante Alighieri'nin 1311'de yazdığı *De Monarchia* adlı eseri, insanlığın birliğini, insan aklının mükemmelliğini, hukukun üstünlüğü altında özgürlüğün arzu edilirliğini ve şehir devletleri arasındaki anlaşmazlıkları çözmek için süper bir ulusal güce ihtiyacı olduğunu ileri sürer (Lopez-Claros vd., 2020). Bu, insanlığın geniş bir çerçevede düşünmeye ve sadakatlerini genişletmeye başladığının erken bir göstergesidir. 1693'te William Penn'in *Avrupa'nın Şimdiki ve Gelecekteki*

Barışı İçin Bir Deneme adlı makalesi ve Jean-Jacques Rousseau'nun Saint-Pierre'nin fikirlerini popülerleştirdiği çalışmaları, süper ulusal güçler ve hukukun üstünlüğü temelli bir düzenin önemini vurgular (Murphy, 2020; Spector, 2011).

Tarih öncesi dönemlerden itibaren ortaya çıkan bu öncü fikirler, yönetişimin temellerinin ve evriminin anlaşılması açısından elzemdir. İnsanlık tarihi boyunca farklı topluluklar ve medeniyetler, karmaşık sosyal, ekonomik ve siyasi sistemlerini düzenlemek ve yönetmek için çeşitli yöntemler ve mekanizmalar geliştirmişlerdir. Bu gelişmeler, güç, otorite ve meşruiyet kavramlarının nasıl anlaşıldığı ve uygulandığı konusunda derin bir etki yaratmıştır. Antik çağlardan modern devlete ve uluslararası ilişkilerin günümüzdeki karmaşık yapısına kadar yönetişim, toplumların nasıl organize olduğu, karar alma süreçlerinin nasıl işlediği ve bu süreçlerin zaman içinde nasıl evrildiği gibi konuları kapsar. Bu evrim, hem yerel hem de küresel düzeyde otorite ve güç yapılarının nasıl kurulduğu ve sürdürüldüğü hakkında önemli bilgiler sunar.

İnsanlık tarihi boyunca görülen bu evrimsel süreç, modern zamanlara ulaşmamızla birlikte daha karmaşık bir hal almıştır. Özellikle İkinci Dünya Savaşı'ndan sonra devletlerin ve yönetişim yapılarının rolü ve etkinliği, önceki dönemlere kıyasla daha fazla sorgulanmaya başlanmış ve eleştiriye açık hale gelmiştir. Zira İkinci Dünya Savaşı'ndan sonra devletler, politika geliştirme ve uygulamanın tek sorumlusu olarak görülüyordu. Geleneksel olarak devletler, toplumu yönetme ve kamu çıkarını belirleme konusunda tek yetkili otorite olarak kabul edilirdi. Bu dönemde devlet, ekonomiyi ve toplumu yönlendirme yeteneğine sahip güçlü bir aktör olarak tasvir ediliyordu. Devletin kamu çıkarını gözetmediği fikri tartışma konusu bile değildi. Ancak, 1970'ler ve 1980'lerde bu durum değişmeye başladı. Devletin yönlendirme kabiliyeti sorgulandı ve devlet davranışları eleştirel bir incelemeye tabi tutulmaya başlandı (Bauer, 2005, s. 3).

1970'lere dek Uİ disiplini, büyük ölçüde devletlerin eylemlerine odaklanmıştı ve uluslararası kurumlar, devletlerin araçları olarak kabul ediliyordu. Ancak 1970'lerin getirdiği küreselleşme dalgasıyla birlikte, devlet dışı faaliyetlerin önemi daha fazla vurgulanmaya başlandı ve uluslararası ilişkilerde ulusötesi etkileşimlerin rolü giderek arttı. Teknoloji, coğrafi ve sosyal mesafeleri azalttıkça, hâkim düzen giderek daha merkezi hale geldi ve dünyanın bir bölgesindeki faaliyetlerin yansımaları diğer bölgelere daha geniş bir şekilde ulaşmaya başladı (Rosenau, 1992, s. 13). Keohane ve

Nye, ulusötesi faaliyetlerin toplumları birbirine daha bağımlı hale getirerek, bu sürecin devletlerin çeşitli birimleri arasındaki bürokratik etkileşimleri ve politika koordinasyonu çabalarını artırdığını savunmuşlardır. Onların analizine göre bu dinamikler, uluslararası kuruluşlara dünya siyasetinde daha belirgin roller üstlenme fırsatı tanımaktadır. Bu perspektif, 1970'lerde uluslararası politikada giderek daha fazla dikkat çeken devlet dışı aktörlerin ve faaliyetlerin önemini ön plana çıkarmıştır. Bu dönemde, Uİ disiplininde geleneksel devlet merkezli yaklaşımlara karşı bir eleştiri oluşmuştur. Bu eleştirel yaklaşım, devletlerin artık uluslararası sahnede tek belirleyici güç olmadığı ve ulusötesi etkinliklerin dünya politikasını önemli ölçüde şekillendirdiği fikrine dayanmaktadır.

1980'lerde, devletlerin uluslararası arenada nasıl hareket ettiğini tanımlayan normlar ve kurallar bütünü olan rejimler ön plana çıktı. 1990'lara gelindiğinde, devletlerin yanı sıra uluslararası kuruluşlar, şirketler ve STK'ların etkisine dikkat çeken küresel yönetişim kavramı belirdi (Weiss & Ozgercin, 2009). Rosenau ve Czempiel'in *Governance without Government: Order and Change in World Politics* (1992) adlı eseri, küresel yönetişim teorisinde devrim yaratmış ve yönetişimin yalnızca devletlerin değil, aynı zamanda uluslararası kuruluşlar, ulusötesi şirketler ve sivil toplum kuruluşları gibi devlet dışı aktörlerin de önemli katkılarıyla gerçekleştiğini öne sürmüştür.

Günümüzde ise devletler, küresel sistemdeki en etkili aktörler olmaya devam etse de, devlet gücü artık piyasalar ve sivil toplum gibi diğer aktörlerle olan karmaşık ilişkilerle şekillenmektedir. Egemenlik, devletlerin hem ulusal sınırları içindeki hem de dışındaki faaliyetler üzerinde kontrol sağlama kapasitesi olarak yeniden tanımlanmaktadır. Aynı zamanda, özel sektör aktörleri kamu hizmetlerini üstlenerek giderek daha fazla kamu işlevi görmektedir. Uluslararası kuruluşlar, şirketler ve STK'lar, küresel yönetişimde önemli roller üstlenmektedir. Bu doğrultuda küresel yönetişimin analizi, devletler, piyasalar ve sivil toplum arasındaki dinamik ilişkileri ve dönüşümleri kapsamlı bir şekilde anlamayı gerektirir (Weiss & Ozgercin, 2009). Bu dönüşümün başlıca nedenleri arasında, küreselleşmenin hızlanması, yeni teknolojik gelişmeler ve sosyal hareketlerin yükselişi sayılabilir. Bu değişim, yönetişim kavramının da yeniden tanımlanmasına yol açmıştır. Yönetişim kavramı artık sadece devletleri değil, tüm paydaşları içeren bir süreç olarak anlaşılmaya başlanmıştır. Bu yeni anlayış, daha katılımcı ve şeffaf bir yönetişim anlayışına yönelimi temsil etmektedir. Dolayısıyla yönetişimin yeniden

tanımlanması, bu genişleyen aktör yelpazesinin ve etkileşimlerinin bir yansıması olarak ortaya çıkmaktadır.

Yönetişim, temelde "güç ve otoritenin kullanımı" olarak tanımlanır (DCAF, 2019, s. 7). Ancak yönetişimin artık bir güç uygulamasından daha fazlası olduğu belirtilmektedir (Kwiatkowska, 2016, s. 130). Genel anlamda yönetişim terimi, herhangi bir kuruluşun yönettiği kurallar dizisini belirtmek amacıyla özel, ticari ve kâr amacı gütmeyen kuruluşlar dahil olmak üzere geniş bir yelpazede kullanılabilir. Devlet, politika kararlarını alma ve uygulama yetkisine sahip iken; yönetişim ise, hem resmi hem de gayri resmî kurumlar tarafından yetkinin kullanımıyla ilgilidir. Yönetişim yapıları, devletin dışında da var olabilir. Örneğin, sivil toplum kuruluşları, şirketler ve hatta bireyler, yönetişim sürecine katkıda bulunabilir. Yönetişim, devletin yasama veya otorite gücüne dayanmaz. Aksine, katılım, işbirliği ve uzlaşma yoluyla çalışır (Juan & Martin, 2019, s. 98). Devletler, yasalar ve politikalar aracılığıyla değerleri otoriter bir şekilde dağıtırken; yönetişim, değerleri daha eşitlikçi ve katılımcı bir şekilde dağıtmaya odaklanır (Czempiel, 1992, s. 250).

Rosenau (2000) yönetişimi, devlet kurumları ile sınırlı olmayan, aynı zamanda gayrı resmi ve devlet dışı mekanizmaları da kapsayan daha geniş bir olgu olarak tanımlar. Rosenau'ya göre, ulusötesi sorunlar, tek bir devletin veya devlet sisteminin tek başına çözebileceği sorunlar değildir. Bu sorunların çözümü, devletler, devlet dışı aktörler ve uluslararası örgütler arasındaki işbirliğine dayanan ortak çözümler gerektirir. Rosenau, yakın gelecekte, farklı ulusötesi kolektivitelerden oluşan parçalı bir sisteme sahip olacağımızı öngörmektedir. Bu sistemde devletler, devlet dışı aktörler ve uluslararası örgütler, ulusötesi sorunları çözmek için birlikte çalışacaktır.

Yönetişim, aynı zamanda, siyaset ve politika oluşturma konusundaki bilimsel perspektifleri genişletmek için kullanılan bir terimdir. Bu terim, devletin toplumu yönetme ve organize etmede tek aktör olmadığını kabul eder. Modern toplumlarda devlet, topluluk ve piyasa ile karşılıklı olarak bağımlı bir durumdadır. Bu üç aktör, karmaşık şekillerde etkileşime girer ve birbirlerinin çözülmemiş sorunlarından giderek daha fazla etkilenir. Bu açıdan devlet, yönetim sürecinin yalnızca bir biçimidir (Adams vd., 2015, s. 27). Bugün modern toplumlarda devlet dışı aktörler, politika sonuçlarını etkilemede artan bir rol oynamaktadır. Bu, devletin rolünü ve toplumla ilişkisini değiştirmektedir. Devlet dışı aktörler, bireyler, gruplar, kuruluşlar ve şirketler olabilir.

Bu aktörler, politika oluşturma sürecine çeşitli şekillerde katılabilirler. Örneğin, kamuoyu oluşturabilir, lobi faaliyetleri yapabilir veya politikaları uygulamaya yardımcı olabilirler. Devlet dışı aktörlerin artan rolü, geleneksel politikanın strateji ve araçlarının etkinliğini ve meşruiyetini sorgulatmaktadır. Bu aktörler, devletin geleneksel rolünü sınırlayabilmekte ve yeni politika yaklaşımlarının geliştirilmesini gerektirebilmektedir (Juan & Martin, 2019, s. 124).

Yönetişim, insanların devletle ve devletin insanlarla nasıl etkileşime girdiğini şekillendirdiğinden, siyasi süreçleri ve kamu kurumlarının işleyişini de etkiler. Ancak yönetişim, yalnızca siyasi süreçleri ve kamu kurumlarını değil, sosyal hayatın diğer alanlarını da etkilemektedir. Yönetişim, özel sektörde, sivil toplumda ve hatta internet gibi yeni alanlarda ortaya çıkabilmektedir. Özel şirketler, hissedarlar, direktörler ve yöneticiler arasında süregelen etkileşimler yoluyla yönetilir. Bu etkileşimler, şirketlerin yönetimi ve işleyişini etkiler. Sivil toplum kuruluşları da, kamu ve özel kuruluşların gündem ve programlarını şekillendirmede giderek daha fazla rol oynamaktadır. Bu durum, ekonomik ve sosyal hayatın her alanında bir yönetişim boyutunun olduğunu göstermektedir (WGIG, 2005).

Yönetişim, öte yandan, fırsatları kontrol etmek ve yaratmak anlamına da gelir. Bu, yalnızca güçle ilgili değil, aynı zamanda sorunlara odaklanmakla da ilgilidir (Kwiatkowska, 2016, s. 130). Yönetişim, kuralların oluşturulması ve uygulanmasına yönelik anlayışları, beklentileri ve kurumları ifade eder. Uluslararası düzeyde ise, devletler ve vatandaşları arasındaki ilişkilerin etkileşimlerinde öngörülebilirlik sağlamak için bir çerçeve sağlanması anlamına gelir (Lewis, 2013, s. 2). Bu yönüyle yönetişim, karmaşık sistemlerin nasıl işlediğini ve geliştiğini anlamanın önemli bir parçasıdır. Bu bağlamda ortaya çıkan rutin faaliyetler, bir sistem düzgün çalıştığında ortaya çıkan faaliyetleri ifade eder. Ancak, sistemler beklendiği gibi çalışmadığında, rutin faaliyetlerin revize edilmesi veya değiştirilmesi gerekebilir. Bu, "kritik anlar" olarak adlandırılan durumlarda olur. Yönetişim, bu kritik anlarda ortaya çıkan koordinasyon sürecini ifade eder (Hofmann & Katzenbach & Gollatz, 2017, s. 1415).

Bu süreç, sistemdeki tüm paydaşların katılımını ve işbirliğini gerektirir. Yönetişim, sistemlerin istikrarını ve sürdürülebilirliğini sağlamaya yardımcı olur. Örneğin, bir şirkette rutin faaliyetler, üretim, satış ve müşteri hizmetleri gibi faaliyetleri içerir. Ancak şirket, yeni bir pazara girerken bu faaliyetler yeni koşullara uyarlanmalıdır. Bu,

yeni pazar araştırması yapılmasını, yeni satış stratejileri geliştirilmesini ve yeni müşteri hizmetleri politikalarının oluşturulmasını gerektirebilir. Bu durum şirket için kritik bir andır ve bu kritik anda ortaya çıkan koordinasyon sürecine "yönetişim" denir.

Bütün bu yönleriyle yönetişim, siber alan gibi yeni alanlarda da önemli bir rol oynamaya başlamıştır. Ancak yönetişim kavramının kendisinin hala gelişmekte olan bir kavram olduğu ve çok çeşitli tanımlarının olduğu unutulmamalıdır. Bu tanımların çeşitliliği, yönetişimin kavramsallaştırılması sorununun bir sonucudur. Ancak kavramın tanımlanmasında genellikle ortak bir nokta dikkat çekmektedir: Kavram olarak yönetişim, hiyerarşi ve komuta zorunluluğuna dayanmayan bir sosyal yönlendirme biçimini ifade eder. Yönetişimde çoğu zaman farklı çıkarları, değerleri ve güçleri olan çok sayıda aktörün etkileşimi söz konusudur (Koenig-Archibugi, 2011, s. 393). Yönetim yapıları ve süreçlerini inceleyen araştırmalar, yönetişimi daha iyi anlamamıza yardımcı olmuştur. Ancak bu araştırmalar aynı zamanda yönetişimin karmaşıklığını ve yönetişim ile ilgili pratik sorunları da ortaya çıkarmıştır. Modern toplumlar ilerledikçe ve değiştikçe, yeni zorluklar ortaya çıkmaktadır. Siber güvenlik de geleneksel yönetişim yapıları ve süreçleri ile ele alınması zor olan bir olgudur. Zira internet ile ilgili birçok farklı süreç, yönetişim tarafından şekillendirilir. Bu süreçler arasında teknik standartların geliştirilmesi, temel kaynakların yönetişimi ve internetin kötüye kullanımının ve suistimalinin düzenlenmesi yer alır. Dolayısıyla yönetişim, siyasi süreçleri ve kamu kurumlarını etkilemenin yanı sıra, sosyal hayatın diğer alanlarını ve hatta yeni alanları da etkiler (WGIG, 2005). Bu tür zorluklar, daha rafine ve spesifik yönetişim kavramlarına duyulan ihtiyacı göstermektedir (Adams vd., 2015, s. 29). Bu nedenle yönetişim teriminin tanımı, yalnızca devleti değil, bütün paydaşları içine alacak şekilde genişletilmelidir (van der Spuy, 2017, s. 16).

1.1.2. Yönetişimin Küreselleşmesi: Küresel Yönetişim

Küresel yönetişimin iki farklı anlamı olduğu belirtilmektedir. Birincisi, küreselleşme sürecini kontrol etmek amacıyla küresel ölçekte bir politika uygulama yoludur. İkincisi, küresel yönetişim sürecinin içinde yer alan yapıları ifade eder. Küresel yönetişim yapıları hem aktörleri hem de onları birbirine bağlayan ilişkileri içerir. Bu ilişkiler, aktörlerin sistemdeki konumlarını tanımlar ve aynı zamanda sistemin kendisini de oluşturur. (Kwiatkowska, 2016, s. 130). Yönetişimin küreselleşmesi ise, ulusal sınırların ötesine geçen karmaşık sorunlara çözüm bulma gerekliliğiyle ortaya çıkmış

bir fenomendir. Küresel yönetişim, ulus-devletlerin yanı sıra çok sayıda uluslararası kuruluş, sivil toplum örgütleri, özel sektör temsilcileri ve diğer paydaşların katılımıyla, küresel düzeyde karşılaşılan meseleleri ele alır. Bu kavramın yükselişi, ekonomik küreselleşme, çevresel sorunlar, transnasyonel suçlar ve pandemiler gibi sınır tanımayan zorlukların artmasıyla paralellik gösterir.

Böyle bir ortamda küresel yönetişim, geleneksel Uİ teorilerinin ötesine geçerek, küresel sorunlara çok boyutlu ve katılımcı bir yaklaşım sunar. Bu süreç, güç ve otoritenin yeniden yapılandırılmasını gerektirirken, uluslararası işbirliğinin ve koordinasyonun önemini vurgular. Küresel yönetişimin ortaya çıkışı, aynı zamanda devletlerarası sistemlerin nasıl işlediği ve küresel politik ekonominin nasıl yönlendirildiği hakkında yeni sorular ve tartışmaları da beraberinde getirmiştir. Özellikle 1990'ların sonlarına doğru, devletlerarası işbirliğine ve Westphalia egemenliğine dayalı geleneksel sistemin daha kapsayıcı ve katılımcı bir yapı olan küresel yönetişim sistemine doğru önemli bir dönüşüm yaşaması, küresel yönetişim sisteminin köklü değişimine dair tartışmaları gündeme getirmiştir (Zürn, 2018b, s. 1).

Küresel yönetişim literatürü, genellikle dünya siyasetinin değişimine göndermelerde bulunur. Ancak tam olarak neyin değiştiği, genellikle belirsiz kalır. Küresel yönetişim, uluslararası siyasi ve ekonomik ilişkilerdeki neo-liberal paradigma değişiminin bir ürünüdür. Sermaye ve piyasa mekanizmalarının devlet otoritesi üzerinde sağladığı üstünlük, özel sektör ve sivil toplum aktörlerini daha önce devletin yetki alanı olarak kabul edilen rolleri üstlenmeye teşvik etmiş ve bu durum, birtakım yönetişim boşlukları yaratmıştır (Jang & McSparren & Rashchupkina, 2016, s. 1).

Zürn (2018b), yönetişimin evrimi ve dinamiklerini anlamak için uluslararası otoritenin tarihsel evrimine odaklanmıştır. İkinci Dünya Savaşı'ndan sonra gelişen liberal düşüncenin ve bu düşüncenin desteklediği kurumların mevcut küresel yönetişim yapısını nasıl şekillendirdiğini anlatmıştır. Bu kurumlar zamanla güç kazanırken, aynı zamanda tartışmaların odağı haline gelmişlerdir. Zürn, yönetişim sisteminin devlet merkezli yapıdan, çok aktörlü bir yapıya evrildiğini ifade etmektedir. Zürn'e göre böylesi bir yönetişim sistemi, özellikle "yetki alanları" bağlamında karmaşıklığa sebebiyet vermiştir. Berlin Duvarı'nın yıkılması ve ardından gelen siyasi değişiklikler, uluslararası örgütlerin artması, yeni normlar ile yasal yapıların oluşturulması gibi olaylar, küresel yönetişimin genişlemesine ve derinleşmesine önayak olmuştur. Zürn,

bu genişleyen yapı içinde meşruiyet, otorite ve itiraz arasındaki süregelen daimî gerginliğe dikkat çekmiştir.

Deborah vd. (2010), uluslararası sistemde kırılma meydana getiren dört değişikliğin devlet dışı aktörlerin önemini artırdığına işaret etmiştir. Bunlar sırasıyla; (i) küreselleşme, (ii) özelleştirme ve devlet denetimini kaldırma, (iii) yeni teknolojiler (iv) Soğuk Savaş'ın sona ermesi. Küreselleşme, devlet sınırlarını ortadan kaldırırken, özelleştirme ve devlet müdahalesinin ortadan kaldırılması gücün devlet dışı aktörlere aktarımını kolaylaştırmıştır. Öte yandan yeni teknolojiler iletişimi ve nüfus akışlarını kolaylaştırırken; Soğuk Savaş'ın sona ermesi iki kutuplu sistemin dayattığı kısıtlamaları ortadan kaldırmıştır. Gerçekten de bugünkü yönetişim manzarası, çok sayıda aktörün şekillendirdiği bir sistemi işaret etmektedir. Devletler, uluslararası kuruluşlar, sivil toplum kuruluşları, çok uluslu şirketler ve sivil toplum grupları gibi pek çok aktör siyasi sistemin yönlendirilmesinde rol oynamaktadır. Bunlar, küresel yönetişim sisteminin karmaşıklığına sebebiyet verirken; aynı zamanda iyi yönetişim unsurlarının güçlendirilmesini de sağlamaktadır. Zira bugün küresel yönetişimin aktörleri, faaliyetlerin kapsamını genişletmekte ve aynı zamanda küresel meseleleri ele almada etkileşim ve işbirliğini benimsemektedir. Bunun yanında, mevcut küresel yönetişim düzenlemeleri, katılık yerine esnekliği tercih etmektedir. Aynı zamanda gönüllü eylemleri bağlayıcı kurallara tercih ederken; bireysel eylemler yerine ortaklıkları seçmekte ve yeni girişimler ve fikirleri desteklemektedir (Jang vd., 2016, s. 2).

Görüldüğü üzere küresel yönetişim sistemi, devletlerin yanı sıra sivil toplum kuruluşları, ulusötesi şirketler ve diğer toplumsal aktörlerin de katılımıyla karakterize edilen, daha karmaşık bir yapıdır. Bu sistem, normatif ilkeler, kurumsallaşmış otorite ve meşrulaştırma anlatıları ile desteklenmektedir. Küresel yönetişim sistemine doğru bu geçiş, uluslararası ilişkilerde paradigma değişikliğine işaret eder. Bu yeni sistem, eski devlet merkezli yaklaşımların ötesine geçerek, çok aktörlü bir sahnede daha dinamik ve esnek bir yapı sunar. Bu geçişin ana itici güçleri arasında ekonomik küreselleşme, teknolojik ilerleme, çevresel sorunlar ve sürdürülebilir kalkınma ihtiyacı, ulusötesi şirketlerin ve sivil toplumun yükselişi ve normatif ilkelerin evrenselleşmesi yer alır. Bu faktörler, daha işbirlikçi ve kapsayıcı bir uluslararası düzen ihtiyacını ortaya koymuştur (Zürn, 2018b, ss. 1-2). Sonuç olarak küresel yönetişim, küresel ölçekte karşılaşılan sorunları çözmek için uluslararası aktörler arasında işbirliği ve koordinasyon anlamına

gelir. Bu aktörler arasında devletler, uluslararası kuruluşlar, sivil toplum kuruluşları ve özel sektör şirketleri yer alabilir.

1.1.3. Küresel İyi Yönetişim

Yönetişim, ulusal devletlerin bölgesel alanlar üzerinde yürüttükleri bir faaliyetten daha fazlasıdır. Yönetişim, yalnızca devletleri ve geleneksel uluslararası kuruluşları değil, aynı zamanda sivil toplum kuruluşlarını ve diğer devlet dışı aktörleri de içeren uluslararası, devletlerarası ve ulusötesi bir faaliyete dönüşmektedir. Ülkeler ve bölgeler arasında büyük farklılıklar söz konusudur. Bölgesel işbirliği daha çok Batı Avrupa'da gelişmiştir. Ancak genel olarak, ulus devlet bağlamında algılanan yönetişim anlayışından çok düzeyli yönetişim anlayışına doğru bir evrim süreci gerçekleşmektedir (Aydınlı & Rosenau, 2005, s. 86). Bu bağlamda, "iyi yönetişim" kavramının ortaya çıkışı, yönetişim pratiklerindeki bu evrimsel değişimin doğal bir sonucu olarak görülebilir.

İyi yönetişim kavramı, siyasi örgütlenmeyle birlikte ortaya çıkmış ve tarih boyunca farklı şekillerde yorumlanmıştır. 1980'lerin sonlarında iyi yönetişim kavramı, sosyal ve ekonomik kalkınma alanındaki tartışmalara dahil edildi. Dünya Bankası (2006), iyi yönetişimin ekonomik kalkınma reformlarının başarısını mümkün kılacak ve kolaylaştıracak bir gereklilik olduğunu savundu. Dünya Bankası'na göre iyi yönetişim, devletin gücünün "öngörülebilir, açık ve aydınlanmış politika oluşturma" için kullanılmasıdır. Bu, devletin karar alma süreçlerinde şeffaf ve hesap verebilir olması, yasalara bağlı olması ve vatandaşların çıkarlarını gözetmesi anlamına gelir. UNDP (1997), iyi yönetişimin dokuz özelliğini belirlemiştir: katılımcılık, fikir birliği odaklılık, hesap verebilirlik, şeffaflık, duyarlılık, etkinlik ve verimlilik, adalet, hukukun üstünlüğü ve stratejik vizyon. Bu özellikler, iyi yönetişimin demokratik ve şeffaf bir yönetişim anlayışı olduğunu vurgular.

İyi yönetişim kavramı, Dünya Bankası tarafından geliştirilmiş ve daha sonra uluslararası kalkınma alanında yaygın olarak benimsenmiştir. Dünya Bankası, yönetişimde şeffaflığın arttığı, yolsuzluğun azaldığı ve verimliliğin artırıldığı bir ortamın teşvik edilmesi amacıyla "iyi yönetişim" terimini kullanmaktadır (Kurbalija, 2016, s. 279). Bu terim, kurumun dünya genelinde desteklediği politika ve reformların temelini oluşturur. Kavram, kamu yönetiminin şeffaflık, hesap verebilirlik, katılımcılık, hukukun üstünlüğü ve etkinlik gibi temel ilkeler temelinde yürütülmesi gerektiğini

vurgulamaktadır. İyi yönetişim kavramının ilk olarak tartışıldığı Dünya Bankası yayını, 1989 tarihli "Sahra Altı Afrika'da Kalkınma için Yeni Yönler" adlı raporudur. Bu raporda Dünya Bankası, Sahra Altı Afrika ülkelerinin kalkınmasını engelleyen temel sorunlardan birinin kötü yönetişim olduğunu savunmuştur. Kısa bir süre sonra iyi yönetişim kavramı, diğer uluslararası kuruluşlar ve Batılı devletler tarafından da benimsenmiştir. Bu kurumlar, iyi yönetişimi, kalkınmayı desteklemenin ve yoksulluğu azaltmanın önemli bir yolu olarak görmektedir (Demmers vd., 2004, ss. 4-5).

Son yıllarda, özellikle gelişmekte olan ülkelerde ekonomik ve idari reformların teşviki için iyi yönetişim kavramına daha fazla vurgu yapılmaya başlanmıştır. Bu kapsamda BM, Dünya Bankası ve diğer uluslararası kuruluşlar tarafından iyi yönetişimin temel ilkelerinin benimsenmesi için çeşitli programlar ve projeler yürütülmektedir. Hepsinin ortak noktası, iyi yönetişimin; vatandaşların ihtiyaçlarına ve beklentilerine cevap veren, şeffaf, hesap verebilir, katılımcı, etkin, ademi merkeziyetçi ve adil bir yönetişim anlayışını temsil ettiğidir. Bu bağlamda iyi yönetişimin temel unsurları şu şekilde özetlenebilir:

1. *Şeffaflık*: Vatandaşların kendilerini etkileyen kararların nasıl alındığını bilmeleri gerekir. Bu, karar alma sürecinin şeffaf ve hesap verebilir olmasını gerektirir.
2. *Hesap verebilirlik*: Devlet, vatandaşlarına karşı sorumlu olmalıdır. Bu, kamu görevlilerinin performansının değerlendirilmesi ve hesap sorulması anlamına gelir.
3. *Katılımcılık*: Vatandaşların karar alma sürecine aktif olarak katılmaları gerekir. Bu, vatandaşların görüşlerinin ve ihtiyaçlarının dikkate alınmasını sağlar.
4. *Etkinlik*: Devlet, kaynakları verimli bir şekilde kullanmalı ve hedeflerine ulaşmalıdır.
5. *Ademi merkeziyetçilik*: Yetkilerin merkezi yönetimden yerel yönetimlere devredilmesi, devlet eylemlerinde etkinlik ve katılımı artırabilir.
6. *Adalet*: Devlet, yasalara ve düzenlemelere uygun bir şekilde hareket etmeli ve vatandaşların haklarını korumalıdır (Patel, 2013).

Küresel yönetişim, toplumsal ya da küresel yapıları belirleyen mekanizmalarla ilgilidir (Komesar, 2014, s. 1). Küresel iyi yönetişim ise, dünya genelinde karşılaşılan

zorluklara etkili, adil ve sürdürülebilir çözümler üretmeyi hedefleyen bir yönetişim anlayışını ifade eder. Bu kavram, yönetişim süreçlerinin şeffaflığı, hesap verebilirliği, katılımcılığı, hukukun üstünlüğü ve insan haklarına saygı gibi temel ilkeler üzerine inşa edilmiştir. Küresel iyi yönetişim, uluslararası toplumu karmaşık küresel sorunlar karşısında ortak hareket etmeye ve çok paydaşlı işbirliği mekanizmalarını güçlendirmeye teşvik eder. Bu yaklaşım, çevresel sürdürülebilirlikten ekonomik kalkınmaya, sosyal adaletten barışın korunmasına kadar geniş bir yelpazedeki küresel meselelerin çözümünde kritik bir role sahiptir. Küresel iyi yönetişim anlayışı aynı zamanda, küresel yönetişim mekanizmalarının etkinliğini artırarak uluslararası toplumun karşılaştığı zorluklara daha hızlı ve etkili yanıt verme kapasitesini güçlendirme amacını taşır. Sürdürülebilir Yönetişim Göstergeleri (SGI),[2] OECD ve AB üyesi 41 ülkeyi karşılaştırarak, sürdürülebilir politikaların, sağlam demokrasilerin ve iyi yönetişimin yaygınlığını ve kalitesini ölçtüğü raporlarda bu amacın gerekliliğini sıklıkla vurgulamaktadır (SGI, t.y.).

Bu alandaki araştırmalar çoğunlukla yönetişimin nihai amacının "yönetilen varlığı kontrol etmek" olmadığı sonucuna varır. Bunun yerine, mümkün olabildiğince ortak işleri düzenlemektir. Yönetişim süreci, işbirliğine dayalı bir düzenleme için çeşitli aktörlerin farklılıklarını yönetir. Bu amaca ulaşmak için gerekli olan ise yönetişimde düzenin oturtulmasıdır. Dolayısıyla iyi yönetişimin esas amacının daha fazla demokrasi olduğu söylenebilir (Nanz & Steffek, 2004, s. 322).

"Yönetişim, güven ve itimat inşa etmek için bir araçtır" (Mahmood, 2017, s. 22). İyi yönetişim, sistemdekilere zaman, emek ve diğer kaynaklara yapılan yatırımların boşa gitmeyeceği konusunda güven verir. İyi yönetişim, iyi fikirlerin alınmasını ve kullanılmasını teşvik ederken kötü fikirlerin ortadan kaldırılmasını amaçlamaktadır. Bu nedenle iyi yönetişimin anlaşılması ve takip edilmesi kolaydır. Aynı zamanda kötüye kullanıma karşı dayanıklı olacak açık ve şeffaf kurallar ve süreçler gerektirir. Buna karşılık, sağladığı demokrasi ile yönetişim sisteminin kabulünü ve meşruiyetini arttırır (Ang & Haristya, 2015, s. 124).

[2] SGI, OECD ve AB ülkelerinde sürdürülebilir yönetişimin en kapsamlı araştırmasını yürüten kuruluştur. Kuruluş, iyi uygulamaların yaygınlaştırılması için savunuculuk faaliyetleri yürütmektedir. SGI'nin veri seti, sürdürülebilir yönetişimin çeşitli boyutlarını ölçen kapsamlı bir veri kümesidir. Kuruluş, bu veri setini araştırmacılar, politika yapıcılar ve diğer paydaşlar ile paylaşarak, yönetişim alanındaki yenilik ve reformları desteklemektedir. Ayrıntılı bilgi için bkz: SGI. (t.y.). Data Analysis. https://www.sgi-network.org/2022/Data_Analysis (20.10.2023).

Daha önce birbirlerine şüpheyle ve rakip olarak bakan aktörler olan devletler ve STK'lar arasında yakınlaşan çıkarlar gözlemlenebilir. Bu, iyi yönetişimin teşvik edilmesi gibi küresel ölçekte ortak çıkarların olduğu alanlarda özellikle belirgindir. Küresel bir pazarda faaliyet gösteren uluslararası şirketler de iyi yönetişimin teşvik edilmesine katkıda bulunmaktadır. Bu şirketler, çalışanlarının haklarını korumak, çevreyi korumak ve yerel topluluklara fayda sağlamak için sosyal ve etik sorumluluklarını yerine getirmeye giderek daha fazla odaklanmaktadır. Bu bağlamda sivil toplum inşası veya iyi yönetişimin teşvik edilmesi, tek bir ülkeden gelen bir faaliyetle sınırlı kalmamalıdır. Bu tür girişimler, çok paydaşlı işbirliği ve ortak çaba gerektirir (Melissen, 2005, ss. 12-14). Devletler, STK'lar ve uluslararası şirketler, iyi yönetişimi teşvik etmek için birlikte çalışarak daha adil, barışçıl ve sürdürülebilir bir dünya yaratmaya yardımcı olabilirler.

1.2.Küresel Dijital Yönetişim

1.2.1. İnternet ve Ortaya Çıkışı

İnternet, Soğuk Savaş'ın tırmanışa geçtiği bir dönemde, iki kutuplu dünya düzeninin yarattığı rekabet ortamında, bir ülkenin bilimle öne çıkma isteğinden türemiş bir ağdır. 1960'lı yıllara gelindiğinde ABD ile SSCB arasındaki ilişkiler oldukça soğuktu. SSCB 1957'de Sputnik uydusunu fırlatarak ABD'de "bilim açığı" konusunda alarma yol açtı ve devletin bilim ve teknolojiye yatırımında artışı beraberinde getirdi (Abbate, 1999, ss. 8-9). Soğuk Savaş dönemindeki bu teknolojik yarış ve bilimsel rekabetin çıktısı olarak ortaya çıkan internet, zamanla sadece askeri ve stratejik bir araç olmanın ötesine geçmiştir.

İnternet, genel olarak karmaşık ve çok katmanlı bir fiziksel altyapıdır (Schewick, 2010, ss. 83-90). "İnternet" terimi ilk kez 1974 yılında öncü bilgisayar bilimcisi Vint Cerf tarafından tek bir küresel ağı tanımlamak için kullanıldı (Venables, 2021, s. 3). TCP/IP aracılığıyla birbirine bağlanan bir bilgisayar ağı olan internet, 1970'lerde Soğuk Savaş için deneysel, bilimsel ve teknolojik projelerle görevlendirilen ABD Savunma Bakanlığı tarafından geliştirildi. İlk adım olarak, 1958 yılında ABD Savunma Bakanlığı İleri Araştırma Projeleri Ajansı (ARPA) kurulmuştur (Abbate, 1999, s. 36). Projenin amacı, araştırma kaynaklarının Sputnik'in 1957'deki ilk lansmanına kadar Sovyetler Birliği'ne karşı teknolojik askeri üstünlük elde etmek amacıyla seferber edilmesiydi. Bu doğrultuda internetin öncüllerinden biri olan ARPANET, 1969 yılında ARPA

tarafından kurulmuştur (Castells, 2001, s. 10). 1970'li ve 1980'li yıllarda ARPANET, ABD ve Avrupa'da ortaya çıkan diğer bilgisayar ağlarına bağlanarak büyümüş ve uluslararası bir hizmet haline gelmiştir. Ağ genişledikçe, ABD ordusu tarafından kullanılan bileşenleri dallara ayrılmış ve ağın geri kalan kısmı araştırmaya ayrılmıştır (Leiner vd., 1997, ss. 102-108).

ARPANET, 1970'ler ve 1980'lerde dünya çapında geliştirilen birkaç ağdan biriydi. Diğer ağlar; SSCB'de OGAS; Fransa'da CYCLADES ve Minitel; ve Şili'de Project CYBERSYN olarak sıralanabilir (Budnitskiy, 2018, s. 75). Özellikle Fransa'daki CYCLADES, ARPANET'e teknik tasarım özellikleri bakımından önemli bir ilham kaynağı olmuştur (Bory, 2020, s. 8). Bununla birlikte internet, farklı üreticilerin cihazları ve ağları arasında çeşitli fiziksel özelliklerde ara bağlantıya izin veren ilk ağdır. Bu yönüyle internet, küresel anlamda kabul gören ilk ağ olmuş ve o zamandan bu yana dünyanın en büyük dijital ağına dönüşmüştür.

1980'ler boyunca internet, ağırlıklı olarak ABD'de olmasına rağmen hızla popülerleşti (Abbate, 1999, s. 181). O dönemde internet yönetişimi ulusal devletlerin açık katılımı haricinde hala teknik bir mesele olarak algılanıyordu. Bunun üzerine ARPANET topluluğunun kilit figürleri tarafından bazı kuruluşlar oluşturulmaya başlandı. 1980'li yıllardan itibaren birbirine bağlı kâr amacı gütmeyen kuruluşlar, internet standartlarının ve politikalarının araştırma ve geliştirilmesinden sorumlu hale geldi (DeNardis, 2014, s. 42). Bu dönemde geliştirilen IETF gibi kuruluşlar hala internetin temel protokolleri[3] üzerindeki nihai yetkisini korumaktadır. Bu bağlamda 1980'lerin, internetin sadece bir bilim ve araştırma projesi olmaktan çıkıp geniş kitleler tarafından benimsendiği ve yaygınlaştığı bir dönem olduğu söylenebilir. Bu süreçte internetin yönetişimi ve standart belirleme faaliyetleri önem kazanmış, teknik topluluklar ve kâr amacı gütmeyen organizasyonlar bu yeni dijital ortamın şekillendirilmesinde kritik roller üstlenmiştir.

Görüldüğü üzere internet, fiziksel ve siber unsurlardan oluşan karmaşık bir sistemdir. Bu nedenle, mevcut politika ve yönetişim mekanizmalarını zorlaştırır. İnternet, ülkeye göre farklılık gösteren ideolojiler ve yönetim yapıları tarafından şekillendirilir. Bu, devletlerin yanı sıra özel aktörlerin de internet politikası oluşturmasına neden olur. İnternetin temelini oluşturan protokoller, ağların birbirleriyle iletişim kurmasını sağlar.

[3] Bu protokollere ve internetin işleyişine dair tüm detaylar çalışmanın ikinci bölümünde yer alan "2.1.1.Teknik Sorun Alanları" başlığı altında kapsamlı bir şekilde incelenmiştir.

Bu protokoller, özel kuruluşlar veya kamu kurumları tarafından kontrol edilebilir (Zangl, 2021, s. 3).

Küresel dijital yönetişim, internetin ortaya çıkışı ve bu yeni ortamda etkileşim, bilgi paylaşımı ve yönetişim mekanizmalarının nasıl şekillendirileceği sorusunun giderek artan önemiyle yakından ilişkilidir. İnternet, 20. yüzyılın son çeyreğinde bilgi ve iletişim teknolojilerinde yaşanan devrimin bir ürünü olarak ortaya çıktı ve kısa sürede küresel iletişim, ticaret, eğitim ve siyasetin yapılandırılmasında merkezi bir rol oynamaya başladı. Bu dijital platform, coğrafi ve kültürel sınırları aşarak, insanları ve kurumları önceki dönemlerde mümkün olmayan yollarla birbirine bağladı. İnternetin ortaya çıkışı, aynı zamanda yönetişim kavramının dijital çağda nasıl uygulanacağına dair yeni soruları da beraberinde getirdi. Dijital ortamda kimin ne üzerinde kontrol sahibi olduğu, nasıl bir düzenleme ve denetim mekanizmasının oluşturulacağı, veri güvenliği ve gizliliğinin nasıl korunacağı gibi konular, küresel dijital yönetişimin temel meseleleri haline geldi. İnternetin ortaya çıkışıyla başlayan bu süreç, dijital çağda küresel yönetişimin nasıl şekillendirileceğine dair süregiden bir tartışmayı ifade eder.

1.2.2. İnternetin Küreselleşmesi: İlk Yönetişim Tartışmaları

İnternetin ilk günlerinde kullanıcılar birbirini tanıyordu ve kimlik doğrulama için özel bir sisteme ihtiyaç yoktu. Normlar da basitti ve kolaylıkla geliştirilebiliyordu. Ancak, internetin büyümesi ile birlikte, kullanıcı sayısı arttı ve kimlik doğrulama ihtiyacı doğdu. Normlar da daha karmaşık hale geldi ve geliştirilmesi zorlaştı (Nye, 2010, s. 15). Özellikle ABD ordusu 1980'lerde internetin gelişimi ve kullanımı üzerindeki tekeli ele geçirdiğinde, internetin kullanıcı tabanı ve yönetim topluluğu büyük ölçüde genişlemiş ve kurumsallaşmaya başlamıştır (Budnitskiy, 2018, s. 76).

1990'lara gelindiğinde ise ABD Savunma Bakanlığı'nın ARPANET'in araştırma kolunu ticarileştirmeye karar vermesiyle internet, küresel bir mahiyet kazandı. İnternetin ticari alanda kullanım kısıtlamalarının kaldırılmasıyla birlikte internete olan ilgi önemli ölçüde artmaya başladı. Özellikle 1990 yılında Avrupa Nükleer Araştırma Örgütü'nden (CERN) Tim Burners-Lee tarafından World Wide Web'in (WWW) geliştirilmesi, internetin katlanarak büyümesinde büyük rol oynadı. WWW ile birlikte ağ üzerinden akan verinin sayısı günden güne artmaya başladı. Dolayısıyla bu durum, adres tahsis sisteminin yeniden düzenlemesi ihtiyacını doğurdu. Ancak böyle bir düzenleme, yönetişim işlevlerinin yeniden tanımlanması anlamına gelmekteydi

(Mockapetris & Dunlap, 1988, s. 123). "Hosts.txt" adında bir sunucu dosyası olarak başlayan sistem, daha önce DNS ve IP gibi pek çok sistemin geliştirilmesinde rol oynayan bir isim olan Jon Postel[4] tarafından yönetilmeye başlandı. Bu noktada, internet standartlarına ek olarak, ticari anlaşmalar düzenlemeyi etkilemeye başladı. Ağın büyümesiyle birlikte iş, eğitim, ekonomi ve güvenlikle ilgili birçok konu internet faaliyetlerinden etkilenmeye başladı. Bunun sonucunda devletler, sivil toplum kuruluşları, düzenleyici ve teknik kurumlar ve özel sektör gibi pek çok aktör, alan adları ve adresleriyle ilgilenmeye başladı. ICANN, tam da böyle bir ortamda, internetin güvenliğinden ve istikrarından ödün verilmeden standartların korunması ihtiyacına karşılık olarak oluşturuldu (Cerf, 1998).

1990'ların ikinci yarısından itibaren internet, ABD'de ve dünyanın diğer gelişmiş ülkelerinde kitle iletişim aracına dönüştü. Bu tarihten önce internetin geliştiricileri ve kullanıcılarının tekelinde olan ve öz-denetim modeliyle düzenlenen internet, artık büyük kuruluşlar ve devletler tarafından yönetilmeye başlandı (Budnitskiy, 2018, s. 78). İnternetin DNS'nin ticarileştirilmesi ve ücretsiz bir hizmetten ücretliye dönüştürülmesi DNS'nin yönetimi üzerinde ciddi bir küresel tartışmaya sebebiyet verdi. O zamandan bu yana internet, muazzam bir politik-ekonomik güce dönüşmüştür (Budnitskiy, 2018, s. 79).

DNS yönetimi üzerinde yaşanan değişim, ABD'yi bu konuda adım atmaya zorlamıştır. ABD yönetimi, DNS'nin kontrolünü ve internetin genel gelişimini sağlayacak yeni bir yönetim sistemi başlatmak için harekete geçmiştir (Mueller, 2012). ABD'nin harekete geçmesi, kâr amacı gütmeyen bir kuruluş olan California merkezli ICANN'in kurulmasıyla sonuçlanmıştır. 1998'deki kuruluşundan bu yana ICANN, küresel internet yönetişiminin politik-ekonomik sisteminde merkezi bir konumda olmuştur. Ekim 2016'ya kadar ICANN'in IANA yönetimi, ABD Ticaret Bakanlığı ile sözleşme garantisi altındaydı. Böylece sistemin yalnızca fiilen değil, hukuki olarak da ABD tarafından kontrol edilmesi sağlanmıştır.[5]

Siber uzayın düzenlenmesi için küresel koordinasyon ve politika oluşturma çabaları 1990'ların ortasında başlamıştır. Ancak bu uzun sürece rağmen bu konuda bir başarı elde edilememiştir (Mueller & Mathiason & Klein, 2007, s. 237). İnternet, Uluslararası

[4] Postel, Etki Alanı Adı Sistemi, Dosya Transferi, Telnet ve İnternet Protokolü gibi birçok temel internet protokolünün geliştirilmesinde yer almıştır.

[5] ICANN'in işleyişiyle ilgili detaylı bilgilere, çalışmanın "1.2.7.3. Uluslararası Standardizasyon Kuruluşları" alt başlığından erişilebilir.

Telekomünikasyon Birliği (ITU) gibi hükümetlerarası kuruluşların yönlendirmelerinden bağımsız bir şekilde ortaya çıkmış ve gelişmiştir. Bunun dışında Uluslararası Telekomünikasyon Yönetmelikleri (ITR'ler) gibi kuruluşların oluşturduğu uluslararası hukuk kurallarından bağımsız olmuştur (Fidler, 2013a). Öyle ki, ICANN, 1998'de kurulduğunda neredeyse devletlerin çoğu tarafından fark bile edilmedi (Ebert & Maurer, 2013, s. 1061). Dolayısıyla bu durum, devlet ve devlet dışı aktörlerin teknik standartların yönetilmesinde söz sahibi olmasını beraberinde getirdi. Öte yandan, çok paydaşlı sistemin internet yönetişiminin gelişimine katkıda bulunmasında etkili oldu. İnternet küresel olarak genişledikçe, ABD başta olmak üzere birçok ülke mevcut durumla ilgilenmeye başladı. Devletlerin ilgisinin bu konuya kaymasının öncelikli amacı, yönetişimi hükümetlerarası süreçlere ve uluslararası hukuk bünyesine dahil etmekti (Fidler, 2013a).

Yukarıda da belirtildiği üzere küresel dijital yönetişim kavramı, internetin ortaya çıkışı ve ardından hızla küreselleşmesiyle birlikte önem kazanmıştır. İnternetin icadı ve yaygınlaşması, bilgiye erişim, iletişim ve iş yapma şekillerini temelden değiştirerek özellikle ulus-devletler açısından "yeni bir tür küreselleşmeyi" beraberinde getirdi (Ermağan, 2022a, s. 136). Bu dijital devrim, sınırların ötesindeki etkileşimleri artırırken, internetin yönetişimi konusunda yeni sorunlar ve zorluklar ortaya çıkardı. İnternetin küreselleşmesi, farklı devletler, uluslararası kuruluşlar, özel sektör, sivil toplum ve bireyler arasındaki ilk yönetişim tartışmalarını tetikledi. Bu tartışmalar, internetin açık, erişilebilir ve çok taraflı bir platform olarak nasıl korunup yönetileceğine dair çeşitli perspektifleri içermiştir. İnternetin küreselleşmesiyle birlikte dijital ekonominin yükselişi, siber güvenlik tehditleri, veri koruma ve gizlilik, online ifade özgürlüğü ve internet erişiminin evrenselliği gibi konular ön plana çıktı. Dolayısıyla ilk yönetişim tartışmalarının da böyle bir atmosferde ortaya çıktığı söylenebilir.

1.2.3. Küresel İnternet Yönetişimi Tanımı

1.2.3.1. Genel Tanım

İnternet yönetişimi konusu yenidir ve kavrama dair net bir bakış açısı mevcut değildir. Akademik literatürde üzerinde fikir birliğine varılamayan pek çok internet yönetişimi tanımı bulunmaktadır. 2005 yılında WGIG (İnternet Yönetişimi Çalışma Grubu), internet yönetişimi için bir tanım geliştirmek için beş kriter öne sürmüştür:

1. *Yeterlilik*: Tanımın, internet yönetişiminin temel boyutlarını yakalaması ve devam eden küresel diyaloğu kolaylaştırması gerekir.
2. *Genelleştirilebilirlik*: Tanımın hem mevcut hem de potansiyel yönetişim faaliyetlerini içermesi gerekir.
3. *Tanımlayıcılık*: Tanımın, internet yönetişiminin ne olduğunu yansıtması gerekir, olmasını istediğimiz şeyi değil.
4. *Kısalık*: Tanımın, anlaşılması ve uygulanması kolay olacak kadar kısa olması gerekir.
5. *Süreç yönelimi*: Tanımın, yönetişim sürecine odaklanması gerekir, belirli yöneticilere değil.

Bu kriterler, WGIG'in internet yönetişimi için bir tanım geliştirmesine yardımcı oldu. Tanımı, internetin küresel doğası, demokratik ve kapsayıcı kullanımı, güvenliği ve yeniliği, erişilebilirliği ve kullanılabilirliği gibi temel unsurları yansıtmaktadır (WGIG Report, 2005, ss. 7-8). Zira internet yönetişimi, internetin işleyişini ve kullanımını etkileyen tüm süreçleri kapsar. Bu süreçler, farklı odak alanlarına, işlevlere, örgütsel bağlamlara, kurumsal biçimlere, güç türlerine, karar verme prosedürlerine, ele alınan konulara, ilgili katılımcılara, uyum mekanizmalarına ve dağıtım önyargılarına sahip olabilir (WGIG Report, 2005, s. 13).

Peki internet yönetişimi nedir? Aralık 2003'te Dünya Bilgi Toplumu Zirvesi'nin (WSIS) ilk aşamasının sonunda oluşturulan WGIG, etkili bir internet yönetişimi tanımı geliştirmiştir. Burada amaç, internet yönetişiminin tartışılması için bir zemin oluşturmanın yanında, çok paydaşlı bir yaklaşıma duyulan ihtiyacı karşılamaktı. Bu saikle internet yönetişiminin önemli bir tanımı, WGIG Nihai Raporu'nda yapılmıştır. WGIG, raporun ikinci bölümünde internet yönetişimini şu şekilde tanımlamıştır (WGIG Report, 2005): "İnternet yönetişimi; devletler, özel sektör ve sivil toplum tarafından internetin gelişimini ve kullanımını şekillendiren ortak ilkelerin, normların, kuralların, karar alma prosedürlerinin ve programların kendi rollerinde geliştirilmesi ve uygulamasıdır."

Bu tanıma göre yönetişim, internetin evrimini ve kullanımını şekillendiren ortak ilkeler, normlar, kurallar, karar verme prosedürleri ve programları ifade eder. Bu süreç, devletler, özel sektör ve sivil toplum tarafından birlikte yürütülür. Yönetişim terimi böylece ilk kez gelişmekte olan ülkelerde yolsuzlukla mücadeleyle ilgili geleneksel "iyi

yönetişim"den tamamen farklı bir anlamla BM belgelerinde yer almaya başlamıştır (de la Chapelle, 2007, s. 22).

İnternet yönetişiminin tanımı, çok sayıda bilimsel tartışmaya da konu olmuştur (Drake, 2004; van Eeten & Mueller, 2013; Haigh & Russell & Dutton, 2015). İnternet yönetişiminin tanımlanmasının zorluğu, bu alanın kapsadığı konuların çeşitliliğinden kaynaklanmaktadır. E-ticaretten siber güvenliğe, sansürden çocuk haklarına kadar uzanan geniş bir yelpazeyi kapsamaktadır (Mueller, 2007). Genel olarak yönetişim, stratejik yönlendirme sağlayan yönetim tarafından uygulanan bir dizi sorumluluk ve uygulamadır. Kurumsal kaynakların sorumluluğunun alınması ve risklerin doğru bir şekilde yönetilmesiyle belirlenen hedeflere ulaşılır (IT Governance Institute. 2010). İnternet yönetişimi ise, tarafların siber uzaya bağımlılığı neticesinde ortaya çıkan kurumsal yönetişim bileşenini ifade eder (Bodeau & Boyle & Fabius & Graubart, 2010). Aynı zamanda, dijital strateji, politika ve standartlar için net hesap verebilirlik oluşturmaya odaklanan bir disiplindir (Welchman, 2015, s. VI). Bu yönüyle dijital yönetişim, bir kuruluşun dijital varlığı için hesap verebilirlik, roller ve karar verme yetkisi oluşturmaya yönelik bir çerçeve olarak tanımlanabilir. Web siteleri, mobil uygulamalar, sosyal medya platformları ve diğer tüm internet ve web özellikli ürün ve hizmetler bu kapsamda değerlendirilmektedir (Welchman, 2015, s. 11). Floridi'ye göre internet yönetişimi, verinin uygun şekilde geliştirilmesi, kullanılması ve yönetimi için politikalar, prosedürler ve standartlar oluşturmak ve uygulamaktır (Floridi, 2018, s. 3). İnternet yönetişimi, aynı zamanda, devlet, vatandaşlar ve şirketler arasındaki etkileşimde demokratik yönetişimi basitleştirmek ve geliştirmek için bilgi ve iletişim teknolojisi araçlarının uygulanmasını teşvik etmektedir (Filgueiras & Almeida, 2021, s. 27).

İnternet yönetişimini tanımlama çabası içerisinde, kavramın sadece sözlüksel anlamına odaklanmak yetersiz kalabilir. Zira internet yönetişimi, bir dizi yaklaşım ve modeli içeren geniş bir alanı kapsar (Zeleke, 2019, s. 2). Bu nedenle, internet yönetişiminin ne olduğunu anlamak için, terimi daha geniş bir perspektifle ele alarak, uygulamadaki çeşitli yöntem ve modellere dair kapsamlı bir bakış açısı sunan tanımlara yönelmek daha faydalıdır. Bu, siber uzayın nasıl yönetilmesi gerektiğine dair çeşitli görüşler arasındaki farklılıkları anlamamıza yardımcı olur. Siber uzayın geleneksel yönetişim yapılarını karşı karşıya bıraktığı yeni zorluklarla başa çıkmak için bunun anlaşılması elzemdir (Filgueiras & Almeida, 2021, s. 85):

İnternet yönetişimi, bu zorlukların üstesinden gelmek için geliştirilen bir yaklaşımdır. Dijital yönetişim, dijital teknolojilerin potansiyelini kullanarak, daha etkili, verimli ve katılımcı bir yönetişim sağlamak için tasarlanmıştır. 2005 tarihli WGIG Raporunda, internet yönetişiminin kapsaması gereken süreçler şu şekilde maddelendirilmiştir:

1. *Önemli odak ve amaç*: İnternet yönetişimi süreçleri, internetin temel kaynakları, güvenliği, teknik standartları, fikri mülkiyeti, ticareti, mahremiyeti, iletişimi ve gelişimi gibi çeşitli konuları kapsayabilir.
2. *İşlevler*: İnternet yönetişimi süreçleri, kıt kaynakları yönetmek, ara bağlantı ve birlikte çalışabilirliği sağlamak, ekonomik işlemler ve iletişim için hüküm ve koşulları belirlemek, işlem ve bilgi maliyetlerini azaltmak, sorumluluk kurallarını oluşturmak, bilgi aktarımını ve toplu öğrenmeyi kolaylaştırmak gibi çeşitli işlevleri yerine getirebilir.
3. *Örgütsel bağlam*: İnternet yönetişimi süreçleri, resmi örgütlerin himayesi altında müzakere edilebilir.
4. *Kurumsal biçim*: İnternet yönetişimi süreçleri, devletlerarası anlaşmalar, özel sektör anlaşmaları veya diğer kurumsal biçimler şeklinde olabilir.
5. *Güç*: İnternet yönetişimi süreçleri, resmi veya gayri resmi, bağlayıcı veya gönüllü olabilir.
6. *Karar verme prosedürleri*: İnternet yönetişimi süreçleri, oylama veya oybirliği, uyuşmazlık çözümü gibi çeşitli karar verme prosedürlerini kullanabilir.
7. *Ele alınan konular*: İnternet yönetişimi süreçleri, çeşitli konuları ele alabilir, örneğin temel kaynaklar, güvenlik, teknik standartlar, fikri mülkiyet, ticaret, mahremiyet, iletişim ve gelişim.
8. *İlgili katılımcılar*: İnternet yönetişimi süreçlerine kamu sektörü, özel sektör ve sivil toplum kuruluşları dahil olmak üzere çeşitli katılımcılar dahil olabilir.
9. *Uyum mekanizmaları*: İnternet yönetişimi süreçleri, merkezi veya merkezi olmayan izleme ve uygulama sistemleri veya bunların yokluğu gibi çeşitli uyum mekanizmaları içerebilir.

10. *Dağıtım önyargıları*: İnternet yönetişimi süreçleri, hakların, sorumlulukların ve faydaların hakkaniyetli veya adaletsiz dağılımı gibi çeşitli dağıtım önyargılarına sahip olabilir (2005, s. 13).

Bu faktörler, internet yönetişimi süreçlerini ve bunların etkisini anlamanın önemli unsurlarıdır. Bu tanımlardan yola çıkarak, internet yönetişimini şu şekilde özetleyebiliriz: İnternet yönetişimi, dijital teknolojilerin potansiyelini kullanarak, daha etkili, verimli ve katılımcı bir yönetişim sağlamak için tasarlanmış bir yaklaşımdır. Bu yaklaşım, yönetişim yapılarının toplumdaki güç dengelerini yansıtan katılımcı ve kapsayıcı bir yapı ile yeni türdeki risk ve tehditlere karşı etkili bir yanıt oluşturmasını hedefler.

1.2.3.2.Paydaş Odaklı Tanım

Son zamanlarda egemenlik üzerine yapılan tartışmalar genellikle siber uzayı kimin kontrol ettiği sorusu üzerinde yoğunlaşmaktadır. Bu tartışmada "egemenlik", "kontrol" ve "güç" terimleri genellikle birbiriyle yakından ilişkilidir. Tartışma, siber uzayı kimin yönettiğiyle ilgili sorunlar üzerinde yoğunlaşması sebebiyle literatüre katkı sağlamaktadır (Crews & Thierer, 2003; Radu & Chenou & Weber, 2016). Egemenlik, kontrol ve güç kavramlarının siber uzayın yönetişimi bağlamında iç içe geçtiği bu tartışmalar, dijital yönetişim alanındaki karmaşıklığı ve bu alandaki çeşitli aktörlerin rollerini daha da önemli hale getirmektedir.

Dijital yönetişim, siber uzayın doğası gereği oldukça karmaşık bir alandır. Bu yönüyle teknik, politik, yasal ve ekonomik yönleri içeren multidisipliner bir yapıya sahiptir. İnternet yönetişimi, devletler, özel sektör ve sivil toplum gibi aktörleri sürece dahil eder. Bu alanı kimin kontrol ettiği, nasıl yönetildiği ve yönetimin nedenleri konusunda farklı görüşler ve tartışmalar mevcuttur. Bu tartışmalar, internetin nasıl kontrol edileceği, teknik standartların nasıl tanımlanacağı ve güvenlik biçimlerinin nasıl oluşturulacağı gibi önemli meseleleri kapsamaktadır (Filgueiras & Almeida, 2021, s. 85; Zeleke, 2019, s. 2). Aynı zamanda küreselden yerele farklı politika düzeylerinde konularla ilgilenir (Kurbalija, 2015, s. 92). Dijital yönetişimin karmaşıklığı ve multidisipliner yapısı, siber uzayın kontrolü üzerine yapılan egemenlik tartışmalarını daha da çetrefilli bir hale getirirken, yönetişim modellerinin çeşitliliği ve etkinliği konusunda da yeni sorular ortaya koymaktadır.

Bir yandan bazıları, siber uzayın bir ulusun egemenliği altında olması gerektiğini ve bu nedenle devletin bu alandaki yönetimi üstlenmesi gerektiğini savunurken, diğer yanda ise siber uzayın yönetişiminin devletler, kuruluşlar ve özel sektör gibi çeşitli aktörlerin işbirliği ile gerçekleştirilmesi gerektiğini öne süren bir görüş bulunmaktadır. Ancak internet yönetişimi, devletlerin, şirketlerin, uluslararası kuruluşların ve sivil toplumun aktif katılımı ile şekillenen geniş bir alandır. Bunun yanında siber uzay, dijital teknolojiler, sosyal medya ve veri yönetişimi gibi bazı kullanımlar birbirlerinin yerine tercih edilebilmektedir. Bütün bu yönetişim biçimleri, yalnızca küresel değil, aynı zamanda bölgesel ve yerel sorunları da ele alır ve çok merkezli bir yönetişim modelini temsil eder. Bu nedenle dijital yönetişim, çok merkezli bir yönetişim modeli oluşturan, birden çok paydaştan, forumdan ve yargı alanından oluşan karmaşık bir alandır (Filgueiras & Almeida, 2021, s. 84).

Bu nedenle internet yönetişimi, teknik boyutun ötesine geçen bütünsel bir yaklaşım olarak anlaşılmalıdır. Yönetişimin karar verme süreci; teknik standartlar, algoritmaların tasarımı, şifreleme dağıtımı gibi pek çok faktör üzerinden değişkenlik gösterebilir. Benzer şekilde kararı kimin (hangi paydaşın) verdiği de aynı derecede önem arz etmektedir. Devlet yetkililerinden mühendislere kadar geniş bir karar mekanizması söz konusu olduğundan, yönetişime çeşitli paydaş gruplarının farklı anlayışları hâkim olmaktadır (van der Spuy, 2017, s. 25). Bu bağlamda internet yönetişimi, teknik detayların ötesinde, katılımcı ve bütünleşik bir yaklaşım gerektirir. Zaten internet yönetişiminin kendisi de internet altyapısı, siber güvenlik sorunları, sistem ve kod standartları, gizlilik, bilgi ve iletişim teknolojilerinin (BİT) kullanımı ve yasal düzenleme gibi hem teknik hem de politik konuları içermektedir. Dolayısıyla bu konular hakkında alınan kararların tek bir otorite tarafından alınması söz konusu değildir. Bazı yazarlar bu otoriteyi devletlere atfen "leviathan" olarak nitelendirirken; özel sektör için de "görünmez el" metaforunu kullanmışlardır (Filgueiras & Almeida, 2021, s. 84). Kısacası, devlet otoritesinin veya piyasayı yönlendiren diğer aktörlerin dijital yönetişim üzerinde tek başına söz sahibi olamayacaklarının altını çizmişlerdir. İnternet yönetişimi, birden fazla paydaşı içerir ve küresel, bölgesel ve yerel olarak alınan kararlar işbirliği çerçevesinde pratiğe dökülür. Siber uzayın yönetişimine ilişkin bu iki zıt görüş, internet yönetişimi alanının, teknik detaylarının ötesinde, geniş bir paydaş yelpazesini içeren ve çok merkezli bir yönetişim modeline dayanan bütünsel bir yaklaşım gerektirdiğini vurgulamaktadır.

WGIG'in internet yönetişimi tanımı, çok paydaşlı katılımı teşvik eden ve yönetişim unsurlarını normlar, ilkeler, kurallar ve prosedürlere kadar genişleten bir tanımdır (van der Spuy, 2017, s. 25). Tanım, devletlerin, özel sektörün ve sivil toplumun katılımına atıfta bulunarak, çok paydaşlı işbirliği için bir temel sağlamıştır. WGIG, terimin yalnızca devletleri değil, özel sektör ve sivil toplum gibi paydaşları da kapsadığını belirterek terimin anlamını hem geliştirmiş de genişletmiştir. Bu tanım, devlet dışı aktörlerin internet yönetişimindeki konumunun uluslararası platformlar aracılığıyla onaylanması açısından elzemdir. Tanım bugün hala "alandaki kurumlar ve mekanizmalar için bir meşruiyet ölçütü" olarak kabul edilmektedir (Cigi & Chatham House, 2016, s. 78). Tanım, çok paydaşlı katılımın önemini vurgulayarak, siber uzayın yönetişiminin yalnızca teknik bir mesele olmadığını, aynı zamanda geniş bir işbirliği ve diyalog gerektiren karmaşık bir süreç olduğunu göstermektedir.

WGIG tanımının tartışmalı "ilgili roller" kısmı, "paylaşılan karar alma prosedürleri" kısmından ayrı tutulmamıştır. Dolayısıyla bu hükümler, egemenlik haklarının sınırsız olarak kullanılması için bir gerekçe olarak değil, daha çok Drake'nin vurguladığı "işbirlikçi egemenlik"e katılıma bir davet olarak değerlendirilmiştir (2015, s. 24). Bu bağlamda tanıma ilişkin geri bildirim genellikle olumlu olmuştur ve tanım, Tunus Gündeminin 34. paragrafına kelimesi kelimesine eklenmiştir (Hubbard & Bygrave, 2009, s. 226). WGIG tanımının sağladığı geniş perspektif, internet yönetişiminin merkezi olmayan ve katılımcı doğasını daha iyi anlamamızı sağlarken, bu sürecin etkinliğinin tüm paydaşların aktif katılımına bağlı olduğunu da hatırlatmaktadır.

Bazıları bu tanımı bütünsel, geniş ve esnek olarak kabul ederken, bazıları tanımın "yönetişim" terimini değerlendirirken "çok dar" olduğunu düşünmektedir (Drake, 2005, s. 255; Mueller, 2010, s. 9). Örneğin Mueller'e göre bu tanım halen çok dar iken Van Der Spuy'a göre ise paydaşları ve internet yönetişiminin karşılaştığı bazı zorlukları tanımlaması bakımından yararlıdır. Ancak, internet yönetişiminin yapısı ve aktörleri hakkında net bir bilgi vermediği için belirsizdir. Dahası, internet yönetişiminde paylaşılan ilkelerin, normların ve kuralların gerekli olduğunu belirtirken, bunların ne olduğuna dair herhangi bir bilgi vermemektedir (2010, s. 10; 2017, s. 15).

Öte yandan WGIG'in tanımı, bu sürecin merkezi bir yapıya sahip olduğunu öne sürmektedir. Ancak, gerçekte siber yönetişim, milyonlarca kullanıcının etkileşimi ile şekillenmektedir. Bu nedenle, siber yönetişimi anlamak için daha geniş bir perspektif

benimsemek ve merkezi olmayan politika yapımını da hesaba katmak gerekir. Siber yönetişimin başarılı olması için, özel aktörlerin ve sivil toplumun sorumluluklarını kabul etmek önemlidir. Bu aktörler, çerçevelerin uygulanabilirliği ve uygulanması için gereklidir. Bununla birlikte, devletler tarafından yönetilebilecek bazı değişkenler ve faktörler de vardır (Zangl, 2021, s. 4). Özetle siber yönetişim, internetin güvenli ve sorumlu bir şekilde kullanılması için gerekli olan bir süreçtir. Pratikteki uygulamaların önemi, internet yönetişimi tartışmalarının yalnızca teorik düzeyde kalmadığını, gerçek dünyada somut sonuçlar doğurduğunu ve siber uzayın telekomünikasyon alanı olarak tanımlanmasının da bu süreçlerin bir parçası olduğunu göstermektedir.

Yönetişim, hem yukarıdan aşağıya hem de aşağıdan yukarıya bir süreçtir. İnternete uygulandığında yönetişim, internete dair yazılım ve donanımı içeren ve etkileyen tüm kurallar ve süreçleri kapsamaktadır. İnternetin doğası gereği, internet yönetişimini uygulamak için çok paydaşlı bir düzenlemeye ihtiyaç vardır. Bunun nedeni, internetteki uygulamaların sürekli değişen doğasının, herhangi bir devletin egemen ve düzenleyici olmasını imkânsız hale getirmesidir. WGIG, akademik ve teknik topluluğun internet yönetişimindeki önemini kabul etmiştir (Ang & Haristya, 2015, s. 124). Bu, tüm paydaşların internet ile ilgili karar alma süreçlerinde rol oynaması gerektiği anlamına gelir. Ancak, bu rollerin tam olarak nasıl oynanacağı, sorunun doğasına ve niteliğine göre değişkenlik göstermektedir. İnternet yönetişimi hakkında ortak bir görüş ve anlayış geliştirmek için, tartışmanın birbirini tamamlayan iki yaklaşımı takip etmesi gerekir. Birincisi, genel ilkelerden veya öncüllerden belirli çıkarımlara geçerek ilerlemektir. 2005 tarihli WGIG Raporunda bir tanımın karşılaması gereken bir dizi temel kriter tanımlanmıştır. Bu kriterler, internet yönetişimi hakkında ortak bir görüş ve anlayış geliştirmeye yardımcı olmak için tasarlanmıştır. Bu kriterleri şu şekilde özetlemek mümkündür (2005, s. 6):

- İnternet yönetişimi, internetin küresel doğasını yansıtmalıdır.
- İnternet yönetişimi, internetin demokratik ve kapsayıcı bir şekilde kullanılmasını sağlamalıdır.
- İnternet yönetişimi, internetin güvenliğini ve emniyetini sağlamalıdır.
- İnternet yönetişimi, internetin gelişimini ve yeniliğini desteklemelidir.
- İnternet yönetişimi, internetin erişilebilirliğini ve kullanılabilirliğini sağlamalıdır.

Bütün bu teorik yaklaşımların ötesinde, pratikteki uygulamalara bakmak önemlidir. Paydaşların rollerine odaklanan tanımlar elbette önemlidir fakat bu tanımların ne denli işlevsel olduğunu pratikteki uygulamalar belirler. Bugünkü internet yönetişimi görünümünde hangi aktörlerin etkin rol aldığı, bu alanın teknik standartlarının ötesinde mi, yoksa onunla sınırlı mı kabul edildiği ancak bu şekilde anlaşılabilir. Günümüz pratiğinde siber uzay, telekomünikasyon için bir etki alanı olarak tanımlanmaktadır. İnternet ise, bilgilerin siber uzayda hareket etmesine izin veren bir altyapı görevi görür. İnternet, Amerikalı bilim insanları ve mühendisler tarafından askeri iletişim için kullanılacak bir araç olarak tasarlanmıştır ve yine ABD hükümetinin finansmanı ile 1995 yılında tamamen ticari kullanıma açık hale gelmiştir. Bu kapsamlı evrim, internetin askeri iletişim aracından küresel bir telekomünikasyon etki alanına dönüşümünün ardından, internet yönetişimi kavramının ve pratiklerinin ortaya çıkışını ve gelişimini kaçınılmaz kılmıştır.

ICANN'in 1998'de kurulmasıyla birlikte internet yönetişiminin anlamı ve kapsamı önemli ölçüde genişlemeye başladı. Bu sayede daha önce ayrı teknolojilerle sunulan ve ayrı yasal ve düzenleyici rejimler tarafından yönetilen internetin işlevleri de genişletilmiş oldu (Mueller, 2010, s. 10). O zamandan bu yana internetin küresel anlamda neredeyse tüm altyapısı özel sektöre ait iken (Kleinwächer, 2009), yönetişim faaliyetlerini yürütme görevi IANA'ya devredilmiştir. Ancak IANA, sorumluluklarını kâr amacı gütmeyen bir organizasyon olan ICANN'e devretmiştir (Milian, 2011). Ancak her halükârda, ICANN ve IANA'nın yetkisinin, siber uzayın yönetişiminin tamamıyla değil, alan adlarının tahsisinin ve dağıtımının yönetimi ile sınırlı olduğunu belirtmek gerekir (Mueller, 2010, s. 10). ICANN ve WSIS gibi dönüm noktaları, internet yönetişimi alanında devlet ve devlet dışı aktörler arasındaki dinamikleri ve bu aktörlerin siber uzayın kontrolü üzerinde nasıl bir etkisi olduğunu anlamamıza yardımcı olur.

Özellikle ICANN'in kurulmasıyla birlikte internet, tüm siber politikalar için en önemli tartışma platformu haline geldi. Mueller'e göre internet yönetişiminin evriminde iki dönüm noktası öne çıkmaktadır. Bunlardan birincisi, ICANN'in kurulmasıydı. ICANN, ABD tarafından kurulmasına rağmen, hükümet dışı bir modeli temsil etmekteydi. Mueller'in deyimiyle "tek taraflı bir küresel rejim" anlayışına dayanmaktaydı (Mueller, 2010, s. 10).

Bir diğer kırılma noktası, BM'nin düzenlediği WSIS idi (Mueller, 2010, s. 10). WSIS, 2002'den 2005'e kadar bilgi toplumuyla ilgili tüm konuları ele almaya çalışan çok taraflı ancak devlet merkezli bir diplomatik konferanslar dizisi idi. Daha sonra, İnternet Yönetişimi Dünya Zirvesi'ne dönüştü. WSIS, internet yönetişiminin nasıl bir rejimle yönetileceğine dair sorunların tartışıldığı bir platform olması açısından önem arz etmektedir. Zira özellikle ulus-devletler arasında uygulanacak model konusunda neredeyse birbirine tamamen zıt iki kutup ortaya çıkmıştır. Bir taraftan internetin devletler aracılığıyla yönetilmesi ve yönetiminin menşei devlete ait olması gerektiğini savunan bir taraf varken, diğer tarafta daha açık, çoğulcu ve ulus ötesi bir politika izlenmesi gerektiğini savunanlar olmuştur. İleriki bölümlerde detaylıca inceleyeceğimiz üzere internet yönetişiminde çekişmeli devletlerin varlığı halen söz konusudur. Ancak WSIS'te ilk çatırdamalara sahne olan tartışmaların esas çıkış noktası, ABD'nin ICANN'i kurmuş olmasıydı. ICANN'in yaratıcısının ABD olması, uluslararası sistemdeki çoğu aktöre rahatsızlık vermiş, bu durum günümüze kadar uzanan bir rekabet ortamının zeminini hazırlamıştır. Bu anlamda WSIS, ABD'nin mevcut yönetişim rejimindeki üstünlüğünün tartışılması için gerekli olan platform görevini üstlenmiştir. İnternet yönetişiminin ilgilendiği konuların genişlemesi, siber uzayın stratejik öneminin ve uluslararası ilişkilerdeki yerinin daha da artmasına neden olmuştur, bu da devletlerin ve diğer aktörlerin bu yeni rekabet alanında nasıl hareket ettiğine dair önemli soruları beraberinde getirmiştir.

Günümüz itibariyle ise internet yönetişiminin ilgilendiği konular oldukça geniş bir alanı kapsamaya başlamıştır. Sansür ve içerik düzenlemesi, fikri mülkiyet haklarının korunması, ticari markalar ve telif hakları, siber güvenlik, insan haklarının korunması, gözetim politikaları, spam kontrolü, siber suçlar, ICANN'in kaynak atama ve koordinasyon politikaları, teknik standartların oluşturulması, iletişim hizmetlerinin ekonomik düzenlemesi bunlardan bazılarıdır (Mueller, 2010, s. 10). IP adreslerinin tahsisi, alan adlarının tanınması veya kök sunucuların yönetişimi gibi internet işlemlerinin en teknik yönleri bile bugün tartışmalı meseleler sınıfına dahil edilebilmekte ve bunların politize edildiği söylenebilmektedir (Ebert & Maurer, 2013, s. 1058). İnternetin teknik yönlerinin politize edilmesi, siber uzayın uluslararası ilişkilerdeki stratejik önemini arttırmış ve bu alanda yaşanan küresel rekabetin somut bir göstergesi olmuştur.

Uluslararası ilişkilerde siber uzayın stratejik öneminin devletler tarafından anlaşılmasıyla birlikte bu alanın yönetişimi de devletler için yeni bir küresel rekabet alanı haline gelmiştir. Özellikle büyük güçlerin politikalarının ifşa edilmesi, gerek insan hakları bağlamında gerekse de gözetim ve gizlilik hakları bağlamında pek çok problemi gün yüzüne çıkarmıştır. Wikileaks'in kurulması,[6] Mandiant Raporu'nun yayınlanması,[7] Edward Snowden'ın ABD hükümetinin gözetim programlarını sızdırması gibi ifşa olayları,[8] bazı yeni gizlilik güvenliğine ilişkin endişeleri gündeme getirmiştir (The Guardian, 2013). Bu bağlamda, siber uzayın stratejik önemi ve uluslararası rekabet alanı olarak yükselişi, devletlerin ve diğer aktörlerin siber güvenlik, gözetim, gizlilik ve insan hakları gibi konularda nasıl hareket ettiğine dair yeni bir perspektif sunmaktadır. İnternet yönetişimine paydaş odaklı bir yaklaşım, bu karmaşık sorunları ele alırken çok yönlü bir işbirliği ve diyalog gerektiğini vurgulamaktadır. Wikileaks'ten Edward Snowden'a kadar yaşanan ifşa olayları, siber uzaydaki eylemlerin geniş çaplı sosyal ve politik sonuçlara sahip olduğunu göstermiştir. Bu nedenle siber uzayın yönetişimi, yalnızca teknik bir mesele olmanın ötesinde, uluslararası ilişkilerde önemli bir diplomasi ve güvenlik meselesi haline gelmiştir. Devletler, sivil toplum, özel sektör ve uluslararası kuruluşlar gibi çeşitli paydaşların katılımıyla şekillenen bu yeni yönetişim modeli, siber uzayın geleceğini şekillendirme konusunda kritik bir öneme

[6] Wikileaks, 2006 yılında Julian Assange tarafından kurulan, gizli belgeleri ve sızıntıları yayımlayarak kamuoyunu bilgilendiren uluslararası bir sızıntı platformudur. Özellikle hükümetlerin, şirketlerin ve diğer kurumların gizli tuttuğu bilgileri ifşa ederek, şeffaflığı ve hesap verebilirliği artırmayı amaçlar. Wikileaks, savaş suçları, casusluk faaliyetleri, yolsuzluk ve çevre ihlalleri gibi çeşitli konularda önemli belgeleri ortaya çıkarmıştır ve bu yayımlarla uluslararası alanda büyük tartışmalara yol açmıştır. Platformun faaliyetleri, bir yandan kamu yararını hedeflerken, diğer yandan gizlilik, ulusal güvenlik ve bireysel mahremiyetle ilgili endişeleri de beraberinde getirmiştir. Ayrıntılı bilgi için bkz: BBC. (2019). Wikileaks: Document dumps that shook the world, https://www.bbc.com/news/technology-47907890 (02.11.2021).

[7] Mandiant, bir Amerikan siber güvenlik şirketidir. Şubat 2013'te Çin'in siber casusluğunu öne süren bir rapor yayınlamıştır. Mandiant, Şubat 2013'te Çin Halk Kurtuluş Ordusu'na bağlı olduğu belirtilen APT1 adlı birim tarafından yürütülen geniş çaplı bir siber casusluk kampanyasını ifşa eden bir rapor yayınladı. Rapor, APT1'in 2006'dan bu yana 141 kurban üzerinde ekonomik casusluk yürüttüğünü, çeşitli endüstrilere yönelik saldırılar gerçekleştirdiğini ve büyük miktarda bilgi çaldığını ortaya koydu. Rapor, APT1'in faaliyetlerine dair 3.000'den fazla göstergeyi içeren bir dijital ek de sağlayarak, bu tehdide karşı savunmaların güçlendirilmesine katkıda bulundu Ayrıntılı bilgi için bkz: Mandiant. (2013). Mandiant, APT 1: Exposing One of China's Cyber Espionage Units. https://www.mandiant.com/sites/default/files/2021-09/mandiant-apt1-report.pdf (02.11.2021).

[8] Edward Snowden, eski bir Ulusal Güvenlik Ajansı (NSA) çalışanı, 2013 yılında ABD hükümetinin geniş çaplı elektronik gözetim programlarını ifşa ederek küresel bir tartışma başlattı. Snowden, ABD hükümetinin telefon kayıtlarını, internet kullanımını izlediğini ve dünya genelindeki insanların gizliliğini ihlal ettiğini ortaya koyan gizli belgeleri sızdırdı. Bu olay, kamuoyunda gizlilik, güvenlik ve hükümet gözetiminin sınırları üzerine yoğun bir tartışma yaratırken, Snowden'ı bir kahraman olarak görenlerle, onu bir hain olarak nitelendirenler arasında bölünmelere neden oldu. Ayrıntılı bilgi için bkz: The Guardian. (2013). NSA Files: Decoded. https://www.theguardian.com/world/interactive/2013/nov/01/snowden-nsa-files-surveillance-revelations-decoded#section/1 (02.11.2021).

sahiptir. Bu çok boyutlu ve paydaşlar arası işbirliği, siber uzayın karmaşıklığını yönetmede ve bu yeni küresel rekabet alanında adil ve etkili politikalar oluşturmada hayati bir role sahiptir.

1.2.3.3.İyi Yönetişim Bağlamında Tanım

Küresel iyi yönetişim, güvenlik ve sürdürülebilirlik için devletler, uluslararası kuruluşlar, şirketler, sivil toplum ve uzmanların işbirliğini içeren bir yaklaşımdır. Ortak faydaları en üst düzeye çıkarmayı hedeflerken; küresel tehditleri en aza indirmeyi hedefler. Siber yönetişim ise, küresel iyi yönetişimin bir bileşenidir. Siber iyi yönetişimin temel amacı, güvenli ve özgür bir siber alan sağlamaktır. Bu amaç doğrultusunda siber yönetişim, aşağıdaki hedefleri gerçekleştirmeyi amaçlamaktadır (Akyeşilmen, 2018b, s. 3):

- Siber uzaydaki tehditleri ve riskleri azaltmak
- Siber güvenlik önlemlerini geliştirmek
- Siber uzayda şeffaflığı ve hesap verebilirliği sağlamak
- Siber uzayda insan haklarını ve temel özgürlükleri korumak

Bu amaçlar, dijital teknolojilerin hızlı bir şekilde benimsenmesi ve akabinde büyük bir dönüşümü beraberinde getirmesiyle ortaya çıkmıştır. Bu dönüşümü yönetmek için geliştirilen standartların, bir dizi temel ilkenin rehberliğinde olması gerektiği fark edilmiştir. Nitekim mevcut dijital standartların belirlenmesinde yedi ilkenin önemli olduğu kanısına varılmıştır: güvenilirlik, kapsayıcılık, sürdürülebilirlik, birlikte çalışabilirlik, emniyet ve güvenlik, veri gizliliği ve uluslararası işbirliği. Bu ilkeler, dijital dönüşümde adil, güvenli ve sürdürülebilir bir gelecek inşa etme amacını taşımaktadır. Bu ilkelere göre, dijital dönüşümün yönetilmesinde standartlar belirlenirken, insanların ve gezegenin refahı ile etik değerler göz önünde bulundurulmalıdır. Bu kapsamda, standart oluşturmada dikkate alınması gereken önemli faktörler, teknolojik gelişmelerin toplumsal ve çevresel etkilerini değerlendirmeyi amaçlar (UNIDO, 2021).

İyi siber yönetişim, internetin güvenli ve özgür bir şekilde kullanılmasını sağlamak için gereklidir. Bu yönetişim biçimi, insan haklarına saygılı ve herkes için adil olmalıdır. Küresel internet kullanıcıları, iyi siber yönetişim ilkeleri aracılığıyla temel insan haklarını korumayı amaçlamaktadır (Mihr, 2014, s. 32). Örneğin, siber saldırılara karşı koruma sağlayarak, kişisel verilerin korunmasını sağlayarak ve ifade özgürlüğünü

destekleyerek internetin güvenli ve özgür bir şekilde kullanılmasını sağlayabilir. Diğer yandan, siber güvenlik farkındalığını artırabilir, siber saldırılara karşı kendilerini koruyabilir ve iyi siber yönetişim ilkelerini destekleyen devletleri ve kuruluşları destekleyebilirler.

İyi siber yönetişim, hesap verebilirlik, şeffaflık ve katılımcılık gibi temel ilkeleri benimser. Bu ilkeler, insan haklarının korunması ve geliştirilmesi açısından hayati öneme sahiptir. Hesap verebilirlik, siber yönetişimin temel taşlarından biridir ve siber yönetişimle ilgili tüm aktörlerin, eylemlerinden sorumlu tutulmalarını gerektirir. Bu, siber saldırılara karşı korunma, kişisel verilerin güvenliği ve ifade özgürlüğünün desteklenmesi gibi konularda önemlidir. Şeffaflık, siber yönetişimin diğer bir önemli ilkesidir ve siber yönetişim aktörlerinin, kararlarını ve eylemlerini kamuoyuyla açıkça paylaşmaları gerektiğini vurgular. Böylece, siber yönetişim süreçlerinin şeffaf ve hesap verilebilir olması sağlanır. Katılımcılık ise siber yönetişimin üçüncü temel ilkesidir ve siber yönetişim süreçlerine tüm ilgili tarafların dahil edilmesi gerektiğini belirtir. Bu, siber yönetişimin daha adil ve kapsayıcı olmasını teşvik eder. Diğer yandan, hukukun üstünlüğü ilkesi, herkesin yasalara eşit şekilde tabi olduğunu ve yasaların herkes için geçerli olduğunu ifade eder. Ancak, eşit ve evrensel yasal standartların bulunmadığı bir ortamda, bu ilke uygulanamamaktadır (Mihr, 2014, s. 32).

İyi yönetişime göre bu ilkelerin temelinde çok paydaşlılık modeli yer almaktadır. İyi siber yönetişimin çok paydaşlılık perspektifi, siber uzayın yönetişimi ve düzenlenmesi süreçlerine devletler, uluslararası kuruluşlar, özel sektör, sivil toplum kuruluşları ve akademi gibi çeşitli aktörlerin katılımını içeren bir yaklaşımdır. Bu yaklaşım, siber güvenlik, gizlilik, insan hakları ve dijital ekonominin sürdürülebilirliği gibi konularda ortak kararlar alınmasını ve uygulanmasını teşvik eder. Çok paydaşlılık, karşılıklı anlayış ve işbirliğini temel alır, böylece siber politikaların ve standartların oluşturulmasında daha geniş bir perspektif sağlanır. Çok paydaşlı karar alma sürecine atfedilen meşruiyet, "daha yüksek kalitede politika sonuçlarının beklentisi" ile yakından ilişkilidir veya basitçe "daha iyi yönetişim" olarak ifade edilir (van der Spuy, 2017, s. 29).

Devletler, ulusal güvenliği koruma, vatandaşların haklarını savunma ve uluslararası normlar oluşturma gibi kritik roller üstlenirken; ABD gibi ülkeler, Siber Güvenlik ve Altyapı Güvenliği Ajansı (CISA) gibi kurumlar aracılığıyla siber tehditlere karşı

koordinasyon sağlamaktadır. Aynı zamanda, BM ve ITU gibi uluslararası kuruluşlar, siber güvenlik ve internet yönetişimi konularında küresel standartlar ve politikalar geliştirerek uluslararası işbirliğini teşvik eder. Özel sektörde, Google ve Microsoft gibi teknoloji devleri, siber güvenlik çözümleri geliştirme, veri gizliliğini koruma ve yenilikçi teknolojiler sunarak siber alanın güvenliğine katkıda bulunur. Sivil toplum kuruluşları, siber uzayda birey haklarını, özgürlükleri ve gizliliği koruma konusunda önemli bir rol oynayarak politika yapıcıları bilgilendirir ve genel kamuoyu farkındalığını artırır. Akademi ise, üniversiteler ve araştırma enstitüleri aracılığıyla siber güvenlik, gizlilik ve etik konularında derinlemesine araştırmalar yaparak bu alanda bilgi birikimini ve politika önerilerini geliştirir.

2005 yılında BM Genel Kurulu tarafından düzenlenen WSIS, internet yönetişimi konusunda benzersiz çok paydaşlı bir yaklaşımın benimsenmesine önemli bir katkı sağlamıştır, bu da internetin geleceği üzerinde derin etkiler yaratmıştır. WSIS'in etkisi, sadece o dönemde değil, sonraki yıllarda da çeşitli uluslararası platformlarda kendini göstermiştir. Örneğin, 2008 yılında OECD'nin, 2009'da Avrupa Konseyi'nin, 2010'da ITU'nun Tam Yetkili Temsilciler Konferansı'nın yanı sıra 2011'deki G8 Zirvesi, 2014'teki NETmundial Toplantısı, 2015'teki BM Genel Kurulu WSIS+10 Yüksek Seviyeli Toplantı ve IGF gibi uluslararası girişimler, bu çok paydaşlı yaklaşımı destekleyerek internet yönetişiminin evrimine katkıda bulunmuştur. Bu süreç, internetin küresel bir varlık olarak nasıl yönetileceği konusundaki tartışmalara daha fazla katman eklerken, uluslararası işbirliğinin ve çok paydaşlı yaklaşımın da önemini vurgulamıştır (ISOC, t.y.a.).

Görüldüğü üzere siber iyi yönetişimde çok paydaşlılık perspektifi, siber yönetişimde geniş bir anlayış ve işbirliği ağının oluşturulmasını sağlar. Bu yaklaşım, siber uzayın karmaşıklığını ve dinamizmini yönetmede daha etkili olmak için farklı perspektiflerin ve uzmanlık alanlarının bir araya getirilmesini teşvik eder. İyi siber yönetişim, bu çok yönlü işbirliğinin bir sonucu olarak, daha güvenli, adil ve özgür bir dijital ortamın inşasını mümkün kılar.

1.2.4. Dijital Yönetişim Yaklaşımları

İnternet yönetişimi karmaşık bir konudur ve farklı alanlarda uzmanlaşmış kişiler bu konuya farklı bakış açılarıyla yaklaşmaktadır. Bu durum, "Elinde çekiç olana her sorun çivi gibi görünür" atasözünü akla getirmektedir. Telekomünikasyon uzmanları

internetin altyapısına ve kablolara odaklanırken, bilgisayar uzmanları standartların geliştirilmesine önem verir. İletişim uzmanları internetin iletişimi kolaylaştırmaya yönelik çalışmalar yürütürken, insan hakları aktivistleri internetin ifade özgürlüğü ve mahremiyet gibi temel hakları korumasına odaklanır. Avukatlar internet yönetişiminde yargı yetkisinin rolünü önemserken, güvenlik uzmanları ise internet altyapısının güvenliğini korumaya çalışır. Her meslek grubu, internet yönetişimi konusundaki bakış açısını kendi uzmanlık alanıyla sınırlandırmaktadır (Kurbalija, 2015, s. 93).

Bu durum, internetin bütüncül bir şekilde yönetilmesini zorlaştırabilir. Ancak, farklı bakış açılarının da faydaları vardır. Farklı uzmanlık alanlarının bir araya gelmesi, internetin daha iyi yönetilmesine katkıda bulunabilir. Önemli olan, farklı bakış açılarının birbirini tamamlaması ve ortak bir paydada buluşmasıdır. İnternet yönetişiminin en büyük zorluklarından biri, bu farklı bakış açılarını dengelemek ve ortak bir zemin bulmaktır. Bu ancak, açık ve şeffaf bir şekilde iletişim kurarak ve farklı paydaşların görüşlerini dikkate alarak yapılabilir.

Literatürdeki genel kategorizasyona bakıldığında yaygın olarak küresel siber yönetişime dair iki ana yaklaşım olduğu görülmektedir: teknik yaklaşım ve politik yaklaşım (Cuihong, 2018, s. 56; Akyeşilmen, 2018a, ss. 259-274; Akyeşilmen, 2018b, ss. 9-11). Teknik yaklaşım genel itibariyle dar bir yaklaşımı temsil ederken; politik yaklaşım merkezi ve ademi-merkeziyetçi yaklaşımları da içerecek şekilde daha geniş bir yönetişim anlayışını temsil eder. Dar bakış açısı, internetin teknik işleyişinin sorunsuz bir şekilde devam etmesine odaklanırken, geniş bakış açısı internetin toplum üzerindeki daha geniş etkilerini ve sorumluluklarını da göz önünde bulundurur. Bu iki bakış açısı arasındaki dengeyi kurmak, internetin adil, sorumlu ve sürdürülebilir bir şekilde yönetilmesi için kritik önem taşır (Souter, 2021). Tartışmalar genel olarak bu iki ana eğilim altında kategorize edilmiştir.

1.2.4.1.Teknik Yaklaşım

Bunlardan birincisi, stardardizasyon ve altyapının ön planda olduğu teknik yaklaşımdır. İnternet yönetişimi hakkındaki tartışmalar, internetin akademik bir ortamdan geniş kitlelere açık bir iletişim platformuna dönüşmesiyle başladı. Bu dönüşüm, özel ve kamusal alanlarda genişleyen bir yelpazede kullanımı da beraberinde getirdi. İnternetin kurucuları ve ilk geliştiricileri, internetin yönetilmesi veya yönetişime ihtiyaç duyulması gerektiğini düşünmemişlerdi. IETF ve IANA'nın çalışmalarında da

görüldüğü üzere, aşağıdan yukarıya, işbirliğine dayalı ve büyük ölçüde gönüllü bir koordinasyon öngörülmüştü (WGIG Report, 2005, s. 6).

Teknik açıdan bakıldığında internet, ARPANET'in bir devamı niteliğindedir. Bu yaklaşım, interneti oluşturan tüm altyapının ve cihazların birbirine bağlanmasını sağlayarak ağ sistemlerinin düzgün çalışmasına yardımcı olan teknik katman ile ilişkilidir. Bu katmanda küresel yönetişim esnek, aşağıdan yukarıya ve fikir birliğine dayalı bir yapıdadır. Genellikle çok paydaşlı bir model izlendiği kabul edilir. Burada önemli olan bağlantı güvenliğini sağlamak, altyapıyı doğru şekilde yönetmek ve güvenli bir alan oluşturmak için siber uzayı açık ve uyumlu bir hale getirmektir (Solana & Lehmann, 2015, s. 13). Bu anlayışa göre tamamen kendi kendini yöneten veya düzenleyen bir internet, teknik mimarisiyle de tutarlı olacaktır. Bu modelin bugünkü düzenlemelerden temel farkı, aşağıdan yukarıya bir yaklaşımı benimsemesidir (Bauer, 2007, s. 14). Bunların bir kısmı, internetin paket anahtarlamalı teknolojisi ve protokollerinin doğasında ademi merkeziyetçi bir güç olduğunu savunur. Bu görüşe göre, internette merkezi bir otorite veya kontrol noktası bulunmaz ve güç son kullanıcılarda yer alır (Souter, 2021). Bu bakış açısını destekleyenler, internetin ilk yıllarındaki açık ve demokratik yapısını ve internetin sansüre karşı direncini örnek gösterirler.

Bu yaklaşımın savunucuları, internetin sürekli bağlantısını sağlamak için büyük ölçüde teknik koordinasyona odaklanmıştır. Fakat internetin ticaret ve güvenliğin merkezindeki küresel bir altyapıya dönüşmesi, yeni bir dizi sorun yaratmıştır. Mevcut yönetişim organları, ticaret, evrensel haklara uyum ve güvenlik gibi uluslararası sorunları ele almak için yeterli yetkiye ve uzmanlığa sahip değildir (Lewis, 2013, s. 5). Dolayısıyla internet yönetişimi artık teknik katmanla sınırlı bir alan değildir. Bu nedenle özellikle gizlilik, veri koruma gibi konularda teknik katman diğer katmanlarla bağlantılı olarak ele alınmalıdır. Zira ağın her bir katmanı, siyasi sonuçlar da doğurmaktadır (Korhan, 2017, s. 98). Örneğin, veri koruma politikaları ve yazılım geliştirmede gizlilik gibi farklı mekanizmalar birbiriyle bağlantılı olarak işlev görür. Bu nedenle, internet yönetişimi en iyi şekilde teknik boyutun ötesine uzanan bütüncül bir yaklaşım olarak anlaşılmalıdır. Yönetişimin karar alma nesneleri de oldukça çeşitlidir. Teknik standartlar, algoritmaların tasarımı, şifreleme gibi teknik konular kadar, blog yazarları, reklamcılar, mühendisler, kamu yetkilileri gibi insanlara ve onların davranışlarına da odaklanabilir (van der Spuy, 2017, s. 25).

Sonuç olarak internetin evrimi ve yönetişimine dair tartışmalar, teknolojinin sosyal, ekonomik ve politik boyutlarının nasıl iç içe geçtiğini göstermektedir. Teknik yaklaşım, internetin altyapısının ve standartlarının yönetilmesi açısından hayati önem taşırken, bu altyapının küresel bir iletişim ağı olarak işlev görebilmesi için çok paydaşlı bir modelin önemi de ortaya çıkmaktadır. İnternetin başlangıçta öngörülen merkeziyetçi yapısı, günümüzde karşılaşılan ticaret, güvenlik ve evrensel haklar gibi karmaşık sorunlar karşısında yeni yönetişim mekanizmaları ve iş birliklerini gerektirmektedir. Bu durum, internet yönetişimi konusundaki tartışmaların sadece teknik meselelerle sınırlı kalmadığını, aynı zamanda geniş bir paydaş yelpazesinin katılımıyla şekillenen siyasi ve sosyal bir alan olduğunu göstermektedir. Dolayısıyla internetin geleceğini şekillendirecek kararlar alınırken, bu geniş perspektifin ve çok boyutlu yaklaşımın göz önünde bulundurulması elzemdir.

1.2.4.2.Politik Yaklaşım

Küresel yönetişim alanında yükselen bir konu olan küresel siber yönetişim; yalnızca siber altyapı, kodlama ve standardizasyon gibi konuları içermez. Bunun yanında, siber güvenlik ve internet ile ilgili diğer ekonomik ve kültürel konuları da içermektedir (Akyeşilmen, 2018a, s. 259). Bu yaklaşıma göre siber yönetişim, teknik altyapının ötesine geçerek sosyal, ekonomik, kültürel, yasal ve politik konuları kapsamalıdır. İnternetin merkezi olmayan doğası, siber yönetişimin de benzer bir yapıda olmasını, yani merkeziyetçi yönetimden uzak, çok paydaşlı ve işbirliğine dayalı bir model olmasını savunur. Bu, her paydaşın katkısının önemli olduğu, yıkıcılık güçlerinin birbirine yakın olduğu ve ortak bir amaç için işbirliği yapılarak güvenli bir siber uzayın inşa edilebileceği anlamına gelir (Akyeşilmen, 2018a, s. 267).

Bu yaklaşıma göre esasında teknolojinin kendisi sosyal bir yapıdır. Bu yönüyle teknolojik gelişmeler yalnızca mühendislik ya da bilimle değil, aynı zamanda sosyal, kültürel ve politik unsurlarla da ilişkilidir. Bu nedenle teknolojiyi üretenlerin kültürel ve toplumsal yapısı, teknolojinin işlevselliğinden estetiğine kadar birçok yönünü etkilemektedir. Bu bağlamda teknoloji yalnızca bir araç değil, aynı zamanda vatandaşlar, işletmeler ve devletler arasındaki ilişkileri mümkün kılan, şekillendiren ve sınırlayan bir yapı olarak işlev görür (Bechtold, 2003, s. 1243).

Ramirez ve Choucri (2016), siber güvenlik yönetişiminde disiplinlerarası işbirliğinin önemine dikkat çekerek, bu işbirliğini kolaylaştırmak için standartlaştırılmış bir siber

güvenlik terminolojisinin gerekliliğini vurgular. Çalışmaları, teknik ve teknik olmayan paydaşlar arasında etkili bir işbirliği ve anlayış geliştirmek için ortak bir dilin ve terminolojinin önemini ortaya koyar. Bu birleşik terminoloji, siber güvenlik konularında farklı disiplinlerden gelen uzmanların birbirleriyle daha verimli bir şekilde iletişim kurmalarını sağlayarak, daha bütüncül ve etkili güvenlik stratejilerinin geliştirilmesine olanak tanır.

Politik yaklaşımın "yöneten" boyutunda ayrıldığı iki yaklaşım söz konusudur: merkezi ve merkezi olmayan yaklaşım. Bunlardan birincisi, egemen devletleri denetim, gözetim ve düzenleme politikaları açısından merkeze alan "merkezi" yaklaşımdır. Bu yaklaşımda daha çok siber faaliyetlerin iç hukuka uygulanması ve ülkelerin küresel yönetişimdeki söylemleri üzerinde durulmaktadır. Devletler; siber güç, hukuk ve kültür bakımından farklıdır. Bu nedenle mevcut küresel siber yönetişim yapısını sürdürmek veya reforme etmek için birbirinden farklı yollar izlemektedirler. Bir tarafta çok taraflı modeli savunan ülkeler yer alırken, diğer yandan çok paydaşlı bir model izlemek gerektiğini savunan bir taraf vardır. Kısacası küresel siber yönetişim, yoğunlaşan küresel tartışmanın odak noktasını oluşturmaktadır (Cuihong, 2018, s. 56).

Merkezi yaklaşım esasen geleneksel devlet düzenlemesini öngörür. Bu yaklaşım, uluslararası düzeyde yüksek oranda devlet müdahalesini öngörür. Tüm anlaşmalar devletlerarasıdır ve ulusal hükümetler, anlaşmaların uygulanması için hizmet eder. Anlaşmalarda genellikle ulusal hükümetler tarafından talep edilen çekinceler ve uyarılar yer almaktadır. Buradaki en belirgin sorun, devletlerin karşılıklı güven düzeyidir. Bunun yanında, bölgesel ve ulusal anlamda büyük farklılıklar ortaya çıkabilmektedir. Ancak genel olarak interneti geleneksel devlet yapısına dahil etmek onun dönüşüm potansiyelini baltalayacaktır. Bu durumda e-ticaret, mahremiyet ve fikri mülkiyet hakları gibi pek çok alanda, resmi devlet müdahalesi kaçınılmaz hale gelebilir (Bauer, 2007, s. 16).

Bu yaklaşım, siber savaş, devlet destekli siber saldırılar, devletlerarası casusluk ve kritik altyapıya yönelik saldırılarla ilgili konuları içermektedir. Burada küresel bir yönetişim çerçevesi mevcut değildir. İşbirliği ve uzlaşma ortamının oluşturulması nispeten daha zordur ve uluslararası örgütlerin rolü etkin değildir. Siber güvenlik, içerik denetimi veya gizlilik hakları gibi konularda ortak bir fikir birliği yoktur. Devletlerin hem savunma hem de saldırı alanında aktif olmaları karşılıklı güveni

aşındırmıştır. Dolayısıyla bu durum, ortak normlar üzerinde anlaşmayı da zorlaştırmıştır (Solana & Lehmann, 2015, s. 14).

Diğer yaklaşım ise, küresel internet yönetişiminin, geniş bir aktör ağı tarafından desteklenen bir süreç olduğunu savunan ademi-merkeziyetçi yaklaşımdır. Nye'ın (2014) analizine göre internet yönetişimi alanında devletler, özel sektör temsilcileri, uluslararası organizasyonlar ve sivil toplum kuruluşlarından oluşan farklı kurumların varlığı, karar alma süreçlerinin çoğulcu bir yapıya sahip olmasını sağlamaktadır. Bu kuruluşlar, dijital düzende karar verme mekanizmalarına aktif olarak katılmakla beraber, yönetişimle ilgili standartlar ve kuralların belirlenmesinde de önemli bir yetkiye sahiptirler. Filgueiras ve Almeida, yaptıkları ortak çalışmalarında siber uzayın yönetişim modelinin ne "daha fazla devlet" ne de "daha fazla pazar" olduğunu savunmuşlardır (2021, s. 107). Zira siber uzay, gücün yalnızca devlet otoritesinde merkezileştiği bir sistemle yönetilemez. Couldry ve Mejias (2018), veri ve bilgi üzerinde devlet kontrolünün siber uzayda "kolonizasyon"u tetikleyeceğini ve mevcut gözetim sistemlerini güçlendireceğini iddia etmişlerdir. Onlara göre bu süreç aynı zamanda devletler arasında yeni bir çatışma düzeni yaratacağından, siber uzayın yönetişimi jeopolitik anlamda da sorun haline gelecektir.

Bu iki uç arasında bir "gri bölge" olan bir yaklaşımdan da bahsedilebilir. Bu bölgede özel sektör, devletler ve bireylerin çıkarlarının kesiştiği bir alan söz konusudur. Bu alanda fikri mülkiyet hakları, devlet dışı aktörlerin bireylere yönelik siber saldırıları, suç faaliyetleri ve veri koruma gibi çeşitli konular yer almaktadır. Bu katmanda siber uzayın yönetişimi teknik veya politik bir yaklaşımdan ziyade, tüm uluslararası araçları kapsayan bir yaklaşımla ele alınmaktadır. Burada uluslararası kurumlar, doğaları ve amaçları bakımından oldukça çeşitlidir. Burada ne çok taraflı ne de çok paydaşlı bir model hakimdir. Siber yönetişimin bu katmanında uluslararası kurumlar, devlet merkezli çok taraflı resmî kurumlar, düzenleyici mekanizmalar, gayrı-resmi forumlar ve özel kuruluşlar gibi pek çok aktör bulunmaktadır. Gri alanda siber uzayla ilgili kurumların dışındaki uluslararası kuruluşlar da oldukça etkilidir. Burada uluslararası toplum, siber tehditleri azaltarak siber yönetişimi önemli ölçüde iyileştirmeyi amaçlamaktadır. Bu bağlamda tekdüze bir yönetişim anlayışından ziyade karmaşık yönetişim modelleri yer almaktadır (Solana & Lehmann, 2015, s. 14). Hem her ülkenin kurumsal kültürünü gözeten, hem de uluslararası yönetişim anlayışı ile uyumlu bir model mevcuttur.

Sonuç olarak internet, hem teknik hem de politik boyutlarıyla incelenmesi gereken kompleks bir ağ yapısını temsil etmektedir. Teknik açıdan internet, bilgi ve iletişim için yenilikçi bir altyapı olarak kabul edilmekte iken; yeni teknolojiler ve araçlar sayesinde işlevselliği ve kullanımı şekillenmekte, verimlilik, erişilebilirlik ve bağlantılılık gibi kavramlar öne çıkmaktadır. Politik açıdan ise internet, güç ve etki mücadelesi için yeni bir arena olarak görülmekte, devletler, sivil toplum kuruluşları ve özel sektör aktörleri kontrol için rekabet etmekte, egemenlik, sansür ve gözetleme gibi konular önem kazanmaktadır. Her iki perspektifin de dikkate alınması internetin adil ve sorumlu kullanımını teşvik edecektir. Bu yöntemle hem teknik hem de politik ihtiyaçları karşılayan çözümler geliştirilebilir. Dolayısıyla interneti yalnızca teknik veya politik bir sorun olarak değerlendirmek, bu çok yönlü yapıyı tam anlamıyla kavramaktan uzak bir yaklaşım olacağından, her iki bakış açısının da entegre edilmesi gerekir.

1.2.5. Yönetişim Tartışmalarının Uluslararasılaşması

1.2.5.1.Uluslararası Konferans ve Zirveler

Aşağıda özetlenen ilgili konferanslardaki tartışmalar, internet yönetişiminin esnek uygulamalardan daha "sistematik" ve "küresel" bir yaklaşıma doğru evrildiğini göstermektedir. Bu evrim, çeşitli paydaşların artan bir şekilde etkileşimde bulunduğu ve ortak yönetişim stratejileri geliştirdiği bir ortamın oluşmasına katkıda bulunmuştur. Bu süreç, internetin küresel doğasına uygun, daha entegre ve katılımcı bir yönetişim modelinin gelişimini teşvik etmiştir.

i. Dünya Bilgi Toplumu Zirvesi

BM, bilgi ve iletişim teknolojileri alanında uluslararası işbirliği ve güvenlik konularında önemli adımlar atmıştır. 1996 yılında Güney Afrika'da gerçekleştirilen BM Bilgi Toplumu ve Kalkınma Konferansı ve 1999 yılında Paris'te yapılan Terörle Mücadele Bakanlar Konferansı sonrasında, aşağıdaki önemli gelişmeler kaydedilmiştir: 1) Uluslararası toplumun, "bilgi ve iletişim teknolojilerinin genişletilmesi ve kullanımı" konusundaki ortak çıkarları; 2) Bilgi ve iletişim teknolojilerinin, uluslararası istikrar ve güvenlik için potansiyel tehditler oluşturabileceği yönündeki artan endişeler; 3) Üye devletlerden, bilgi güvenliği ile ilgili kavramlar, genel bilgi güvenliği konuları ve uluslararası ilkelerin oluşturulması gerekliliği hakkında raporlar talep edilmesi; 4) Bilgi ve telekomünikasyonun uluslararası güvenlik perspektifindeki rolünün BM Genel Kurulu'nda ele alınması. Bu süreçte BM, üye devletlerin bilgi toplumu ve siber

güvenlik konularında son 20 yıllık ilerlemesini özetleyen toplantılar düzenlemiştir (Fang, 2018, s. 244).

İnternet yönetişimi ile ilgili uzlaşmazlıkları çözmek amacıyla oluşturulmuş uluslararası girişimlerden biri WSIS idi. WSIS, BM himayesi altında ITU tarafından geliştirilen ve düzenlenen çok paydaşlı bir dizi uluslararası konferanstı. 1999 yılında BM Genel Sekreteri, WSIS fikrini onayladı ve diğer BM organları ve bağlı kuruluşların üst düzey yöneticilerinden oluşan bir Yüksek Düzeyli Zirve Organizasyon Komitesi (HLSOC) atadı (Hubbard & Bygrave, 2009, s. 213). Sürecin bir sonraki kısmı, ITU'nun böylesine iddialı bir girişimin başarısı için gerekli olan maddi ve prosedür unsurlarını geliştirmesiydi. ITU Konseyi, Zirve'nin iki aşamada yapılmasını önerdi. Cenevre'deki ilk aşama Aralık 2003'te yapılacak ve tüm üyelerin üzerinde anlaşabileceği bir İlkeler Bildirgesi ve Eylem Planı oluşturulacaktı. Tunus'taki ikinci aşama, Eylem Planı'ndaki ilerlemeyi gözden geçirmek ve 2015 yılına kadar hedeflere ulaşmak için somut bir gündem geliştirmek amacıyla 2005 sonlarında planlandı. BM Genel Kurulu, 21 Aralık 2001 tarihli 56/183 sayılı Karar ile ITU önerisini onayladı. Bu Karar yoluyla Genel Kurul, ITU'yu Zirve'nin tüm hazırlık süreçleri için birincil kurumsal sorumlu olarak kabul etti (Hubbard & Bygrave, 2009, s. 215). Nihai olarak WSIS, ilki 2003'te Cenevre'de ve ikincisi 2005'te Tunus'ta olmak üzere iki forum halinde gerçekleşti.

WSIS, küresel internet yönetişimi için üç önemli sonuç ortaya çıkarmıştır. İlk olarak WSIS, internet yönetişimini teknik meselelerden bağımsız bir şekilde kamu politikasına doğru genişletmiştir. Bunun en önemli göstergesi ise yukarıda sıklıkla atıfta bulunulan internet yönetişimi tanımıdır. İkinci olarak WSIS, küresel internet yönetişimine dair sorunların tartışılması amacıyla bağlayıcı politika yapma yetkisi olmayan ancak yıllık olarak düzenlenen toplantılarda çok paydaşlı bir katılımın sağlandığı IGF'yi kurmuştur Üçüncüsü, tanımdan da anlaşılacağı üzere WSIS, internet yönetişimi anlayışına çok paydaşlılık ilkesini kazandırmıştır. IETF, ICANN gibi kuruluşlara ek olarak devletler, özel sektör ve kullanıcılar gibi paydaşların da karar alma sürecine dahil edilmeleri, bu sürecin çok paydaşlı bir mahiyet kazanmasında büyük rol oynamıştır (Mueller, 2010, s. 78).

Öte yandan WSIS, internet yönetişimini küresel iletişim politikasının önemli bir sorunu olarak yansıtması açısından büyük önem teşkil eder. Zira bunun sonucunda internet yönetişimi, devletlerin dış politikalarında ve küresel politikada önemli meseleler haline

gelmiştir (Choucri, 2012; DeNardis, 2014). WSIS, devlet ve devlet-dışı aktörler nezdinde internet yönetişimine ilişkin politika söylemini teknik alandan küresel alana taşımıştır (Hubbard & Bygrave, 2009, s. 213). Bu yönüyle WSIS, internet yönetişiminin "jeopolitik bir alan" olarak tanınmasındaki ilk adım olarak kabul edilebilir (Mueller, 2010, s. 68).

ii. İnternet Yönetişimi Çalışma Grubu

11 Kasım 2004 tarihinde BM Genel Sekreteri Kofi Annan, Cenevre'de ifade edilen talepler doğrultusunda İnternet Yönetişimi Çalışma Grubu'nun (WGIG) kurulduğunu açıkladı. Çalışma Grubu'nun görevi, Kasım 2005'te Tunus'ta düzenlenecek olan WSIS'in ikinci aşamasında bir karar alınması için zemin hazırlamaktı (ICANN Archives, t.y.). Bu grubun oluşturulmasıyla birlikte internet yönetişiminin küreselleştiği iddia edilmektedir (Hubbard & Bygrave, 2009, s. 224).

WGIG'in görevi, tüm paydaşlar arasında internet yönetişimi konusunda açık bir diyalog düzenlemek ve WSIS'in ikinci aşamasına bu konuda tavsiyeler getirmekti (ICANN Archives, t.y.). Topluluk; internet yönetişiminin tanımını geliştirmek, kamu politikası sorunlarını belirlemek ve çeşitli paydaş gruplarının birlikte nasıl çalışabileceğini önermekle görevlendirilmiş ve bu işlevleri yerine getirmiştir. Diğer yandan, internetin teknolojik, yasal, kültürel ve politik yönleri üzerindeki görüş farklılıklarını ve sorunları belirlemiştir.

WGIG'in önemli bir başarısı, internet yönetişimi konularının ele alınması için BM'ye bağlı açık, çok paydaşlı bir forum oluşturma önerisiydi (WGIG Report, 2005). Bu öneri, Tunus Gündemi'nde onaylandı ve IGF kuruldu. WGIG Nihai Raporu, Küresel Kamu Politikası ve Gözetim için çeşitli alternatif modelleri araştırmayı öngörmüştür. Bu modellerden en belirgin olanı, ICANN'in değiştirilmesi ya da gözetim işlevlerinin ABD Ticaret Bakanlığı'ndan yeni bir uluslararası kuruluşa aktarılmasını öngören modeldi. Bu modelin DNS yönetiminin mevcut yapısında büyük değişiklikler önerdiği söylenebilir. Önerilen model, BM'ye bağlı hükümetlerarası bir Küresel İnternet Konseyi (GIC) öngörmüştür. Bu konseyin, ABD Ticaret Bakanlığı'nın internetin uluslararası yönetimi üzerindeki işlevlerini üstlenecek ve aynı zamanda ICANN Devlet Danışma Komitesi'nin (GAC) yerini alacaktı (WGIG Report, 2005, s. 13). Ancak ne bu model ne de önerilen diğer modeller çok tartışılan konular olmasına rağmen, Tunus Gündemi'nde onaylanmamıştır (Hubbard & Bygrave, 2009, s. 226).

iii. Dünya Uluslararası Telekomünikasyon Konferansı

İnternet yönetişimine yönelik ulusal ve uluslararası yaklaşımlardaki farklılıkların artması, küresel internet düzeninin de tehdit altında olduğuna dair korkuları artırmaya başladı (Mueller, 2017). İnternet yönetişimine dair farklılıkların git gide arttığı ve yönetişim faaliyetinin yeni bir jeopolitik tartışmanın ortasına çekildiği bir dönemde önemli bir konferans gerçekleştirilmiş ve endişeler burada dile getirilmiştir. 3-14 Aralık 2012 tarihinde Dubai'de gerçekleşen Dünya Uluslararası Telekomünikasyon Konferansı (WCIT), bu yönüyle önemli bir dönüm noktası olmuştur (ITU, 2012).

ITU bünyesinde gerçekleştirilen WCIT, ITU'nun uluslararası telekomünikasyon hizmetlerinin sağlanması için bağlayıcı olan ancak güncelliğini yitirmiş 1988 tarihli Uluslararası Telekomünikasyon Yönetmelikleri (ITR) antlaşmasının yeniden müzakere edilmesi için düzenlenmiştir. WCIT, küresel iletişim politikasının oluşturulmaya çalışıldığı en tartışmalı dönemlerden birinde düzenlenmiş olması nedeniyle önem arz etmektedir (Brooks, 2012).

WCIT-12, birçok ülkenin internetin yönetişimine dair kendi vizyonlarını ve politikalarını dile getirdiği bir platform olmuştur. Bu, hem uluslararası işbirliği için fırsatlar sunmuş hem de çeşitli ülkeler arasında internet yönetişimi konusunda fikir ayrılıklarının ve çatışmaların ortaya çıkmasına neden olmuştur. Örneğin, bazı ülkeler internetin daha fazla devlet kontrolünü savunurken, diğerleri internetin özgür ve açık kalmasının önemini vurgulamıştır. Burada yaşanan en önemli tartışmalardan biri, internet yönetişiminin geleceği ve uluslararası telekomünikasyon düzenlemelerinin internet üzerindeki etkisi konusundaydı (Fidler, 2013a). Bir yandan, internetin küresel doğası ve sınır ötesi etkileşimleri, uluslararası koordinasyon ve işbirliğinin önemini artırmaktadır. Diğer yandan, ulusal güvenlik, yerel yasalar ve kültürel değerler gibi konular, ulusal düzeyde internet yönetişimine yönelik farklı yaklaşımların benimsenmesine yol açmaktadır.

WCIT-12'nin sonuçları, uluslararası toplumun internet yönetişimi konusunda birlikte çalışma konusunda hem fırsatlar hem de zorluklarla karşı karşıya olduğunu göstermiştir. Bazı önemli anlaşmazlıklar ve farklı görüşler devam etmekle birlikte, konferans aynı zamanda ülkelerin ortak hedeflere ulaşmak için bir araya gelebileceği ve küresel internet düzenini güçlendirebileceği bir diyalog ve işbirliği platformu sağlamıştır.

1.2.6. "Kaynak" Yönetişiminden "Tehdit" Yönetişimine Evrim

Dünya genelinde büyük miktarda bilgi ve veri akışı söz konusudur. 1992'de internet trafiği günde yaklaşık 100 GB (Gigabayt) iken bugün 7 milyar GB civarında bir trafik söz konusudur. Ocak 2024 itibariyle dünya genelinde 5,35 milyar internet kullanıcısı mevcuttur ve bu rakam küresel nüfusun %66,2'sine tekabül etmektedir (Statista, 2024). Bu oran, 1995 yılında %1'den azdı (Internet Live Stats, 2024). Özellikle küreselleşme süreci ile birlikte küresel ekonomi için kamu ve özel sektör arasındaki veri aktarımı artmış ve bilginin kendisi önemli bir "hammadde" haline gelmiştir (Kuner, 2013, ss. 1-6). BİT'in devletler, kuruluşlar ve bireyler gibi aktörler arasında ulusal veya bölgesel anlamda sınır tanımaksızın dünyanın her yerine veri aktarabilmesi ve bunu anında yapması, birtakım endişeleri de beraberinde getirmiştir. Dolayısıyla siber uzayın aktörleri, veri akışının düzenlenmesine yönelik adımlar atmaya başlamıştır.

Veri akışlarının düzenlenmesine ilişkin endişeler özellikle "sınır ötesi veri akışları" bağlamında olmuştur. Bunun en belirgin yaşandığı dönem ise bilginin giderek daha önemli hale geldiğine dair bir algının oluştuğu 1970'lere ve 1980'lere kadar uzanmaktadır (Robinson, 1987, s. 369). 1974 yılında bir OECD uzman grubu toplantısında ilk kez "sınır ötesi veri akışı" terimi ortaya atıldı (UNCTAD Report, 2017, s. 94). Bu gelişmelere paralel olarak, ekonomik gelişme ve kişisel mahremiyetin korunmasına dair endişeler de söz konusuydu. Örneğin, 1980'de OECD, BİT'in sağladığı ekonomik avantajları göz önüne alarak veri akışına büyük oranda müdahale etmemiş, daha asgari düzeydeki önlemlere başvurmuştur. Bunun yanında, kişisel verilerin korunmasına yönelik yönergeler de yayınlamıştır.[9] Benzer şekilde UNESCO, 1984 yılında sınır ötesi veri akışlarını düzenlemenin önemi vurgulamıştır. Sınır ötesi veri akışlarını düzenlemek ve kaostan kaçınmak amacıyla "bilişim için bir tür uluslararası trafik kuralları kanunu oluşturma" çağrısı yapmıştır (UNESCO, 1984).

Bu çağrıların yapıldığı dönemde henüz World Wide Web veya Nesnelerin İnterneti gibi teknolojiler geliştirilmemişti. 1980'lerde bilginin gittikçe daha merkezi hale geldiği ve uluslararası veri akışlarını düzenlemek için kurallara ihtiyaç duyulduğu tartışılmaya başlandı. Kurallara duyulan bu ihtiyaç, yalnızca ekonomik veya toplumsal endişelerden değil, uluslararası güvenlik ve çatışmaya kadar varan endişelerden kaynaklanmaktaydı.

[9] Ayrıntılı bilgi için bkz: OECD. (t.y.). OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data https://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm (10.04.2021).

Bu dönemde kişisel mahremiyet, siyasi özgürlük, ulusal ekonomik kalkınma, kültürel kimlik ve ulusal egemenlik gibi konular, sınır ötesi veri akışları bağlamında değerlendirilmeye başlandı (Fishman, 1980, s. 1).

1980'lerde telgraf gibi teknolojiler için de düzenlemeler yapılmış ve bunlar çoğunlukla ulusal sınırlardan bağımsız olarak çalışan yeni teknolojileri düzenlemeye yönelik girişimlere ön ayak olmuştur. Bu bağlamda kurulan Uluslararası Telgraf Birliği, yeni teknolojinin ortaya çıkardığı sorunlara yanıt olarak kurulmuş ilk uluslararası kuruluştur. Reinalda'ya göre on dokuzuncu yüzyılın uluslararası telgraf ve posta kuruluşları, modern kapitalizm ve teknolojinin genişlemesine yanıt vermelerine karşın; ulusal sınırları dikkate almamışlardır (2009, s. 83).

Uluslararası Telgraf Birliği, bir yandan bilginin hızlı aktarımını sağlamak amacıyla devletlerin telgraf altyapısını geliştirmeye çalışmış, diğer yandan uluslararası hukuka aykırı sayılan bilgi akışını sınırlandırmaya çalışmıştır (International Telegraph Convention, 14 Ocak 1872, Madde 1&2). Bu düzenlemeler yalnızca telgrafı kapsamamış, telefon, televizyon ve radyo gibi teknolojilerden iletilen verileri de kapsamıştır. Örneğin, 1936 tarihli Barış Amaçlı Yayın Kullanımına İlişkin Uluslararası Sözleşme, bir devletin iç düzenine zarar veren veya onunla bağdaşmayan her türlü yanlış bilgi veya propaganda aktarımını yasaklamayı amaçlamıştır. Sözleşmenin 3. Maddesinde, yanlış bilginin "iyi uluslararası anlayışa" (*good international understanding*) zarar verme olasılığının yüksek olduğu belirtilmiştir (International Convention concerning the Use of Broadcasting in the Cause of Peace, 23 Eylül 1936).

Uluslararası Telgraf Birliği'nin halefi ITU, "farklı ülkelerin radyo istasyonları arasında zararlı girişimi önlemek" ve "farklı ülkelerin radyo istasyonları arasında zararlı girişimi ortadan kaldırmak için çabalamak" amacıyla radyo frekanslarını tahsis etme ve kaydetme görevini yürütmüştür. Benzer şekilde bilgisayar sistemlerine ve verilerin kullanımına ilişkin bazı düzenleme ve kısıtlamalar getirilmiştir. Devletlerin iç hukuk mekanizmalarında yer alan kısıtlamalara ek olarak, Siber Suçlar Sözleşmesi gibi uluslararası sözleşmelerle de ağların uygunsuz kullanımlarına ilişkin cezai işlemler uygulanmakta ve bu kullanımlar yasa dışı olarak kabul edilmektedir (CoE, 2001). Siber Suç Sözleşmesi, ulusal yasaların uyumlaştırılması yoluyla ağların ve verilerin zararlı kullanımlarını düzenlemeyi amaçlamaktadır. Sözleşme'nin 2. Maddesinde, bilgisayar sistemlerine haksız yasadışı erişimin önlenmesine atıfta bulunulurken; 3. Maddesi

gizlilik haklarının ihmal edilerek verilerin ele geçirilmesini içerir (CoE, 2001, s. 3). Sözleşmeden anlaşılacağı üzere siber uzaydaki suç faaliyetlerinden kaynaklanabilecek zararların uluslararası hukuk bağlamında düzenlenmesi giderek daha fazla önem kazanmaktadır. Zira devletlerin BİT'e artan bağımlılığı göz önüne alındığında uluslararası barış ve güvenliği zayıflatma potansiyeline sahip zararlı veri akışları düzenlenmeye daha fazla ihtiyaç duymaktadır.

Görüldüğü üzere "gücü oluşturabilecek bilgilerin aktığı bu alan kısa sürede güvenlik problemleriyle anılır hale gelmiştir" (Bıçakçı, 2014, s. 102). Devletlerin veri akışlarını düzenlemeye yönelik uluslararası girişimlerine rağmen dijital veri akışlarının mevcut düzenlemesi ve yönetimi, çeşitli kamu ve özel aktörleri de kapsamaktadır. Başlangıçta daha küçük bir teknik topluluk tarafından düzenlenmiş olsa da bugün internet teknik protokolleri ve standartları özel aktörlerden oluşan ICANN ve devlet ve devlet dışı aktörlerden oluşan BM'ye bağlı ITU tarafından düzenlenmektedir. Çalışmanın dördüncü bölümünde detaylı olarak ele alınacak bu kurumlar, dijital alanın yalnızca teknik alanıyla ilgilenmeyip, aynı zamanda politik düzenlemeler konusunda da söz sahibi olmak için çabalamaktadır.

1.2.7. Dijital Yönetişimin Aktörleri

"İnternet yönetişimi, küresel paydaşların bundan anladığı şeydir" der Pigatto vd. (2021). Dolayısıyla farklı küresel paydaşlar arasında internet yönetişimine ilişkin farklı bakış açılarının mevcut olduğu ve bu durumun interneti küresel düzeyde yönetmeyi zorlaştırdığı söylenebilir. İnternet yönetişimi, internetin geleceğine dair kararların alındığı, devletler, özel sektör, sivil toplum ve teknik topluluk gibi çeşitli paydaşların yer aldığı karmaşık bir süreçtir. Her bir paydaş grubunun internetin nasıl yönetilmesi gerektiğine dair farklı çıkarlara ve görüşlere sahip olması, internet yönetişimindeki güç dinamiklerini daha da karmaşıklaştırmaktadır.

Devletler, interneti düzenleyerek ve kontrol ederek ulusal güvenlik ve kamu düzeni gibi unsurları koruma eğilimindedirler. Öte yandan özel sektör, internet altyapısı ve hizmetlerinin sağlanmasında önemli bir rol oynar ve internetin kendi çıkarları doğrultusunda kârlı bir platform olarak kalmasını ister. Sivil toplum, internetin açık, erişilebilir ve demokratik bir platform olarak kalmasını savunarak kullanıcı hakları ve ifade özgürlüğünün korunmasını önemser. Teknik topluluk ise internetin teknik altyapısının geliştirilmesi ve korunmasını, açık ve standartlara dayalı bir platform

olarak sürdürülmesini önceliklendirir. Bu gruplar, güç dengesini sürekli olarak değiştiren ittifaklar kurarak internet yönetişimindeki etkilerini artırmaya çalışır. Bu güç dengesi, internetin yönetişimi, kimlere fayda sağladığı ve geleceği üzerinde önemli etkilere sahiptir. Güçlü paydaşların aşırı etkisi, internetin açık, erişilebilir ve demokratik bir platform olma niteliğini tehdit edebilirken, bu paydaşların altyapı ve hizmet sağlamadaki rolleri internetin gelişimi için zorunlu olabilmektedir.

İnternetin ticarileşmeye başladığı zamanlardan bu yana, siber uzayın kontrolünün küresel mekanizmalar tarafından mı yoksa ulus devletler tarafından mı sağlanacağı konusunda farklı görüşler bulunmaktadır. Temelde küresel internet yönetişimine dair tartışmalar bu temel soru üzerinde şekillenmiştir (Goldsmith & Wu, 2006, s. 150). Bu tartışmaların nispeten "yeni" olarak kabul edilebileceği bir dönemde WSIS, internet yönetişimine beş farklı paydaş grubunu dahil ederek alanın yönetişimi için çok paydaşlı bir modeli işaret etmiştir. Bunlar; devlet, özel sektör, sivil toplum, hükümetlerarası kuruluşlar ve uluslararası kuruluşlardır.

WSIS tarafından atanan roller ve sorumluluklar, Tunus Gündemi'nin 35. paragrafında tanımlanmıştır. Paragrafta internet yönetişiminin hem teknik hem de kamu politikası konularını kapsadığı belirtilmiştir. Bunun yanında, internet yönetişiminin tüm paydaşları kapsaması gerektiği ifade edilmiştir. Bu bağlamda Tunus Gündemi'nin 35. Paragrafında aşağıdaki sıralanan maddeler kabul edilmiştir:

a. İnternet ile ilgili kamu politikası sorunları için politika otoritesi, devletlerin egemenlik hakkıdır. Devletin internetle ilgili uluslararası kamu politikası sorunları için hakları ve sorumlulukları vardır.
b. Özel sektör, internetin gelişiminde hem teknik hem de ekonomik alanlarda önemli bir role sahiptir ve bu rolü sürdürmeye devam etmelidir.
c. Sivil toplum, özellikle toplum düzeyinde internet konularında önemli bir rol oynamış ve oynamaya devam etmelidir.
d. Hükümetlerarası kuruluşlar, internet ile ilgili kamu politikası konularının koordinasyonunda kolaylaştırıcı bir role sahip olmuş ve sahip olmaya devam etmelidir.

e. Uluslararası kuruluşlar da internet ile ilgili teknik standartların ve ilgili politikaların geliştirilmesinde önemli bir role sahip olmuş ve sahip olmaya devam etmelidir (ITU, 2005a).

35. Paragrafta teknik ve ekonomik yönlerin gelişiminde özel sektörün rolü kabul edilirken; uluslararası kamu politikası alanlarında devletlerin egemenlik hakkının bulunduğu ifade edilmiştir. Gündem tarafından sivil topluma, özellikle toplum düzeyinde önemli bir rol verilmiştir. Koordinasyon rolü için hükümetlerarası kuruluşlar uygun görülürken; uluslararası kuruluşlar, teknik standartlarda ve ilgili politikalarda önemli görülmüştür. Ancak tamamen açık bir iş bölümü yapmanın mümkün olmadığı Gündem tarafından da dile getirilmiştir. Gündem bu durumu, "tüm rollere değerli katkıda bulunanlar" şeklinde açıklamıştır (Tunus Gündemi, Par. 36).

Genel olarak çok paydaşlı yaklaşımların tartışmalı bir yönü, WSIS tanımındaki "kendi rolleri dahilinde" ifadesidir. Her paydaş grubu için roller ve sorumluluklar ayrı ayrı detaylandırılmıştır. İnternetle ilgili kamu politikası konuları için "politika otoritesinin egemenlik hakkı" devletlere aittir, özel sektörün ise "teknik ve ekonomik alanlarda" internetin geliştirilmesinde "önemli bir rolü" olmaya devam etmesi gerekmektedir. Uluslararası organizasyonlar, internetle ilgili teknik standartların ve ilgili politikaların geliştirilmesiyle görevlendirilirken; sivil toplumun ise özellikle topluluk düzeyinde internet meselelerinde "önemli bir rol oynamaya" devam etmesi gerektiği ifade edilmiştir. Çok taraflı hükümetlerarası organizasyonların ise ilgili kamu politikası konularının koordinasyonunda "kolaylaştırıcı bir rol" üstleneceği belirtilmiştir (van der Spuy, 2017, s. 27).

WSIS tanımı, internet yönetişimi sürecindeki önemli paydaşları tanımlamada faydalı bir başlangıç noktasıdır. Ancak, bu tanımın sınırlamalarının farkında olmak ve internet yönetişiminin gerçek karmaşıklığını ve nüanslarını anlamak önemlidir. WSIS tanımı, internet yönetişiminde devletler, uluslararası kuruluşlar, özel sektör ve sivil toplum gibi belirli paydaş gruplarına atıfta bulunur. Bu, karmaşık bir dinamik yaratır, çünkü yukarıda da belirtildiği üzere her bir paydaş grubunun farklı çıkarları ve rolleri vardır. Dolayısıyla bu süreç, devletlerin ulusal çıkarlarını temsil ederken; aynı zamanda bireysel çıkarları da gözetmelerini gerektirir. Zira internet, devletlerin çıkarlarının ötesinde, özel çıkarları da barındırmaktadır. Hatta çoğu zaman bu özel çıkarlar, ulusal çıkar çatışmalarına dahi yol açabilecek düzeyde olabilmektedir (van der Spuy, 2017, s.

26). Bu nedenle, internet yönetişiminin yalnızca devletlerin çıkarlarının temsil edildiği tek taraflı bir süreç olmadığı vurgulanmalıdır. Buradaki faaliyetler, çeşitli paydaşların katılımıyla gerçekleşir. Bu nedenle her bir paydaşın katılımı, diğerlerinin rollerini ve çıkarlarını gölgelememeli, aksine geniş bir yelpazedeki aktörlerin etkileşim içinde olmasını sağlamalıdır. Devletin buradaki rolü, yalnızca belirli politikaları belirlemekle kalmayıp, aynı zamanda geniş internet yönetişimi konularına katkı sağlayacak şekilde evrilmelidir.

Bazıları, bu süreçte paydaş kategorizasyonuna aşırı odaklanmanın bu grupların gerçekte sahip oldukları çıkarları ve katkıları gölgeleyebileceğini iddia etmektedir. Özellikle, teknik ve akademik topluluklar gibi bazı grupların, ayrı paydaşlar yerine kesişen çıkarlara sahip gruplar olarak değerlendirilmesi gerektiği belirtilmiştir. Bu, yanlış temsillere yol açabilir ve çok paydaşlı yaklaşımın temel amacı olan çoğulcu bilgi ve uzmanlık temelli bir politika hazırlama sürecini zayıflatabilir (Belli, 2015, ss. 5-6). Örneğin; gizlilik konusunda, bireylerin ve gizlilik odaklı sivil toplum kuruluşlarının kullanıcı verilerinin korunması ve şeffaflık konusunda daha katı düzenlemeler istemesi muhtemeldir. Öte yandan, büyük veri analitiği[10] ve hedefli reklamcılık[11] faaliyetlerinden yararlanan büyük teknoloji şirketleri, bu tür düzenlemelere karşı çıkabilir. Bu, gizlilik konusunda farklı paydaşların çıkarlarının nasıl çatışabileceğine bir örnektir.

Aşağıda paydaş kategorizasyonuna sadık kalınarak –fakat biraz da ayrışarak–[12] internet yönetişiminde etkili olan paydaşların somut ifadelerle tanımlanmasından ziyade, paydaşların geniş bir perspektifte –rolleri, sorumlulukları ve beklentileri bağlamında– yorumlanması amaçlanmıştır. Zira bu sürece dahil olması gereken belirli paydaşların rolü, küresel internet yönetişimi sorununun doğasına bağlı olarak değişkenlik

[10] Büyük veri analitiği, büyük ve karmaşık veri setlerinden değerli bilgilerin, kalıpların, eğilimlerin ve ilişkilerin keşfedilmesi için kullanılan süreçler ve teknikler bütünüdür. Geleneksel veri işleme uygulamalarının yetersiz kaldığı büyüklükteki veya karmaşıklıktaki verilerle çalışır. Büyük veri analitiği, işletmelerin ve organizasyonların veriye dayalı daha bilinçli kararlar almasına imkân tanır. Ayrıntılı bilgi için bkz: (BMSCE, t.y.).

[11] Hedefli reklamcılık, reklam verenlerin belirli demografik özelliklere, ilgi alanlarına, davranışlara veya önceden belirlenmiş kriterlere göre segmente edilmiş hedef kitlelere özel reklamlar sunmasını sağlayan bir reklam stratejisidir. Bu yaklaşım, reklamların ilgili ve potansiyel olarak daha etkili olmasını sağlamak için kullanıcı verileri ve analizlerinden yararlanır. Hedefli reklamcılık, çeşitli kanallar ve platformlar aracılığıyla gerçekleştirilebilir, bunlar arasında sosyal medya, arama motorları, web siteleri, mobil uygulamalar ve daha fazlası bulunmaktadır. Bu yöntem, reklamın doğru kişilere ulaşmasını sağlayarak reklam bütçesinin daha verimli kullanılmasına olanak tanır. Ayrıntılı bilgi için bkz: (Shin &Yu, 2021).

[12] WSIS, kategorizasyona sivil toplumu dahil ederken, bireyleri/kullanıcıları göz ardı etmiştir. Çalışmada bireyler de kategorizasyona dahil edilecektir.

göstermektedir. Burada internet yönetişimi konusunda meşru bir menfaati olan her bir aktör, "paydaş" olarak kabul edilmiş ve bu kavram geniş bir şekilde yorumlanmıştır.

1.2.7.1.Devletler

Tarih boyunca ulus-devletler, "yönetim sanatında" temel bir rol oynamışlardır. Diğer devletlerle kurdukları ilişkilerle hem güç dağıtımını gerçekleştirmiş hem de meşruiyet kazanarak konumlarını sağlamlaştırmışlardır. Bunu, kendilerini belirli bir bölge üzerinde yaşayan insanların temsilcisi olarak konumlandırarak ve uluslararası ile yerel düzeyler arasında bir aracı görevi görerek gerçekleştirmişlerdir (Hirst & Thompson & Bromley, 2009, s. 322). Westphalian yönetişim modeli, ulus devletlerin egemenliğini ve uluslararası ilişkilerde merkezi rolünü savunur. Bu modelde devletler, kendi halklarının çeşitli normlarını ve çıkarlarını temsil eder ve bunları dış etkilerden korumak ve geliştirmek için çalışır. Küresel yönetişimin ortaya çıkışı, alternatif temsil ve siyasi örgütlenme biçimlerini yeniden gözden geçirmemiz için bize alan açmıştır. Ancak bu aşamada devletlerin vatandaşlarının çıkarlarını koruma ve destekleme sorumluluğundan kurtulduğu söylenemez. İnternet yönetişimi bu açıdan çekişmeli bir alan olmaya devam etmektedir. Bunun başlıca nedeni, farklı normlar ve çıkarlar içeren küresel bir ağ üzerinde egemenlik ve kontrol kurma sorunudur (Carr, 2015; van der Spuy, 2017, s. 32).

Devletlerin internet yönetişimindeki rolleri de internet yönetişimi düzenlemelerinde egemenliğin sağlanmasıyla ilgili endişelerin merkezinde yer alır. Küresel internet yönetişiminin 2000'li yıllardan itibaren daha çok gündeme gelmeye başlamasının en önemli nedeni, çok sayıda devletin interneti yerel ve uluslararası olarak yönetme yetkisini elinde bulundurmak istemesiydi (Goldsmith & Wu, 2006, s. VII; Mueller, 2010, s. 1). Bu endişeler, çoğunlukla internet yönetişimi mekanizmalarındaki güç dengesizliklerini ortaya çıkarmaktadır. Çoğu devletin internet yönetişimi sürecine "geç" katılmış olması ve özel sektörün sahip olduğu teknik ve erişim kapasitesine sahip olmaması (yargısal kısıtlamalar nedeniyle) bu güç dengesizlikleri tartışmalarının merkezinde yer almaya başlamıştır (van der Spuy, 2017, s. 32).

Devletlerin bu alana nispeten geç katılmış olması veya bu alanda yeni kabul edilmesi, onu etkisiz yahut etkisi sınırlı bir aktör yapmaz. Zira devletler, potansiyel olarak ilk nesil internet yöneticilerinin faaliyetleri üzerinde "en büyük" etkiye sahiptir. Bu nedenle internet mimarisinin gelişimini şekillendirebilmekte ve düzenleyici politikalar

üzerinde doğrudan etkiye sahip olabilmektedir. Özellikle internetin ilk zamanlarında adlandırma ve numaralandırma sisteminin ABD hükümetinin denetimine tabi olması, süregelen zaman diliminde de devletlerin bu konudaki etkinliğinin referansı olarak kabul edilmiştir (Bygrave & Michaelsen, 2009, s. 115).

Bugünkü konjonktürde ise küresel internet yönetişimine devletin katılımı, yeni ekonomik ve jeopolitik dinamikler ışığında kaçınılmaz hale gelmiştir. Devletler, açık ve ağa bağlı sistemler ile güvenlik ihtiyaçları arasındaki dengeyi sağlama konusunda kilit bir role sahiptir. Her ne kadar tüm devletler aynı değerleri paylaşmasa da, kamusal değerlerin korunması üzerine istikrar ve tartışma sağlayabilecek tek kurumlar olarak öne çıkmaktadırlar. Bu, yalnızca teknik bir mesele olmanın ötesinde, demokratik süreçlerle ele alınması gereken önemli bir politika sorunu olarak kabul edilmektedir (Baird, 2014, s. 16). Çünkü devletler, çoğu durumda hala eşit katılımın önüne geçecek şekilde davranmaktadır. Örneğin, yasa yapımı, kamu katılımı ve eğitim gibi konularda çok paydaşlı katılıma teşvik ederken; siber güvenlik gibi konularda tek taraflı karar alma yetkisini kendilerine saklayabilmektedir (van der Spuy, 2017, s. 31). Bu durum, pek çok tartışmaya konu olmaktadır. WSIS, yaptığı tanımlamada; devletler, özel sektör ve sivil toplum gibi spesifik paydaş gruplarından bahseder. Burada hükümetlerin kendi devletlerinin çıkarlarını – yani ulusal çıkarları – temsil etmeleri beklenirken, bireysel çıkarlara da sahip oldukları belirtilmiştir. Zira internet yönetişimi, yalnızca devletlerin meselesi değildir. Ancak bazıları WSIS tanımında "devletler"in birincil aktör olarak görüldüğü konusundaki endişelerini dile getirmişlerdir (DeNardis, 2014, s. 38). Bazıları ise, devletlerin teknik ve akademik topluluklardan önce dahil edilmesinden rahatsızlık duymuştur. Aynı zamanda bu aktörlerin farklı paydaş grupları olarak değil, kesişen gruplar olarak kabul edilmesi gerektiğini ifade etmişlerdir (Maciel & de Souza, 2011, s. 5). Başka bir grup ise, paydaşları kategorize etmenin, paydaşların sahip olduğu çeşitli çıkarları incelemeden herhangi bir yarar sağlamayacağına dikkat çekmiştir (Souter, 2017).

Drezner'e göre başlıca aktörler devletler olsa da tek aktör değillerdir. Araştırmalar, devlet dışı aktörlerin özellikle teknik meseleler ve gündem belirleme noktasında yönetişim sürecini daha çok etkileyebildiklerini göstermiştir (2008, s. 118). Bygrave ve Michaelsen de devletlerin diğer aktörlerden daha az etki yarattığını ifade etmişlerdir. Bu bağlamda, devletlerin temel internet mimarisini değiştirmek için hiçbir zaman

gerçek bir girişimde bulunmadığını iddia etmişler ve bu iddialarını şu benzetmeyle ifade etmişlerdir:

> Genel olarak, internet geliştirme aracında devletler (en azından Batı dünyasında), dışarı atılmakla tehdit edildiklerinde el frenini çekmeye hazır olsalar da, genellikle yolcu koltuğuna oturmuşlardır. Kısmi olarak uygunluk nedenleriyle, ama aynı zamanda aracın iyi sürüldüğü ve ağır bir el müdahalesi ile zarar görmemesi gereken çok değerli mallar taşıdığı görüşüne eğildikleri için orada oturmaktan büyük ölçüde memnundular (2009, s. 118).

Bygrave ve Michaelsen'e göre bu durum, Batılı devletler tarafından internetin ekonomik ve sosyal büyüme için öneminin anlaşılmaya başlandığı 1990'ların başında yayınlanan çeşitli politika belgelerinde açıkça görülmektedir. AB içinde yayınlanan Bangemann Raporu bu konuda örnek olarak gösterilebilir (CORDIS, 1994). Martin Bangemann'ın başkanlık ettiği bir görev gücü, özel sektör ve piyasa güçlerinin ana itici güç olduğu Avrupa Bilgi Altyapısı'nın hızlı bir şekilde uygulanmasını sağlamıştır. ABD de bununla paralel olarak yüksek hızlı bilgi aktarımı için bir yol veya ağ olarak geliştirilen Bilgi Süper Otoyolu'nun (*Information Superhighway*) inşasını başlatmıştır. Bu girişim, birçok yargı alanında devleti bilgilendirmeyi amaçlayan bir hattır (2009, s. 118). Bu hattın devleti bilgilendirmesi, Başkan Yardımcısı Al Gore'un zorladığı teknolojilerden biri olduğu iddialarının gündeme gelmesinde etkili olmuştur (Andrews, 1993).

Bygrave ve Michaelsen'ın (2009) gözlemleri, devletlerin internetin temel mimarisine yönelik tutumlarının pasifliğini ve özel sektör ile piyasa güçlerinin bu alandaki hakimiyetini ortaya koymaktadır. 1990'lardan itibaren Batılı devletler, internetin ekonomik ve sosyal büyümenin katalizörü olarak rolünü tanımaya ve bu yeni teknolojinin potansiyelini destekleyen politikalar oluşturmaya başlamışlardır. Ancak bu politikalar genellikle arka planda kalmış ve özel sektörün liderliğindeki gelişmelerin önünü açmıştır. Öne sürülen girişim örnekleri, devletlerin bu süreçte daha çok yönlendirici ve destekleyici roller üstlendiğini, doğrudan müdahalelerden kaçındıklarını göstermektedir. Bu durum, devletlerin internetin gelişiminde önemli bir rol oynamalarına rağmen, bu sürecin şekillenmesinde asıl gücün özel sektör ve piyasa dinamiklerinde olduğu fikrini desteklemektedir.

Bazı aktörler de, devletlerin internet yönetişimine katılımını sınırlandırmaya çalışmaktadır. Bu çabaların arkasında yatan temel motivasyon, mevcut durumu korumak ve statükoyu muhafaza etmektir. Özellikle ABD, bu yaklaşımı kendi nüfuzunu korumak ve muhalif devletlerin etkisini sınırlamak için kullanmaktadır. Bu durum, internetin daha az demokratik ve daha az katılımcı bir şekilde yönetilmesine yol açabilmektedir. Öyle ki, devletlerin internet yönetişimine katılımının sınırlandırılması, bazı devletlerin "internet egemenliği" fikrine yönelmesine neden olabilmektedir. Bu fikir, her devletin kendi internet alanını kontrol etmesi ve yönetmesi gerektiğini savunduğundan, internetin daha bölünmüş ve parçalanmış bir hale gelmesi riskini taşır. Bu durumda farklı devletler farklı kurallara ve düzenlemelere sahip olabilir ve bu durum internetin küresel işlevini ve erişilebilirliğini olumsuz etkileyebilir (Carr, 2015).

Devletlerin internet yönetişimi sürecindeki rolleri ve katılımları hem tarihsel bir perspektiften hem de mevcut dijital dönüşüm bağlamında karmaşık ve çok boyutludur. Devletlerin internetin temel mimarisini şekillendirme sürecine katılımları genellikle pasif bir yaklaşımla karakterize edilmiş olsa da, bu, onların ziyadesiyle katılım sağladığı –hatta çoğu durumda diğer aktörlere alan açmadığı– gerçeğini değiştirmez. Bu nedenle devletlerin iyi yönetişim unsurlarının sağlanması için hem ulusal çıkarları temsil etme hem de küresel internet yönetişiminde eşit katılımı sağlama konusunda dengeli bir yaklaşım benimsemesi gerektiği söylenebilir.

1.2.7.2.Hükümetlerarası Kuruluşlar

İnternet yönetişimi, internetin nasıl geliştirildiği, yönetildiği ve kullanıldığına dair kurallar ve politikaları kapsar ve bu süreçte birçok hükümetlerarası kuruluş önemli roller üstlenir. İnternet yönetişimi, çok katmanlı ve dinamik bir yapıya sahip olduğundan, bu yapı içinde BM sistemi çerçevesinde faaliyet gösteren çeşitli kuruluşlar önemli roller oynar. UNESCO, ITU ve BM Kalkınma için Bilim ve Teknoloji Komisyonu (CSTD) gibi kuruluşlar, BİT'in kalkınma, eğitim, bilim, kültür ve iletişim alanlarında kullanılmasını teşvik ederek özel amaçlı süreçlere öncülük ederler. Bu kuruluşlar, internetin yönetişimine ilişkin politikaların ve standartların geliştirilmesinde kritik bir role sahiptir ve teknolojinin toplumsal fayda sağlamasını destekleyen çerçeveler oluştururlar (Levinson & Marzouki, 2016, s. 7).

ITU, BM'ye bağlı olarak çalışır ve telekomünikasyon teknolojileri için uluslararası standartlar belirleyerek internet protokollerinin ve standartlarının geliştirilmesine

katkıda bulunmaktadır. Dünya Fikri Mülkiyet Örgütü (WIPO), internet üzerinden yapılan yayınların, yazılımların ve diğer dijital içeriklerin fikri mülkiyet haklarının korunması konusunda çalışmalar yapar. Dünya Ticaret Örgütü (WTO), elektronik ticaret de dahil olmak üzere, internet üzerinden yapılan ticaretin kurallarını belirlemede önemli bir rol oynar. Uluslararası Standartlar Örgütü (ISO) internet teknolojileri ve güvenliği alanında standartlar belirleme konusunda faaliyet gösterir. IGF, internet yönetişimi konusunda küresel bir diyalog platformu sağlar ve devletler, özel sektör, teknik topluluk ve sivil toplum kuruluşlarını bir araya getirir. Bu kuruluşların her biri, internetin küresel olarak nasıl işlediğini, geliştirileceğini ve düzenleneceğini etkileyen politikalar ve standartlar üzerinde önemli bir etkiye sahiptir ve kendi uzmanlık alanları doğrultusunda internetin yönetişimine katkıda bulunurlar (Ministry for Europe and Foreign Affairs, 2020).

Hükümetlerarası kuruluşlar, küresel internet yönetişimi ekosisteminde karmaşık ve ince etkileşimlerle bu alanın teknik, mimari ve politik yapısındaki değişimlere katkıda bulunmaktadır. WSIS'ten NETmundial'e kadar uzanan süreçte, uluslararası organizasyonların yapısında ve işlevlerinde önemli dönüşümler yaşandığı gözlemlenmiştir. Bu dönüşüm, yeni kuruluş kategorilerinin ortaya çıkışı ve paydaş olarak tanınmalarıyla daha da belirginleşmiştir. İnternet yönetişiminde "ara organizasyonel altyapı" olarak işlev gören bu yapılar, çeşitli paydaşlar arasında bilgi akışlarını ve güç dinamiklerini yönlendirerek, yönetişim sisteminin şekillenmesinde proaktif roller üstlenmektedir. Bu etkileşimler, teknik altyapının geliştirilmesine katkı sağlamakla kalmayıp, aynı zamanda bu altyapı tarafından da şekillendirilmektedir (Levinson & Marzouki, 2016).

İnternet yönetişimi üzerine yapılan çalışmalar, genellikle ulus-devletler ve internet kuruluşları arasındaki dinamiklere odaklanmış olup, hükümetlerarası kuruluşların bu alandaki rolleri ve kuruluşlar arası ilişkiler görece daha az incelenmiştir. Bu durum, internet oluşumlarının yenilikçi doğasının ve devletin internet yönetişimindeki yerinin yeniden değerlendirilmesi gerekliliğinin bir sonucu olarak görülebilir. Goldsmith ve Wu (2006), Drezner (2007) ve Mueller (2010) gibi yazarların çalışmaları, internet yönetişiminde devletler ve özel sektör aktörlerinin rollerine dikkat çekerken, hükümetlerarası kuruluşların bu alandaki etkinlikleri ve kuruluşlar arası etkileşimler daha az ele alınmıştır. Oysa ki hükümetlerarası kuruluşların çalışmaları, internet yönetişiminin gelecekteki yönünü şekillendirme konusunda kritik bir rol oynamaktadır.

Ulus-devletler ve özel sektör arasındaki dinamiklerin yanı sıra, hükümetlerarası kuruluşların ve çeşitli kuruluşlar arası etkileşimlerin ayrıca incelenmesi gerekmektedir.

Bu çalışmanın 1.2.5. alt başlığında hükümetlerarası kuruluşların düzenlediği konferanslar ve oluşturduğu platformlara detaylıca değinildiğinden bu kısımda geniş bir şekilde yer verilmemiştir. Diğer yandan, çalışmanın ilerleyen bölümlerinde hükümetlerarası kuruluşların etkilerine ve internet yönetişimi üzerindeki rollerine daha detaylı bir şekilde yer verilecek olup, bu kuruluşların internetin evrimi, hukuki süreçlere katkısı ve yönetişimdeki kritik önemi vurgulanacaktır.

1.2.7.3. Uluslararası Standardizasyon Kuruluşları

İnternetin kendine has tasarımı ve yapısı, geleneksel yönetim hatta yönetişim biçimlerinin ötesine geçen ve devletlerin ve hükümetlerarası kuruluşların yanı sıra çeşitli paydaşların katılımını teşvik eden yönetişim biçimlerini gerektirir. İnternet; açıklığı, dağıtılmış yapısı, birbirine bağlılığı, katılımcı doğası ve aşağıdan yukarıya süreçleri ile tanımlanır ve bu özellikler, çok paydaşlı katılımın temel prensipleriyle örtüşür (van der Spuy, 2017, s. 19). İnternetin yönetişiminde de bu süreçlerle uyumlu olarak hareket ettiğini öne süren bir dizi kuruluş görev almaktadır.

İnternet yönetişiminde görev alan bu kuruluşlar genellikle temel mimari, altyapı, DNS, kök sunucuları ve IP adreslerini içeren Kritik İnternet Kaynaklarının (CIR) yönetişimi ile ilgilenmektedir. Bu konuda öne çıkan kuruluşlar; ISOC, IAB, IETF, W3C, IANA ve ICANN şeklinde sıralanabilir. Aşağıda detaylı olarak inceleyeceğimiz bu organ ve kuruluşlar, internetin özellikle teknik anlamda "yöneticileri" arasında yer almaktadır. Bu kurumlar, oynadıkları rol veya önem sıralamasına göre değil; kronolojik sıralama göz önünde bulundurularak ele alınmıştır.

i. İnternet Mimarisi Kurulu

İnternet Mimarisi Kurulu (IAB), başlangıçta İnternet Faaliyetleri Kurulu olarak adlandırılmıştır. 1983'te Dave Clark başkanlığında, internetin hala büyük ölçüde ABD hükümetinin bir araştırma faaliyeti olduğu günlerde kurulmuştur (IAB, t.y.a). IAB'nin kökeni, 1979'da DARPA'da program yöneticisi olan Vinton Gray Cerf tarafından kurulan İnternet Yapılandırma Kontrol Panosu'na (ICCB) dayanmaktadır. 1984'te ICCB dağıtılmış ve yerini IAB almıştır. Bu değişiklik, DARPA'da internet araştırma programının yönetimini devralan Dave Clark ve Barry Leiner tarafından başlatılmıştır. IAB, yeni oluşturulan araştırma görev güçlerinin başkanlarından ve RFC editörü olarak

görev yapan Jon Postel'den oluşmaktaydı. Görev güçlerinin ilk başkanları ICCB üyeleriydi. IAB'ye de Dave Clark başkanlık etmiştir (IAB, t.y.b).

Bugün IAB, herhangi bir şirketin, ajansın veya başka bir kuruluşun temsilcisi olarak değil, birey olarak hizmet veren 13 üyeden oluşur (IAB, t.y.c). IAB, hem IETF'nin bir komitesi hem de ISOC'un bir danışma organı olarak yetkilendirilmiştir. Sorumlulukları arasında IETF faaliyetlerinin mimari gözetimi, İnternet Standartları Süreci gözetimi ve temyizi ve RFC editörünün atanması yer alır. IAB ayrıca IETF protokolü parametre kayıtlarının yönetiminden de sorumludur (IAB, t.y.d).

IAB, internet tarafından kullanılan protokoller ve prosedürler için mimari denetim sağlar. Bunun yanında, internet ve interneti sağlayan teknolojilerle ilgili teknik, mimari, prosedürel ve (uygun olduğunda) politika konularında Mütevelli Heyeti ve İnternet Topluluğu Yetkilileri için bir tavsiye ve rehberlik kaynağı olarak hareket eder. IAB belgeleri genellikle internetin ve protokollerinin düzgün çalışması için gerekli olduğuna inanılan genel teknik ilkeleri açıklamayı amaçlamaktadır. IAB'nin tetikleyebileceği başka bir eylem türü, belirli bir alanda fikirler geliştirmek için standartlar sürecinin dışında bir atölye çalışması veya geçici panel oluşturmaktır (IAB, t.y.a).

ii. İnternet Topluluğu

"İnternet herkes içindir" vizyonuyla hareket eden İnternet Topluluğu (ISOC), 1992 yılında "internetin babaları" olarak kabul edilen Vinton Gray Cerf ve Bob Kahn tarafından kuruldu. Misyonu, dünyanın her yerinden insanların yararına internetin açık gelişimini, evrimini ve kullanımını teşvik etmektir (ISOC, t.y.b). Bununla birlikte, internetin çalışmasını sağlayan toplulukları oluşturmak ve desteklemek; internet altyapısının, teknolojilerinin ve açık standartların geliştirilmesini ve uygulanmasını ilerletmektir (ISOC, t.y.c.).

Kuruluşun diğer bir önemli amacı, internet standartları geliştirmede ana kuruluş olan IETF'nin çalışmalarını finanse etmekti. Topluluk ayrıca IETF'ye standartlardan kaynaklı maruz kalınabilecek olası hasarların sorumluluğunu karşılamak için sigorta sağlamaktaydı. Ancak 2018 yılında IETF, kendi tüzel kişiliğini (IETF Administration LLC) oluşturarak ISOC'tan ayrıldı. ISOC ise, bir bağış ve rezerv fonu oluşturmasına yardımcı olmak için 2020 yılına kadar IETF'ye ödeme yapmayı taahhüt etmiş, bu tarihten itibaren mali açıdan bağımsız olmuştur. IETF ve ISOC, 2020 yılında yeni bir finansal kapsamı olan 6 yıllık bir anlaşmaya imza atmışlardır. Yeni anlaşma uyarınca

ISOC, IETF'nin yıllık işletme giderlerinin bir kısmı için 6 yıl boyunca ortalama 7 milyon ABD doları tutarında sürekli mali destek sağlayacak. 1 Ocak 2021'de yürürlüğe giren anlaşma, 31 Aralık 2026'ya kadar devam edecek (ISOC, 2020). Ayrıca ISOC, RFC'leri finanse etmektedir. 2019 yılında RFC'lerin 50. Yılını kutlayan ISOC, halen tüm RFC'lerin telif hakkını elinde tutmaktadır (York, 2019).

Covid-19 salgını nedeniyle ISOC, 2021 yılı için "İnsanları Daha Büyük ve Daha Güçlü Bir İnternet Yaratmak İçin Güçlendirmek" adıyla bir Eylem Planı hazırlığına girişmiştir. Gerekçe olarak da şu ifadeleri kullanmıştır:

> Hiç kimse 2020 olaylarını tahmin edemezdi. Her şeye rağmen internet, birçok insanın hayatında değişmeyen tek şey oldu. Çevremizdeki dünyayla sarsılmaz bağlantımız oldu. Temelleri nedeniyle, internet güvenilir ve dayanıklı kalmıştır - dünya çapında pek çok insan için bir yaşam çizgisi. 2020, her yıl olduğundan daha fazla bize misyonumuzun önemini hatırlattı (ISOC, 2021).

ISOC, internetle ilgili kararlara ulaşmak için devletler, ulusal ve uluslararası kuruluşlar, sivil toplum, özel sektör ve diğer taraflarla birlikte çalışarak işbirliği kapsamında faaliyet göstermektedir. Ağ tarafsızlığını, açık erişimi, internetin esnekliğini ve istikrarını, ifade özgürlüğünü, kullanıcıların mahremiyetini ve kimliğini desteklemektedir. İnterneti güvence altına almak için çok boyutlu yaklaşımlarla, internetin işleyişini etkileyen çeşitli politika kararların alınmasında etkili olmuştur. Kullanıcıların mahremiyetini ve kimliğini korumaya yönelik önemli girişimleri, sosyal medya ve diğer bilgi teknolojisi kullanıcıları için geniş kapsamlı etkilere sahiptir (Pushyamitra, 2022, s. 629).

Kuruluş amacı, internet standartlarının geliştirilmesi için örgütsel bir şemsiye sağlamaktı. Bunun yanında, standartların geliştirilmesine dahil olan bireylerin davalardan korunması da topluluğun birincil amaçları arasında yer almaktaydı. ISOC'un kurulmasından önce oluşturulan standartlar için herhangi bir özel kuruluşun yasal sorumluluğu olmadığından, bireylerin standartlardan kaynaklı zararlardan kişisel olarak sorumlu olmaları endişesi söz konusuydu. Öte yandan, DARPA ve ABD'nin diğer devlet organlarının internet standartlarının geliştirilmesi için mali desteklerini azaltmaya başlamaları, finansman sorununu da beraberinde getirmiştir (Bygrave ve Michaelsen, 2009, s. 95).

Diğer bir tartışma alanı, internet üzerinde faaliyet gösteren bazı standardizasyon kurumlarının sıklıkla ISOC ve benzeri yapılar aracılığıyla bir araya gelmesiydi. Bu gruplar, internet yönetişiminin politik sorunlarının göz ardı edilmesi için lobi faaliyetleri yürütmekteydi (Mueller, 2010, s. 117). Bu gruplar, kâr amacı gütmeyen kuruluşlar ile özel sektör arasında, aynı zamanda akademi ve devlet destekli araştırma programları ile iletişim halindeydi. Bu aktörler arasında, üniversitelerde veya kâr amacı gütmeyen kuruluşlarda yer alan ancak aynı zamanda teknoloji şirketleriyle düzenli olarak istişarede bulunan yönetim kurulu üyeleri; Cisco, Google, IBM gibi büyük ticari şirketlere sıkı sıkıya bağlı bireyler ve devlet veya askeri araştırma fonlarından yararlanan kişiler bulunmaktaydı. Bu aktörler ve kurumlar, genellikle Batı'ya ve özellikle ABD'ye odaklanmışlardır. Geleneksel devlet temelli kurumlardan bağımsız olarak gelişmişler ve ilk yıllarında geleneksel devlet güç yapılarından uzak durma eğiliminde olmuşlardır. Bu yapıyı tanımlamak için Mueller, "organik olarak gelişmiş internet kurumları" terimini kullanır (2010, s. 217).

ISOC'un kritik internet kaynaklarının yönetişimi gibi teknik standartlara çok fazla odaklanarak politik konuların tartışılması konusunda yetersiz kaldığına dair eleştiriler de yapılmıştır (Mueller, 2010, s. 117). Zira internet erişimi ve kullanımı konusunda dünya çapında eşitsizliklerle mücadele etmek için yeterince kaynak ayrılmamakta ve bu alandaki projeleri yeterince desteklememektedir (Dutton & Blank & Groselj, 2013, s. 47). Ayrıca, ISOC'un .org alan adının yönetimini Ethos Capital'e satma kararı, topluluk içinde ve dışında büyük bir tartışma yaratmış ve birçok kişi ve organizasyon tarafından internetin ticarileşmesi ve kâr amacı güden şirketlerin eline geçmesi konusundaki endişeleri artırmıştır (Wroblewski, 2020).

Görüldüğü üzere ISOC, IETF gibi kritik kuruluşlara mali destek sağlayarak ve RFC'leri finanse ederek internet standartlarının geliştirilmesine büyük katkılar sunmuştur. Ancak, ISOC'un politik konulara yeterince odaklanmamış olması, eleştirilere neden olmuştur. Bu eleştirilere rağmen, ISOC'un internetin açık, güvenli ve herkes için erişilebilir kalması yönündeki çabaları, dijital çağda bilgi ve iletişim teknolojilerinin demokratikleşmesine katkıda bulunmaktadır. Dolayısıyla ISOC'un gelecekteki faaliyetlerinin hem teknik standartlar hem de genişleyen internet erişimi ve kullanımıyla ilgili politik ve sosyal konuları daha kapsamlı ele alacak şekilde dengelenmesi gerektiğinin altı çizilmelidir.

iii. World Wide Web Konsorsiyumu

World Wide Web Konsorsiyumu (W3C), Ekim 1994'te WWW'nin mucidi Tim Berners-Lee tarafından kuruldu. Berners-Lee, Avrupa Nükleer Araştırma Örgütü CERN'in işbirliğiyle; DARPA ve Avrupa Komisyonu'nun desteğiyle Massachusetts Teknoloji Enstitüsü Bilgisayar Bilimleri Laboratuvarında (MIT/LCS) W3C'yi oluşturmuştur (W3C, t.y.a.). W3C bugün Direktörü Tim Berners-Lee ve CEO'su Jeffrey Jaffe tarafından yönetilmektedir. W3C'nin misyonu, Web'in uzun vadeli büyümesini sağlayan protokoller ve yönergeler geliştirerek WWW'i tam potansiyeline ulaştırmaktır (W3C, t.y.b.).

Web standartları, üyeliği her türlü kuruluş ve kişiye açık olan W3C tarafından belirlenir. Standartlar, ayrıntılı bir fikir birliğine dayalı süreç yoluyla geliştirilir ve "W3C Önerileri" olarak yayınlanır (UNCTAD, 2015, s. 11). W3C'nin tek bir fiziksel merkezi yoktur. Tesisler ve altyapı için 4 ev sahibi kuruma dayanmaktadır. Bunlar; ABD'deki Massachusetts Teknoloji Enstitüsü Bilgisayar Bilimi ve Yapay Zekâ Laboratuvarı (MIT/CSAIL), Japonya'daki Keio Üniversitesi, Fransa'daki Avrupa Bilişim ve Matematik Araştırma Konsorsiyumu (ERCIM) ve Çin'deki Beihang Üniversitesi'dir (W3C, t.y.c.).

Konsorsiyum'un dünya çapında 17 bölgede ofisi mevcuttur (Brown, 2019). Bunlar genellikle daha büyük araştırma kurumlarında bulunur. 2021 itibariyle Konsorsiyum'a üye 437 kuruluş bulunmaktadır (W3C, t.y.d.). Üyelik, herhangi bir kuruluşa ücret karşılığında açıktır. Ancak ücretler bir kuruluşun yıllık gelirlerine, türüne ve genel merkezinin konumuna bağlı olarak değişir. Örneğin, 2021 itibariyle, Hindistan'daki küçük bir şirket yılda 1,905 ABD doları, ABD'deki kâr amacı gütmeyen bir şirket 7,900 ABD doları ve Fransa'daki büyük bir şirket 59,500 Avro ödeyecektir (W3C, t.y.e.). W3C standartlarının ekonomik öneminin yüksek olması, internet endüstrisinin ve yazılım geliştiricilerinin W3C standartlarının geliştirilmesine aktif katılımını sağlamıştır (UNCTAD, 2015, s. 12).

W3C'nin ana hedefleri arasında web teknolojilerinin uyumluluğunu ve erişilebilirliğini artırmak, kullanıcı deneyimini iyileştirmek ve Web'in tüm kullanıcılar için adil bir şekilde çalışmasını sağlamak yer alır. Ancak, W3C'nin karar alma süreçleri ve bazı standartların kabulü zaman zaman topluluk içinde tartışmalara yol açmıştır. Özellikle, Dijital Haklar Yönetimi (DRM) teknolojilerinin web standartlarına entegrasyonu

konusundaki kararlar, özgür yazılım hareketi ve bazı internet aktivistleri tarafından eleştirilmiştir. Tim Berners-Lee'nin HTML'in gelecek sürümlerine DRM entegrasyonunu desteklemesi, web içeriğinin "flash" gibi erişilemez ve bağlantı kurulamaz formatlarda kilitlenmesini önleme iddiasıyla dikkatleri üzerine çekmiştir. Bu durum, HTML üzerindeki tartışmaları canlandırarak, genel amaçlı bilgisayarların tasarımı konusundaki uzun süreli çatışmayı tekrar gündeme getirmiştir. Eğlence endüstrisinin, dosyalara erişim için parça başı ücret talep ederek karlarını artırma stratejisi, bilgisayarların kullanıcıların kontrolü dışında hareket etmesi gerektiği yönündeki uzun süreli beklentilerle uyumludur. Bu kapsamda, DVD üreticilerinin bölgesel kısıtlamalar uygulaması, bu kısıtlamaların etkinliği ve üreticilerin bu yöntemi neden benimsedikleri konuları önem kazanmaktadır (Doctorow, 2013). Bu tartışmalar, W3C'nin misyonunun ve karar alma mekanizmalarının şeffaflığı ve katılımcılığı açısından önemli soruları gündeme getirmektedir.

Zaman zaman bu tür tartışmalar gündeme gelse de W3C, fikir birliği ile gönüllü standartlar geliştiren, açık ve çok paydaşlı bir sürece sahip, kamu yararına çalışan üye odaklı bir organizasyon olarak kabul edilir. İfade özgürlüğü, gizlilik, güvenlik ve erişilebilirlik gibi insan hakları, Web tasarımının dünya çapındaki kullanıcılar için önemli yararlar sağladığı temel alanlardır. Bu nedenle, W3C gibi kuruluşların teknik standartların tasarımında bu hakları dikkate alması ve desteklemesi, geniş kapsamlı teknik standart geliştirme sürecinin kritik bir yönünü oluşturmaktadır. Bu bağlamda W3C, "Herkes için Web" ilkesini rehber alarak, Web'in sosyal değerini ve insan haklarını desteklemeyi önceliklendirir. Bu yaklaşım, teknik standartlar ve yeni iletişim teknolojilerinin insan hakları üzerindeki etkilerini geniş bir perspektifle değerlendirmeyi içerir. Bunun yanında W3C, geniş kapsamlı bir inceleme süreci ile yeni teknolojilerin insan hakları üzerindeki etkilerini düzenli olarak değerlendirir ve bu teknolojilerin tasarımında insan haklarını destekleyici yönergeler ve ilkeler geliştirmeye devam etmektedir (Doty & Cooper & Seltzer, 2023).

iv. İnternet Mühendisliği Görev Gücü

IETF, internet mimarisinin gelişimi ve internetin sorunsuz çalışmasıyla ilgilenen ağ tasarımcıları, operatörleri ve araştırmacılarından oluşan büyük bir uluslararası topluluktur. Bunun yanında, açık süreçler aracılığıyla açık standartlar geliştiren önde gelen internet standartları kuruluşudur. İnternetin işleyişini, yönetimini ve gelişimini koordine etmek için 1986 yılında kurulmuştur. IAB tarafından denetlenmekte ve

ISOC'tan idari destek almaktadır (IETF, t.y.a). İnternetin mimarisi bir dizi teknik standarda dayanmaktadır. IETF, internet standardını şu şekilde tanımlamıştır (Bradner, 1996): "İstikrarlı ve iyi anlaşılmış, teknik olarak yetkin, önemli operasyonel deneyime; çoklu, bağımsız ve birlikte çalışabilir uygulamalara, önemli kamu desteğine sahip ve internetin bazı veya tüm bölümlerinde fark edilir derecede yararlı olan bir spesifikasyon".

IETF, internet standartları geliştirmede ana iş gücüdür. Birçok internet teknik standardı, IETF tarafından RFC biçiminde belirlenir. Bunlar, TCP/IP'nin tanımlanmasında kullanılan standart numaralara sahip belgelerdir ve tüm ilgili taraflara açık olan çalışma gruplarında gönüllü olarak geliştirilirler. IETF, kararlarını genellikle "kaba fikir birliği ve çalışan kod" (*rough consensus and running code*) olarak tanımlanan açık ve fikir birliğine dayalı bir süreç aracılığıyla alır. Standardizasyon çalışmaları, IAB tarafından denetlenen İnternet Araştırma Görev Gücü'nde (IRTF) de gerçekleştirilmektedir (Resnick, 2014). Bunun yanında IAB, IETF ve IRTF için harici irtibat ilişkilerini yönetir ve bazı gözetim işlevlerini yerine getirir. IAB ve IETF, kurumsal olarak ISOC'a bağlıdır (UNCTAD, 2015, s. 10).

Temel misyonunu kısaca "internetin daha iyi çalışmasını sağlamak" şeklinde ifade etmektedir. Bu misyonun bir parçası olarak, RFC'de yayınlanan bir dizi protokol standartları ve uygulamaları gibi internetteki acil operasyonel ve teknik sorunları tanımlar ve bunların standart özelliklerine uygun çözümler önerir. IETF Bölge Direktörlerinden oluşan İnternet Mühendisliği Yönlendirme Grubu (IESG), IETF faaliyetlerinin teknik yönetiminden ve internet standartları sürecinden sorumludur. IETF'nin çalışması 100'den fazla çalışma grubunda yer alır ve tüm kararlar "kabaca fikir birliği ve çalışma kodu" temelinde alınır (IETF, t.y.b).

IETF'nin ilgilendiği sorunlardan biri, IP adreslerinin sayısı ve kullanılabilirliğidir. IPv4 yaklaşık 4,29 milyar IP adresini desteklemektedir. Ancak internete bağlanan cihaz ve kullanıcı sayısının artması nedeniyle bu sayı yeterli olmamıştır. Bu nedenle IETF, çok daha büyük bir adres havuzu sağlayan ve böylece çok daha fazla sayıda cihazın kendi

IP adreslerine sahip olmasına izin veren yeni bir IP sürümü olan IPv6'yı geliştirmiştir. IPv6 ise, IPv4'ten 1.028 kat daha fazla IP adresini desteklemektedir.[13]

IETF'nin çalışma prensibi, belirli konulara ayrılmış gruplar tarafından çalışmaların yürütülmesi şeklindedir. Güncel olarak 100'den fazla çalışma grubu mevcuttur.[14] Her grup; genel alan, internet alanı, operasyonlar ve yönetim alanı, yönlendirme alanı, güvenlik alanı ve ulaşım alanı olmak üzere 7 konu alanından oluşan bölümlere ayrılmıştır. Her alan için, çalışma grubunun çalışmalarını yönetecek ve koordine edecek bir bölge direktörü mevcuttur (IETF, t.y.b).

IESG, IETF'in teknik operasyonlarını yönetir ve denetler. Esasen IETF'nin yürütme organı olarak görülebilir. Tüzüğü hiçbir zaman resmi olarak oluşturulmamış olsa da, mevcut sorumlulukları RFC 3710'da belgelenmiştir (Alverstrand, 2004). IESG, IETF'nin doğrudan işletilmesinden ve IETF tarafından üretilen işin kalitesinin sağlanmasından sorumlu gruptur. IESG, çalışma grubu belgelerinin ve IETF standartları izleme adaylarının teknik incelemesini ve onayını gerçekleştirir. Bunun dışında, IETF'nin toplantı etkinlikleri de dahil olmak üzere lojistiğini yönetir.

IRTF, IETF'ye bağlı olmasına rağmen resmi olarak ondan ayrılır. IETF daha kısa vadeli standart sorunlarla ilgilenirken; IRTF, uzun vadeli araştırma konularına odaklanır (Bygrave & Michaelsen, 2009, s. 100). IRTF, küçük birkaç Araştırma Grubundan (RG) oluşur. Aktif olarak 14 grup mevcuttur. Örneğin; İnsan Hakları Protokolü Hususları Araştırma Grubu (HRPC), Herkes için İnternete Küresel Erişim Araştırma Grubu (GAIA) ve Ağ Yönetimi Araştırma Grubu (NMRG) bunlardan bazılarıdır. IRTF, İnternet Araştırma Yönlendirme Grubu (IRSG) tarafından yönetilmektedir (IRTF, t.y.).

IETF, internet yönetişimine yalnızca teknik anlamda katkı sağlayan paydaşlardan ziyade, tüm paydaşların katılımını teşvik etmeye çalışmaktadır. Zira internet yönetişimine tüm paydaşların katılımının sağlanamaması, standartların geliştirilmesinde insan hakları, rekabet politikası ve güvenlik gibi teknik olmayan sonuçlar doğurabilmektedir. IETF bu zorluğun farkına varmış ve teknik olmayan paydaş temsilcilerinin katılımını artırmaya yönelik adımlar atmıştır (UNCTAD, 2015, s. 11).

[13] Desteklenen tam rakam; 340,282,366,920,938,463,463,374,607,431,768,211,456 şeklindedir. Detaylı bilgi için bkz: RIPE NCC. (t.y.). Understanding IP Addressing and CIDR Charts. https://ipv6.metu.edu.tr/tr/node/1 (21.04.2023).

[14] Aktif grupların tam listesi için bkz: IETF (t.y.). Active IETF working groups. https://datatracker.ietf.org/wg/ (21.04.2023).

IETF örneği, yüksek düzeyde söylemin ve geçerli kural oluşturmanın mümkün olduğunu göstermektedir (Froomkin, 2003, s. 869). IETF, açık ve kapsayıcı bir süreç kullanarak, farklı çıkarları temsil eden farklı kişilerden gelen fikirleri birleştirmeyi başarmıştır. Bu, IETF'nin, internetin başarısının anahtarlarından biri olan sağlam ve işlevsel standartlar geliştirmesine olanak tanımıştır. IETF'nin başarısının birkaç nedeni vardır. Birincisi, IETF, herkesin katılımına açık bir süreç olduğundan, herkes fikirlerini ifade etme ve standart geliştirme sürecine katkıda bulunma fırsatı bulur. İkincisi, IETF, tüm görüşlerin eşit olarak ele alındığı bir süreç olduğundan, farklı çıkarları temsil eden kişilerden gelen fikirleri birleştirmesine olanak tanır. Üçüncüsü, IETF, açık ve şeffaf olduğundan, IETF'nin çalışmaları izlenebilir ve hesap verilebilirdir.

IETF'nin açık katılımcı modeli, herkese internet standartları üzerinde çalışma ve etki etme fırsatı sunar, bu da onu demokratik bir yapı olarak öne çıkarır (Harris, 2001). Ancak, bu modelin bazı zorlukları da beraberinde getirdiği görülmüştür. Özellikle, teknik tartışmaların uzmanlık gerektirmesi nedeniyle katılımın teknik bilgiye sahip bireylerle sınırlı kalması[15] eşitlik ve çeşitliliği engelleyebilmektedir. Bu durumda IETF'nin açık katılımcı modeli, teoride herkese eşit bir şans verirken, pratikte uzmanlık ve teknik bilgi gereksinimleri nedeniyle katılımı sınırlayan bir yapıya sahiptir. Bu durum, diğer katılımcıların sürece dahil olmalarını zorlaştırabilir ve sonuç olarak, internet standartlarının geliştirilmesi sürecinde belirli bir demografik veya coğrafi bölgeden gelen seslerin hâkim olmasına yol açabilir. Bu, IETF'nin çeşitliliği ve kapsayıcılığı artırma çabalarını engelleyen önemli bir zorluktur. IETF'nin demokratik yapısını daha da güçlendirmek ve geniş bir katılımcı tabanını teşvik etmek için, teknik uzmanlığı olmayan katılımcıları dahil etmek, eğitim programları düzenlemek ve katılım için mali destek sağlamak gibi çözümler üzerinde çalışması gerekmektedir. Bu tür girişimler, IETF'nin gerçekten küresel, çeşitli ve kapsayıcı bir platform olma vizyonuna ulaşmasında kritik bir rol oynayacaktır.

v. İnternet Atanmış Numaralar Kurumu

İnternet Atanmış Numaralar Kurumu'nun (IANA) öncelikli işlevi; benzersiz kodları, numaralandırma sistemlerini ve internet iletişimi için gerekli olan diğer parametreleri yönetmektir. DNS Kök Bölgesinin (ccTLD'lerin ve gTLD'lerin atamaları) *.int* ve .arpa

[15] IETF Atama Prosedürleri için bkz: Daigle, L. (2003). IETF ISOC Board of Trustee Appointment Procedures, Network Working Group: Request for Comments: 3677. https://datatracker.ietf.org/doc/rfc3677/

bölgeleri gibi diğer işlevlerle birlikte yönetimini sağlamaktadır (IANA, t.y.a). Birçok internet protokolünde kullanılan protokol adı ve numarası kayıtları için "merkezi" kurumdur (IANA, t.y.b). Bunun yanında, Bölgesel İnternet Kayıtlarına yapılan tahsisler gibi küresel IP ve AS numara alanlarının koordinasyonunu üstlenmiştir (IANA, t.y.c).

IPv4 ve IPv6 adresleri genellikle hiyerarşik bir şekilde atanmaktadır. Kullanıcılara internet servis sağlayıcıları (ISS'ler) tarafından IP adresleri atanır. ISP'ler, IP adreslerinin tahsisini yerel bir internet sicilinden (LIR) veya Ulusal İnternet Kayıt Defterinden (NIR) veya uygun Bölgesel İnternet Kayıt Defterinden (RIR) alır.

IANA'nın IP adresleri için birincil rolü, küresel politikanın ihtiyaçlarına göre RIR'lara ayrılmamış adres adlarını tahsis etmek ve IETF tarafından yapılan protokol atamalarını belgelemektir (IANA, t.y.c). IANA'nın çalışmaları, başlangıçta DARPA tarafından finanse edilen bir araştırma projesi olarak University of Information Sciences Institute (ISI) himayesi altında Jon Postel tarafından yürütülmüştür (Bygrave & Michaelsen, 2009, s. 102). Postel, 1988'de DARPA ile ISI arasında imzalanan yeni bir araştırma sözleşmesinde protokol standartlarının yönetimini IANA'nın bir işlevi olarak adlandırmaya başladı. DARPA ile ISI arasındaki sözleşme 1999'da sona erdiğinde, ABD hükümeti IANA'nın işlevlerini ICANN'e devretti (Snyder, 2016). Bu işlevler ICANN tarafından ABD Ticaret Bakanlığı ile yenilenebilir bir sözleşme kapsamında yürütülmüştür.

vi. İnternet Tahsisli Sayılar ve İsimler Kurumu

Bugünkü küresel internet yönetişimi literatürünün büyük bir bölümünü İnternet Tahsisli Sayılar ve İsimler Kurumu'nun (ICANN) rolü ve ABD'nin bu kuruluş üzerindeki hakimiyeti oluşturmaktadır. Tartışmaların büyük bölümünün ana odağı bu konu üzerine şekillenmektedir. Bu tartışmaların mahiyetini anlayabilmek için ICANN'in kuruluş sürecine bakmak gerekir.

İnternet alan adlarının ve adreslerinin küresel koordinasyonu ile ilgili sorunlar özellikle 1990'larda süregelen bir dizi tartışmayla hareketlilik kazandı. ICANN, bu tartışmaların doğal bir sonucu olarak ortaya çıkan bir kurum oldu. ICANN'in kurulması, internet yönetişimi açısından ciddi bir dönüm noktası olarak kabul edilebilir. Zira internet yönetişimi teriminin ICANN'in kurulmasıyla birlikte genişlediği öne sürülmektedir (Mueller, 2010, s. 10).

ABD Ticaret Bakanlığı'nın yeni bir tüzel kişilik (NewCo) çağrısına yanıt olarak oluşturulan ICANN'in en önemli işlevi, internette atanmış parametreleri yönetmektir (NTIA, 1998a). ABD Ticaret Bakanlığı'nın bu çağrısı, ABD hükümetinin o sırada yürürlükte olan yönetim rejiminden rahatsız olduğunu göstermiştir. Bunun nedeni; rejimin geçici, görece gayrı resmi ve ABD merkezli olmasıydı (Bygrave & Michaelsen, 2009, s. 104). Hükümet ayrıca, alan adlarının tescili konusunda herhangi bir rekabet olmamasından da rahatsızdı. Zira kayıt hizmetleri konusunda egemen olan tek aktör Network Solutions, Inc. (NSI) idi. NSI'ye, Ulusal Bilim Vakfı (NSF) ile yapılan bir sözleşme kapsamında üst düzey alan adları olan .com, .net ve .org için tekel kayıt yetkileri verilmiştir. Bu sorunların yanında hükümet, ticari marka sahipleri ile alan adı sahipleri arasındaki anlaşmazlıkları çözme mekanizmalarının ağır maddi yükümlülükler getirdiğinin de altını çizmiştir. Bu doğrultuda hükümetin bu sorunlara önerdiği ilk çözüm, NewCo öncülüğünde yeni bir yönetim sistemi oluşturmaktı (NTIA, 1999). Bunun üzerine Jon Postel'in merkezi katılımıyla ICANN kuruldu.

Kaliforniya merkezli ICANN, Eylül 1998'de ABD hükümetinin DNS'nin politikasını ve teknik yönetimini küresel katılımlı ABD merkezli kâr amacı gütmeyen bir şirkete devretme taahhüdünden doğdu. İlk başta IANA'nın görevlerini yürüten ICANN, IANA Yönetim Devri'nin Ekim 2016'da tamamlanmasıyla bütün yetkiyi devralmıştır (ICANN, t.y.a). Bu devir işlemi, internetin yönetişiminde önemli bir değişikliği temsil eder. Zira internetin temel kaynaklarının yönetimi, ABD hükümetine bağlı Ulusal Telekomünikasyon ve Bilgi İdaresi'nden (NTIA) daha küresel ve çok paydaşlı bir yapı olan ICANN'e resmi olarak geçmiştir.

ICANN; dünyanın her yerinden katılımcıları olan, kâr amacı gütmeyen ve kamu yararına çalışan bir kuruluştur. ICANN'in misyonu ve ilkesi; teknik işlevleri demokrasi, işbirliği ve yasal süreç çerçevesinde yürütmektir. İnterneti güvenli, istikrarlı ve birlikte çalışabilir durumda tutmaya çalışır. Rekabeti teşvik eder ve internetin tanımlayıcıları konusunda politika geliştirir. İnternetin adlandırma sisteminin koordinasyonunu yürütür. Öte yandan sağlıklı bir rekabet düzeyini teşvik etmek için piyasa mekanizmalarını baz alır ve buna yönelik bir denge kurmayı hedefler (ICANN, t.y.b).

ICANN, misyonunu yerine getirmek amacıyla birtakım sözleşme ve gayri resmi anlaşmaya imza atmıştır. Bunlardan en önemlisi, ICANN ile ABD Ticaret Bakanlığı arasında imzalanan Ortak Proje Anlaşması (JPA) olarak da bilinen yenilenebilir

Mutabakat Muhtırası'dır (MOU) (NTIA, 1998b). 25 Kasım 1998'de yürürlüğe girmiş olan Muhtıra, ICANN'in internet yönetişimindeki rolünün yasal temelini oluşturmaktadır (Bygrave & Michaelsen, 2009, s. 105).

ICANN, seçim ve diğer karar alma süreçleri bakımından karmaşık ve çok katmanlı bir organizasyon yapısına sahiptir (Bygrave & Michaelsen, 2009, s. 107). Resmi olarak ICANN politikasını belirleyen organ Kurul'dur. Ancak, politikaların çoğu genellikle Politika Geliştirme Süreçlerini (PDP) başlatmakla görevli Destekleme Kuruluşları çerçevesinde, ICANN seçmenleri tarafından başlatılır ve geliştirilir (GNSO, t.y.). Adres Destekleme Kuruluşu (ASO); internet adreslerinin işletilmesi, atanması ve yönetimi ile ilgili politika konularında Kurul'a tavsiyelerde bulunur (ASO, t.y.).

Genel Adları Destekleme Kuruluşu (GNSO), gTLD'lerle ilgili temel politikalar geliştirmek ve Kurul'a tavsiye etmekten sorumludur. Kuruluş, yeni gTLD'lerle kökün genişletilmesine ilişkin politik süreçlerde ICANN'i destekler. Politika geliştirme genellikle aşağıdan yukarıya, fikir birliğine dayalı bir süreçtir (Bygrave & Michaelsen, 2009, s. 108). Ülke Kodu Adlarını Destekleme Kuruluşu (ccNSO), GNSO'ya benzer bir işleve sahiptir. Ancak ccNSO, ülke kodu üst düzey alan adlarını kapsayan küresel politika konularıyla ilgilenmektedir. Katılıma onay veren ccTLD yöneticilerinden oluşmaktadır (CCNSO, t.y.).

Buradaki en önemli aktör, Devlet Danışma Komitesi'dir (GAC). ICANN'in politikaları hakkında özellikle devletlerin talepleri doğrultusunda Yönetim Kuruluna tavsiye vermekle görevlidir. Öte yandan, ICANN politikaları ile çeşitli kanunlar ve uluslararası anlaşmalar arasında etkileşim olması veya kamu politikası sorunlarının etkilenmesi gibi durumlar söz konusu olduğunda da tavsiyeler vermektedir (GAC, t.y.). ICANN rejimine yönelik itirazların başında ABD hükümetinin bu kuruluşun gelişimi üzerinde oynadığı merkezi rol gelmektedir. Bu nedenle GAC, DNS yönetimi ve politikasına daha fazla uluslararası katılım sağlanması için önemli bir araç olarak görülmektedir (Bygrave & Michaelsen, 2009, s. 108).

Güvenlik ve İstikrar Danışma Komitesi (SSAC), Kurul tarafından atanan temsilcilerden oluşur. Kurul'a, internetin adlandırma ve adres tahsis sistemlerinin güvenliği ve bütünlüğü ile ilgili konularda tavsiyelerde bulunmaktan sorumludur (SSAC, t.y.). At-Large Danışma Komitesi (ALAC), bireysel internet kullanıcılarını temsil eder. ALAC üyeleri, internet kullanıcılarının coğrafi ve sosyal çeşitliliğini yansıtmayı amaçlayan

seçim prosedürlerine sahiptir. At-Large yapılarının altında Bölgesel At-Large Kuruluşları (RALO's) bulunmaktadır (ALAC, t.y.). Her coğrafi bölgede (Afrika, Asya Pasifik, Avrupa, Latin Amerika ve Kuzey Amerika) bir RALO mevcuttur.[16]

Kasım 2004'te ICANN, üyeler tarafından yapılan şikayetlerin bağımsız olarak değerlendirilmesini sağlamak amacıyla Ombudsman ofisini kurmuştur. Burada amaç, ICANN topluluğu üyelerinin kendilerine yönelik herhangi bir adaletsiz tutum karşısında şikayetlerini dile getirebilecekleri bir platform sağlanmasıdır. Ancak Ombudsman'ın şikâyete konu olan organlar tarafından alınan kararları iptal etme veya değiştirme yetkisi yoktur. Ombudsman yalnızca arabuluculuk yapabilmekte veya tavsiyelerde bulunabilmektedir (ICANN, t.y.c.).

ICANN, olgunlaşan bir kuruluştur ve hesap verebilirliğini ve şeffaflığını geliştirmek için adımlar atmaktadır. Bunlardan biri, yukarıda da ifade edildiği gibi Mart 2014'te NTIA'nın DNS'yi yönetme görevini küresel çok paydaşlı bir topluluğa devretme niyetini açıklamasıydı. Bu karar, internet yönetişiminin geleceği üzerine geniş çaplı tartışmaları tetikledi. NTIA, ICANN'e mevcut gözetim rolünün bir geçiş planı geliştirmesi için küresel paydaşları bir araya getirme görevi verdi (U.S. Department of State, 2015). Bu sürecin sonucu, 1 Ekim 2016'da, DNS üzerindeki gözetim rolünün başarıyla bir çok paydaşlı model ile değiştirilmesiydi. Bu geçiş, internet yönetişiminin geleceğinde önemli bir dönüm noktası olarak kabul edildi ve geniş ölçüde internetin küresel, açık ve çok paydaşlı yönetişimine olan bağlılığı yansıttı.[17]

ICANN'e dair meşruiyet sorunları halen devam etmektedir. Alan adı ve numaralandırma sistemini yönetme yetkisi, ABD Ticaret Bakanlığı ile 1998'de yapılan bir anlaşma sonucu ICANN'e verilmiştir. Ancak zamanla, ICANN'in meşruiyetine ve devletlerin internet yönetişimine dahil edilmesine yönelik tartışmalar artmıştır. NETmundial Girişimi gibi çabalar, küresel internet yönetişiminde daha fazla devlet katılımını savunmuş ancak somut değişikliklere yol açmamıştır. ICANN, GAC tavsiyelerine daha fazla uyum sağlanmasını teşvik etmek için yönetmeliklerinde

[16] AFRALO, APRALO, EURALO, LACRALO ve NARALO olmak üzere 5 tane bulunmaktadır. Ayrıntılı bilgi için bkz: ICANN At-Large. (t.y.). Regional At-Large Organizations (RALOs). https://atlarge.icann.org/ralos (02.04.2021).

[17] Ayrıntılı bilgi için bkz: U.S. Government Publishing Office. (2016). Examining the Multistakeholder Plan for Transitioning the Internet Assigned Number Authority. https://www.govinfo.gov/content/pkg/CHRG-114shrg23872/html/CHRG-114shrg23872.htm

değişiklikler önermiş, böylece teknik yönetişim ile jeopolitik kaygılar arasında daha dengeli bir ilişki kurmayı amaçlamıştır (Sylvain, 2015).

İnternetin küresel yönetişimi konusundaki bu tartışmalar ve ICANN'in rolüne dair sorun alanları, bu metnin dördüncü bölümünde detaylı bir şekilde ele alınmaktadır. Bu nedenle bu kısımda daha çok ICANN'in işleyişi, yapısı ve amaçlarına yer verilmiştir. Özetle, ICANN'in kuruluşu ve evrimi, internet yönetişimi alanında önemli bir dönüm noktası olmuş ve bu kuruluş, internetin adlandırma ve numaralandırma sistemlerinin küresel koordinasyonunu sağlayarak kritik bir işlev üstlenmiştir. ICANN'in çok paydaşlı yapısı, internet yönetişiminde demokratik bir modelin benimsenmesine olanak tanımış; fakat aynı zamanda ABD'nin bu kuruluş üzerindeki etkisi, küresel katılım ve eşitliğe dair soru işaretlerini de beraberinde getirmiştir. Özellikle, ABD Ticaret Bakanlığı ile yapılan anlaşmalar ve ICANN'in karar alma mekanizmaları, bu kuruluşun küresel meşruiyeti ve devletlerarası dengeler üzerinde tartışmalara yol açmıştır. GAC gibi organlar aracılığıyla devletlerin katılımını artırma çabaları, ICANN'in politikalarını daha bütüncül ve hesap verebilir hale getirme yönünde atılmış adımlar olsa da, hala eleştirilen noktalar mevcuttur.

1.2.7.4.Özel Sektör

Özel sektör, WSIS tarafından yapılan çok paydaşlı kategorizasyondaki önemli paydaşlardan biridir ve güçlü bir etkiye sahiptir. Özel sektör, küresel internet yönetişiminde yetki sahibi iken; devlet, politikaları belirleme noktasında kilit paydaştır (DeNardis, 2014, s. 227). İnternetin temeli ve online hizmetlerin büyük bir bölümü, özellikle Batı menşeili özel şirketlerin ve kuruluşların elindedir ve onlar tarafından işletilir.

Bu bağlamda özel sektör, internetin altyapısını ve hizmetlerini sağlar ve internet yönetişiminde önemli bir rol oynar. Şirketler ayrıca interneti ve kurallarını şekillendirmeye yardımcı olur. Örneğin, birçok web hizmeti ve sosyal ağ, sundukları hizmetler için "şartlar ve koşullar" veya "kullanım koşulları" oluşturmuştur. Bu şartlar, bir kullanıcının belirli bir platformda sunulan hizmetlere erişirken ne yapmaya yetkili olduğunu veya ne yapmaya yetkili olmadığını düzenler.[18] Telekomünikasyon sağlayıcıları ve diğer hizmet sağlayıcılar, veri akışı altyapısını, veri merkezlerini ve uluslararası denizaltı kablolarını “omurga” adı verilen ana hatlar aracılığıyla yönetir

[18] Örnek için bkz: Google (t.y.). Google Hizmet Şartları. https://policies.google.com/terms?hl=tr (23.03.2024).

(BIS Shrapnel, 2001, s. 6). Kamu yetkilileri ve sivil toplumun yanı sıra şirketler, belirli genel kural ve süreçleri uygulamak için birlikte çalışabilirler. Bunun bir örneği, devletlerin ve dijital teknoloji devlerinin ilk kez online terörist ve aşırılık yanlısı içeriği ortadan kaldırmak ve internetin teröristler tarafından araçsallaştırılmasına son vermek için bir dizi somut önlem almayı taahhüt ettiği Christchurch Eylem Çağrısı'dır.[19] İnternet ekonomisinde çalışan birçok ülke, çıkarlarını kurumsal ve kamusal alanda teşvik etmek için profesyonel dernekler kurmuştur. Örneğin France Digitale, The Galion Project ve Syntec Numerique bunlardan sadece birkaçını temsil etmektedir (Ministry for Europe and Foreign Affairs, 2020).

Özel sektörün bu rolleri, internetin işleyişi ve gelişimi üzerinde derin bir etkiye sahiptir. Bazı özel sektör paydaşları o kadar güçlü hale gelmiştir ki, çok paydaşlı mekanizmalara katılmaya ihtiyaç duymazlar ve hizmet şartları gibi kararları tek başlarına veya devletlerle birlikte almaktadır. Buna ithafen van der Spuy, "en önemli kararların çoğu küresel işletmelerin yönetim kurullarında ve araştırma-geliştirme tesislerinde alınır" ifadesini kullanmıştır. Bu durum; kullanıcılar, devletler, sivil toplum ve akademi gibi diğer paydaşların karar alma süreçlerinden dışlanmasına yol açabilmektedir. Güç dinamikleri, devletlerden ve sivil toplumdan özel sektöre doğru kaymaktadır (2017, s. 31).

Özel sektörün büyük oyuncuları, kullanıcı sayılarını maksimize edebilme, kapsam ve ölçek ekonomilerinden faydalanabilme ve verileri tüketiciler ve kendileri için değer yaratma amacıyla kullanabilme avantajları sayesinde ağlardan büyük güç elde ederler. Bu durumun sonucu olarak teknolojik güç, büyük oranda birkaç küresel şirkette yoğunlaşmıştır. Bu şirketler, çoğu devlet tarafından etkili bir şekilde denetlenmeden faaliyet gösterme özgürlüğüne sahiptir ve günümüzde internet yönetişiminin en güçlü aktörleri haline gelmiştir. Karar alma süreçleri, çok paydaşlılık ilkelerine bağlı olmaktan ziyade, bu şirketlerin kendi iç dinamikleri tarafından yönlendirilmektedir (Souter, 2021). Özel sektörün seçilmemiş olması, şeffaflık ve hesap verebilirlik eksikliği gibi unsurlar, internet yönetişiminde "kamuoyuna açık olmayan yollarla" iş yürütmelerine ve çok paydaşlı uygulamanın demokratik potansiyelini göz ardı etmelerine yol açmaktadır (Carr, 2015).

[19] Christchurch Eylem Çağrısı, terörist ve şiddet içerikli materyallerin online ortamlardan kaldırılması için 130'dan fazla devlet, çevrimiçi hizmet sağlayıcı ve sivil toplum kuruluşunun bir araya geldiği bir topluluktur. Daha fazla bilgi için bkz: https://www.christchurchcall.com/ (23.03.2024).

Ancak özel sektörün bu uygulamaları, gerek siber uzaydaki diğer aktörler, gerekse de uluslararası insan hakları hukuku bağlamında "sorunlu" olarak kabul edilmektedir. Zira şirketler, uluslararası insan hakları hukukuna doğrudan bağlı değillerdir. Bu kapsama yalnızca devletler dahildir. Nitekim internet altyapısının önemli bir kısmını elinde bulunduran bu özel kuruluşların faaliyetlerine ulusal hukukun uygulanması da son derece zordur. Ancak devletlerin siber suçlara karşı koyma hakkı ve görevi saklıdır. Bu durumda devlet, bu görevini yerine getirebilmek amacıyla ilgili özel sektörün yardımını alabilmektedir. Bu doğrultuda özel sektör, ürün ve hizmetlerinin suç amacıyla kullanılmasından kaçınmak isteyecektir (Council of Europe Commissioner for Human Rights, 2014, s. 10).

Özel sektörün kendi iç denetim mekanizmalarını uygulamasının yol açtığı sosyo-politik sorunlardan bir diğeri de insan hakları sorunlarıdır. Özellikle insan haklarının entegrasyonu konusunda internet, özel sektör için -bilhassa internet ve telekomünikasyon alanındaki şirketler için- giderek artan bir sorumluluk alanı haline gelmiştir. BM Özel Raportörü David Kaye'nin 2017 yılındaki raporunda vurgulandığı üzere, teknoloji şirketlerinin ürün ve hizmetlerini, insan hakları ihlallerine sebep olmayacak veya bu ihlaller için bir araç olarak kullanılmayacak şekilde tasarlamaları gerekmektedir (UNGA, 2017).

Öte yandan özel sektördeki oyuncular devlete meydan okuyacak kadar büyüdüğünde – özellikle denetim mekanizmaları bakımından– güçlü bir muhalefetle karşı karşıya kalırlar ve son Alibaba, Didi ve Tencent örneklerinde[20] olduğu gibi planlarını uyarlamaları veya tamamen değiştirmeleri gerekir (Pigatto & Datysgeld & Silva, 2021, s. 3). Pigatto vd., özel sektörün bu öz denetim uygulamalarından vazgeçtiğini ve toplumsal açıdan karmaşık kararlar alma sürecinin getirdiği yükten uzaklaşmayı tercih ettiğini belirtmektedir (2021, s. 8). Bu durum, özel sektörün işleyişinde ve devletle olan ilişkilerinde bir dönüşümü işaret etmektedir. Bu görüşe göre özel sektör, genellikle kâr amacı güderken, artık toplumsal sorumluluklarını da gözetmek durumundadır.

[20] Çin'in rekabet düzenleyicisi, 2011'den itibaren gerçekleşen ancak bildirilmeyen birleşme ve satın almalar nedeniyle Tencent, Alibaba ve Didi dahil olmak üzere teknoloji devlerine cezalar verdi. Bu işlemler, sosyal medya ve video oyunu devi Tencent ile ilgili 12 vaka, e-ticaret devi Alibaba ile ilgili 5 vaka ve yolculuk paylaşım platformu operatörü Didi ve iştirakleri ile ilgili 4 vakayı içeriyordu. Her bir ihlal için 500.000 yuan (yaklaşık 74.600 ABD doları) -Devlet Piyasa Düzenleme İdaresi'nin (SAMR) antitröst yasası uyarınca uygulayabileceği maksimum ceza miktarı- para cezası verildi. Detaylı bilgi için bkz: South China Morning Post. (2022, Ekim 11). Tencent, Alibaba and Didi fined by China antitrust watchdog for unreported merger deals as early as 2011. Yahoo Finance. https://finance.yahoo.com/news/tencent-alibaba-didi-fined-china-093000180.html?guccounter=1.

Karmaşık kararlar, etik, çevresel, sosyal ve ekonomik boyutları içerebilirken; bu kararların alınması, şirketler için hem maliyetli olabilmekte hem de itibar yönetimi açısından riskler taşıyabilmektedir. Öz denetimden vazgeçmek, şirketlerin daha esnek ve hızlı hareket etme imkânı sunarken, bu sürecin toplumsal sorumluluk ve sürdürülebilirlik gibi kavramlarla nasıl uyum sağlayacağı noktasında önemli bir soru işareti oluşturur.

Facebook'un Gözetim Kurulu,[21] büyük bir teknoloji şirketinin içerik yönetimi ve karar verme süreçlerinde dış kaynak kullanımına başvurduğunun önemli bir örneğidir (Pigatto vd., 2021, s. 8). Gözetim Kurulu'nun oluşturulması, Facebook'un içerik yönetimi konusundaki eleştirilere yanıt olarak görülebilir. Platformun, nefret söylemi, yanlış bilgilendirme, şiddet içeren içerik ve diğer zararlı materyalleri yönetme biçimi, sık sık kamuoyu ve düzenleyici kurumlar tarafından sorgulanmıştır. Kurul, Facebook'un bu tür içeriklerle ilgili kararlarının şeffaflığını ve hesap verebilirliğini artırmayı amaçlamaktadır.

Özel sektörün bu hamlelerini "meşruiyet" çerçevesinde değerlendirenler de vardır (Carr, 2015). Özel sektörün internet yönetişiminde artan rolü, bu aktörlerin meşruiyeti ve internetin demokratik bir şekilde yönetilip yönetilmediği konularında sorgulamaları beraberinde getirmiştir. Özel sektör, seçilmiş bir kurum olmamakla birlikte, uzmanlık alanındaki bilgi birikimi ve sivil toplumla olan uyumunu ön plana çıkararak meşruiyet kazanmaya çalışmaktadır. Ücretsiz online hizmetler sunarken kullanıcıların gizliliğini ihlal etse de, devlete karşı sivil toplumun yanında olduğunu savunarak meşruiyetini korumaya çalışmaktadır. Bu savunma biçimi, özel sektörün meşruiyet arayışının bir temelini oluşturmakla birlikte, bu argümanların güvenilirliği üzerine tartışmalar devam etmektedir. Google'ın "Project Nightingale"[22] isimli gizli projesi, Facebook'un

[21] Facebook'un Gözetim Kurulu (Facebook Oversight Board), Facebook ve Instagram'daki içerikle ilgili kararları gözden geçirmek üzere tasarlanmış bir bağımsız denetim organıdır. 2020 yılında faaliyete geçen bu kurul, kullanıcıların ve Facebook'un kendisinin itiraz ettiği içerik kararlarını inceleyip, bu kararların platformun politikaları ve uluslararası insan hakları standartlarına uygunluğunu değerlendirir. Kurulun verdiği kararlar, ilgili içerikler için Facebook ve Instagram'ı bağlayıcıdır ve kurul ayrıca politika tavsiyelerinde bulunabilir, ancak bu tavsiyeler zorunlu değildir. Ayrıntılı bilgi için bkz: https://oversightboard.com/ (20.10.2023).

[22] 2019 yılında ortaya çıkan bu proje kapsamında, Google ve Ascension (ABD'nin en büyük ikinci sağlık hizmetleri şirketi) arasındaki gizli bir anlaşma kapsamında, milyonlarca Amerikalının kişisel sağlık bilgilerinin Google tarafından toplandığı ve işlendiği açığa çıkmıştır. Bu bilgiler arasında hastaların isimleri, doğum tarihleri, laboratuvar sonuçları, teşhisler ve hastaneye yatış bilgileri gibi oldukça hassas veriler bulunmaktadır. Bu proje, hastaların bilgisi veya açık rızası olmadan gerçekleştirilmiş olması nedeniyle ciddi gizlilik ve etik endişeleri doğurmuştur. Ayrıntılı bilgi için bkz: Worldhealth.net. (2019,

Cambridge Analytica Skandalı[23], Yahoo E-posta İhlalleri[24] gibi olaylar, özel sektör ve sivil toplum uyumu anlatısını zayıflatan örnekler olarak karşımıza çıkmaktadır. Bu meşruiyet zorlukları ve özel sektörün bunları hafifletmek için kullandığı mekanizmalar, çok paydaşlı süreçte gücü dengelemek veya karşı koymak yerine güç toplamaya hizmet etmektedir (Carr, 2015).

Diğer yandan devletler, interneti politika oluşturma suretiyle şekillendirebilmekte ve bazı durumlarda interneti özel sektör aracılığıyla kontrol edebilmektedir (Carr, 2016, s. 10). ABD'nin internet yönetişiminde özel sektörün liderliğini önceliklendiren yaklaşımı bununla ilintilidir. ABD hükümeti ile ICANN arasındaki yakın ilişkiye rağmen, özel sektörün öncülüğünde bir yönetişim modelinin desteklenmesi sürekli olarak ön plana çıkarılmaktadır (Mueller, 2010; Carr, 2015). Carr'a göre (2015) özel sektör, internet yönetişimi konusunda ABD hükümeti ile güçlü ilişkiler kurarak avantaj elde etmiş, ancak aynı zamanda dijital hakların uygulanması konusunda interneti "balkanlaştırmada"[25] diğer aktörlerden çok daha fazlasını yapmıştır. DeNardis'e göre ise devletin interneti bu özel aktörler aracılığıyla kontrol etmesi, devletlerin veri akışları üzerinde hesaplanabilir ve şeffaf olmaktan uzak bir güce sahip olmasına sebebiyet vermiştir (2014, s. 15). Zira BİT, doğası gereği küreseldir ve her ne kadar "bulut" teknolojisinden söz edilse de güvendiği altyapı fizikseldir ve gerçek konumda bulunur, devlet kurumlarından çok özel kuruluşlar tarafından yönetilir ve kontrol edilir (Council of Europe Commissioner for Human Rights, 2014, s. 33).

Ancak bu çalışma açısından sorunlu olan internet üzerinde şirketlerin devletlerden daha üstün rol oynaması değildir. Çünkü bu çalışma, nihayetinde internet yönetişiminin "çok

---

Kasım 13). Google & Ascension's Data Project Sparks Privacy Concerns. https://www.worldhealth.net/news/google-ascensions-data-project-sparks-privacy-concerns/.

[23] 2018'de, Cambridge Analytica'nın 87 milyon Facebook kullanıcısının verilerini, kullanıcıların bilgisi dışında siyasi reklamlar için kullanmak üzere topladığı ortaya çıktı. Bu durum, kullanıcı gizliliğine yönelik ciddi endişeleri gündeme getirdi ve sosyal medya platformlarının veri yönetişimi ve gizlilik politikaları üzerinde daha fazla denetim talep edilmesine yol açtı. Ayrıntılı bilgi için bkz: The New York Times. (2018 Nisan 4). Facebook Says Cambridge Analytica Harvested Data of Up to 87 Million Users. https://www.nytimes.com/2018/04/04/technology/mark-zuckerberg-testify-congress.html.

[24] Yahoo, 2013 ve 2014 yıllarında gerçekleşen ve 1 milyardan fazla kullanıcının hesap bilgilerinin çalındığı iki büyük veri ihlalini 2016'da duyurdu. Bu ihlaller, internet şirketlerinin kullanıcı verilerini nasıl koruduğu ve ihlalleri kamuoyuna bildirme konusundaki şeffaflığı hakkında soruları beraberinde getirdi. Ayrıntılı bilgi için bkz: The New York Times. (2016, Aralık 14). Yahoo Says 1 Billion User Accounts Were Hacked. https://www.nytimes.com/2016/12/14/technology/yahoo-hack.html.

[25] "İnternetin balkanlaşması" ifadesi, internetin giderek daha fazla parçalanmış ve bölgeselleşmiş bir yapıya bürünmesini ifade eder. Bu terim, genellikle ulusal sınırlar, politik çıkarlar veya ekonomik faktörler nedeniyle internetin küresel bir ağ olmaktan çıkıp, farklı bölgelerde farklı kuralların, düzenlemelerin ve erişim politikalarının uygulandığı bir yapıya dönüşmesini anlatmak için kullanılır. Bu durum, aynı zamanda "internetin parçalanması" veya "dijital demir perde" gibi ifadelerle de tanımlanabilmektedir (Taneja & Wu, 2014; Carr, 2015; Lytvynenko & Kantur, 2023).

paydaşlı" bir doğaya sahip olduğunu ve olması gerektiğini savunmaktadır. Burada esas sorunlu olan nokta, tek bir devletin menşeinde olan özel şirketlerin internet üzerinde söz sahibi olmasıdır. Zira özel kuruluşlar, kuruldukları veya aktif oldukları ülkelerin ulusal yasalarına tabidirler ve bu yasalar her zaman uluslararası hukuka veya uluslararası insan hakları standartlarına uygun olmayabilir. İfade özgürlüğü başta olmak üzere uluslararası insan hakları hukukunu ihlal etmeye varan kısıtlamalar getirebilir veya gözetim mekanizmalarını kullanabilirler. Bu tür eylemler, diğer devletlerin egemenliğine aykırı sınır ötesi uygulamaları beraberinde getirebilir veya kullanıcıların gizlilik haklarını büyük oranda ihlal edebilir. Bu durumda internet altyapısını elinde bulunduran özel kuruluşlar, hangi devletin egemenliğinde olursa olsun "sorunlu" olarak kabul edilecektir. Çünkü diğer devletler tarafından menşei devletin çıkarlarını gözetmekle suçlanacaklardır (Council of Europe Commissioner for Human Rights, 2014, s. 9).

Bu şirketlerin kullanıcı sayılarını ve veri üzerindeki kontrolünü maksimize etme yetenekleri, onlara önemli bir güç kazandırmış ve internet yönetişimi üzerinde belirleyici bir etkiye sahip olmalarını sağlamıştır. Ancak, bu gücün merkezileşmesi ve karar alma süreçlerindeki şeffaflık ve hesap verebilirlik eksikliği, internetin demokratik yönetişimi ve çok paydaşlı yapısına dair endişeleri de beraberinde getirmiştir. Bu bağlamda özel sektörün internet üzerindeki hakimiyetinin uluslararası insan hakları standartlarına uygun bir şekilde denetlenmesi, sınırlandırılması ve uyarlanması zorunluluğu açıktır. Özellikle özel sektörün alandaki hiyerarşik üstünlüğü göz önünde bulundurulduğunda, rollerin dengelenme ihtiyacı daha da belirginleşmektedir.

1.2.7.5.Sivil Toplum

Gramsci, sivil toplumu hegemonyanın doğrudan bir ifadesi olarak görmüştür. Gramsci'ye göre hegemonya, sadece hakimiyet meselesi değil, aynı zamanda "yönlendirme" gerektiren bir durumdur. Bu bağlamda sivil toplum, fethedilmesi gereken bir nesne, farklı sosyal ve politik gruplar arasında bir savaş alanı ve güçlerin yapılanmasının sonucu olarak ortaya çıkar (Brighenti, 2019, s. 483). Rosenau ise küresel düzen ve büyük ölçekli yönetişim kavramlarının makro toplulukları ve kurumları, düzenin alabileceği her türlü biçimin temeli olarak ele aldığını ifade eder (1992b, s. 273). Sivil toplum da küresel düzenin ve yönetişimin temel bir bileşeni olarak, insanların ortak çıkarları peşinde koşmak için bir araya geldikleri alan olarak tanımlanabilir. Burada amaç, çıkar veya siyasi iktidar elde etmek değil, kolektif

eylemde bulunmaktır. Bu bağlamda sivil toplum, küresel kamu çıkarlarını koruyarak güçlü bir etki yaratabilmektedir (DiploFoundation, 2006, s. 5). Sivil toplum terimi, STK'lar veya vakıflar gibi yapıları ifade eder. Bilinçlendirme kampanyaları, politika oluşturma süreçlerine katılım ve yeni teknolojiler ve uygulamalarla ilgili ortak değerlerin araştırılması yoluyla internetin düzenlenmesini veya kendi kendini düzenlemesini etkiler (Ministry for Europe and Foreign Affairs, 2020).

Küresel internet yönetişiminde sivil toplum, WSIS tarafından yapılan ilk hazırlık toplantısında (PrepCom1) internet yönetişimi için önemli bir aktör olarak kabul edilmiştir. Bunun yanında, WSIS'in ilk aşamasının ardından Sivil Toplum Bürosu (CSB) kurulmuştur. CSB, sivil toplumdaki farklı seçmenleri temsil eden çeşitli aileler ve grup toplantılarından oluşmaktadır. Müzakere süreciyle ilgili bilgileri topluluğun tüm üyelerine yaymak için ağ oluşturma kanalları sağlanmıştır. Büro ayrıca, Afrika, Latin Amerika ve Karayipler, Asya Pasifik, Avrupa, Kuzey Amerika, Orta Doğu ve Batı Asya'dan bölgesel grupları da temsil etmektedir. CSB'nin işlevi, Zirve'ye sivil toplum katılımını en üst düzeye çıkarmaktır (WSIS, t.y.). CSB'nin kurulması, BM tarihinde ve uluslararası müzakerelerde bir "dönüm noktası" olarak kabul edilmektedir. Zira sivil toplum ilk kez, hükümetlerarası diyaloğu kolaylaştıran mekanizmalara sahip bir BM zirvesi tarafından aktör olarak kabul edilmiştir (DiploFoundation, 2006, s. 5).

Sivil toplum düzeyinde küresel internet yönetişimi sorunlarına odaklanan çeşitli aktörler ve etkinlikler vardır. Bu alanı kapsamlı bir şekilde tanımlamak zor olsa da küresel olarak aktif olan sivil toplum kuruluşları, grupları ve girişimleri mevcuttur. Bugün sivil toplumun kilit oyuncuları olarak yukarıda çalışmanın 1.2.7.3. alt başlıkta bahsi geçen uluslararası standardizasyon kuruluşları da dahil edilse de, yukarıda belirtildiği üzere bu kuruluşların kendilerini bu kategoriye dahil etme çabası tartışmaları tetiklemektedir. Zira bahsi geçen kuruluşlar, sivil toplumdan ziyade teknik topluluk adı altında birleşen uluslararası kuruluşları ifade etmektedir. Oysa spesifik olarak sivil toplum adına faaliyetler yürüten alt birimlerin varlığı söz konusudur. Bu doğrultuda sivil toplumun önemli aktörleri arasında şu kurumlar gösterilmektedir: Aşamalı İletişim Derneği (APC), Best Bits, İnternet Yönetişim Grupları (IGC), Just Net Coalition (JNC), Commercial Non Commercial Payolder Group (NCSG) ve Sivil Toplum Koordinasyon Grubu (CSCG) (Haristya, 2020, s. 253). Sivil toplumun bu aktörleri, kendi sivil toplum ağlarında internet yönetişimi ile ilgili konulara ilişkin tartışmalara katılarak internet yönetişiminin gelişimine katkı sağlamaktadır.

Sivil toplum, kamu yetkililerinin temsil ettiği genel çıkarın ötesine geçen farklı grupların sesini temsil eder. STK'lar, kendi çıkarlarını değil, temsil ettikleri toplulukların çıkarlarını savunur ve aracı rolü oynar. Resmi veya gayri resmi olabilir ve farklı yasal ve organizasyonel yapılara sahip olabilirler. Aynı zamanda yerel veya küresel çıkar gruplarını temsil edebilirler. Diğer yandan, çok paydaşlı süreçlerde kurumların meşruiyetini ve hesap verebilirliğini sağlarlar (Meyer & Shahin, 2021, s. 3).

Sivil toplum, devletler ve diğer sektörler arasında halkın taban düzeyinde karşılaştığı temel sorunlar ve sivil toplumun gerçek ihtiyaçları konusunda farkındalığı artırır. Aynı zamanda, internete evrensel erişim için güçlü bir savunucudur. Bu, geleneksel veya modern teknolojileri kullanma kapasitesine bakılmaksızın herkesin bilgi ve iletişim teknolojilerinden yararlanabileceği anlamına gelir. Bunun yanında, bilgi toplumuna katılımda toplumsal cinsiyet eşitliğini teşvik eder ve bilgi toplumunda insan haklarının korunmasını ve geliştirilmesini savunur (DiploFoundation, 2006, s. 26).

Sivil toplumun etkisi, diğer konuların yanı sıra insan hakları, ifade özgürlüğü, açık kaynak geliştirme ve bilgi paylaşımı ile ilgilidir. Bu bağlamda sivil toplum özellikle internetin bu unsurlarının savunulması açısından "yükselen bir güç" olarak kabul edilmektedir. Kowack'a göre internet modelinin ilerlemesi, dünya çapında uzmanlardan oluşan bir seçmen kitlesinin ortaya çıkmasına bağlı olacaktır. Ona göre bu kitle, yalnızca teknik uzmanlarla sınırlı olmamalıdır. Aksine, daha fazla gelişmeyi teşvik edebilecek politika uzmanları sürece dahil edilmelidir. Bunun yanında Kowack, sivil toplumun üç işleve hizmet ettiğini öne sürmüştür. Bunlardan birincisi; forumlarda bu unsurları destekleyecek ve savunacak önemli sayıda insanın olmasını sağlamak. İkincisi, en uygun sonuçları elde etmek için geniş bir fikir yelpazesi getirmek. Üçüncüsü ise, dünyanın dört bir yanındaki insanlara ve uluslara katılımlarına açık kanallar olduğunu göstermek için konferanslar ve çalıştaylar düzenlemektir (1997, s. 56). Mueller ve diğerlerine göre de sivil toplumun uluslararası karar alma sürecine katılımı, küresel yönetişim unsurlarını ilerletmek için önemli bir fırsattır. Bunun yanında, sivil toplumun internet yönetişimi sürecine güçlü katılımını önemli olarak görmektedirler (2007, s. 252).

Normatif perspektifler genellikle daha kapsayıcı ve katılımcı yönetişim biçimlerini savunarak küresel düzeyde demokratik ilkelerin önemini vurgular. Bu, uluslararası kurumların demokratikleştirilmesi ve sivil toplumun küresel karar alma süreçlerinde

güçlendirilmesi tartışmalarını içerir. Drezner'e göre internet, uluslararası ilişkilerin devlet merkezli teorilerine meydan okurken; küresel sivil toplumu savunanlar için kolaylıklar sağlamaktadır. Şayet devletler, internet yönetişiminde kilit aktörler olarak kabul edilecekse, küreselleşme literatürünün devletler ve devlet dışı aktörler arasındaki ilişkiyi yeniden gözden geçirmesi gerekecektir. Zira uluslararası kuruluşlar ve sivil toplum, küresel yönetişimde önemli bir role sahiptir. Bazı durumlarda devletlerden bağımsız hareket etseler de, devlet çıkarları doğrultusunda hareket ettikleri takdirde devletler tarafından önemli aktörler olarak kabul edilirler (2008, s. 118).

Bugünkü konjonktürde sivil toplumun internet yönetişimindeki zayıf temsili ve heterojen yapısı, normatif perspektiflerin savunduğu daha kapsayıcı ve katılımcı yönetişim biçimleriyle çelişmektedir. Sivil toplum, diğer paydaşlara kıyasla daha dağınık ve heterojen bir yapıya sahip olduğundan, STK'ların ortak bir sesle konuşması ve ortak bir hedefe doğru koordineli bir şekilde hareket etmesi birtakım zorluklar teşkil etmektedir. Sivil toplumun internet yönetişimindeki temsili, diğer paydaşlara kıyasla daha zayıftır. Bunun sebebi, STK'ların seçimler yoluyla veya başka bir demokratik mekanizmayla seçilmemiş olmasıdır. Bu durum, sivil toplumun diğer paydaşlar tarafından meşru bir temsilci olarak kabul edilmesini zorlaştırır. Ancak bu güçsüzlük, diğer iki ana paydaş (devletler ve özel sektör) için, sivil toplumun katılımını tanıyarak ve onayını alarak, kendi pozisyonlarını güçlendirmek ve meşruiyet kazanmak için bir fırsat sunar. Bu durum, sivil toplumun görüşlerinin ve katkılarının yüzeysel bir şekilde kabul edilip desteklenmesine yol açarken, aslında devlet ve özel sektörün çıkarlarına hizmet etmesine sebebiyet vermektedir (Carr, 2015).

Görüldüğü üzere sivil toplum paydaşları, tanınma mücadelesi ve çekişmesinin yanı sıra, küresel çok paydaşlı süreçlere bir grup olarak katıldıklarında kararlara varmaya çalışırken aralarındaki çeşitliliği yönetmek gibi daha az bilinen zorluklarla da karşılaşmaktadır (Haristya, 2020, s. 252). Bu nedenle, sivil toplumun bu eşitsiz katılım zeminini değiştirmek için bazı adımlar atması gerekir. İlk olarak, özel sektörün internet yönetişimindeki artan rolüne karşı dikkatli bir bakış açısına sahip olmalı ve bu alandaki demokratik değerlerin korunması için gerekli adımları atmalıdır (Carr, 2015). Çok paydaşlı internet yönetişiminde diğer paydaşların gözetim ve hesap verebilirlik sağlama vaadinin takipçisi olmalı; insan hakları, özgür ve açık internet, eşit erişim ve ağ tarafsızlığı gibi değerleri teşvik eden normatif bir gündemle birleştirmelidir. Bu

bağlamda sivil toplum, maddi kazanç veya kamu görevi odaklı olmaktan ziyade, diğer paydaşların kural koyma çabalarını geliştirmeye odaklanmalıdır.

1.2.7.6.Bireyler/Kullanıcılar

WSIS'te (2005) tanımlanan paydaş sınıflandırmasında bireyler yer almamaktadır. Buna karşılık, NETmundial (2014) internet yönetişiminde devletler, özel sektör, sivil toplum, teknik topluluk, akademi ve kullanıcıları, her birinin rolleri ve sorumlulukları çerçevesinde temel aktörler olarak tanımlamıştır. NETmundial'e göre kullanıcılar, bu ekosistemin merkezinde yer alır. Bireyler, gündelik internet kullanımlarıyla dijital dünyanın şekillenmesine katkıda bulunur. Onların tercihleri, geri bildirimleri ve katılımları, internetin nasıl geliştiğini ve yönetildiğini doğrudan etkiler. Kullanıcıların sesleri, internetin daha demokratik ve erişilebilir olmasında kritik bir role sahiptir.

Bu çalışmada, WSIS tarafından bireylerin internet yönetişimi sürecindeki rollerinin göz ardı edilmesi, önemli bir eksiklik olarak ele alınmıştır. Bu bağlamda, NETmundial'in sürece dahil ettiği "kullanıcılar" kategorisi, bu çalışmanın analizine entegre edilmiştir. Zira internet, bireylerin günlük hayatının ayrılmaz bir parçası haline gelmişken, onların bu süreçte aktif bir rol almaları elzem görülmektedir. Bireylerin seslerinin duyulması, ihtiyaç ve beklentilerinin karşılanması, internetin demokratik, açık ve herkes için erişilebilir olmasını sağlamada kritik bir öneme sahiptir. Bu bağlamda, Zimmermann ve Renaud'un (2019) ele aldıkları "insan odaklı paradigma değişikliği", siber güvenlik alanında olduğu gibi, internet yönetişimi sürecinde de bireylerin önemini vurgulayan güçlü bir örnek teşkil eder. Zimmermann ve Renaud, siber güvenlikteki geleneksel "insanı zayıf halka olarak görme" yaklaşımını eleştirel bir şekilde sorgulamaktadır. Yazarlar, insanların doğal güçlü yönlerini kullanarak ve onların kısıtlılıklarına uyum sağlayacak şekilde sistemler ve protokoller tasarlayarak, siber güvenlikte daha etkili ve kullanıcı merkezli bir yaklaşımın mümkün olduğunu savunur. Bu bağlamda, "sorun olarak insan" anlayışından "çözüm olarak insan" anlayışına geçiş yapılmasının, sistem tasarımında insan faktörlerini ön plana çıkararak siber güvenliği güçlendireceğini öne sürmektedir.

Diğer yandan Venables, siber güvenliğin teknik önlemlerin ötesinde, insan davranışlarını ve sosyal dinamikleri anlamayı gerektiren bir süreç olduğunu belirterek siber alanın karmaşıklığını ve güvenliğin insan odaklı yaklaşımını vurgular (2021, ss. 9-10). Siber uzay, insan etkileşimi olmaksızın var olamaz; her adımda insanların

müdahalesine ihtiyaç duyar. Bu etkileşim, siber güvenliğin anlaşılması ve uygulanmasında kritik bir role sahip olan insan katmanı aracılığıyla gerçekleşir. İnsan katmanı, siber uzayı nasıl kullandığımızı ve güvenlik açıklarına karşı nasıl korunduğumuzu şekillendiren, hem güvenlik tehditlerinin kaynağı hem de çözümün parçasıdır. Bu katmanda, kullanıcı eğitimi ve denetim en etkili güvenlik önlemleri arasında yer alır. İnsan faktörünü dikkate almak, siber uzayın daha sezgisel kullanımını sağlayarak, her kullanıcı seviyesinde güvenliği artırabilir. Aynı zamanda, sosyal mühendislik gibi insan odaklı tehditlere karşı savunmayı güçlendirir. Bu bağlamda, siber uzayın ve teknolojik araçların evrimi, insan-makine etkileşiminin derinleşmesine işaret ederken, güvenlik stratejilerimizin de bu dinamik etkileşime uyum sağlaması gerektiğini vurgular.

Venables, siber uzaydaki "insan katmanı"nda üç ayrı sınıflandırma yapar: birey, persona ve sosyal gruplar. Ona göre siber uzayda bireylerin varlığı, her birimizin eşsiz dijital kimliği ile tanımlanır. Bu kimlik, bankacılık işlemlerinden sosyal medya hesaplarına kadar geniş bir yelpazede kullanılır ve dijital imzaların temel taşını oluşturur vurgular. Bu nedenle, kişisel bilgilerin güvenliği, kimlik avının önlenmesi için kritik öneme sahiptir. Bireysel kimliklerin yanı sıra, her kişi birden fazla persona sahibi olabilir; mesleki rollerden kişisel ilgilere kadar değişen bu roller, sosyal mühendislik saldırılarında hedef alınabilir. Sosyal gruplar ise, bireylerin ve personaların bir araya geldiği, ortak ilgi alanlarına dayalı topluluklardır. Bu gruplar, bireylerin davranışlarını tahmin etmede kullanılabilir (2021, s. 10).

Küresel internet yönetişimi, çok büyük ve çeşitli bir aktörler topluluğunu içerir. Bu durum, Olson'un (1993) büyük gruplardaki kolektif eylem sorununu[26] akıllara getirir. Keza NETmundial toplantısının ardından, çok paydaşlı internet yönetişimi süreçlerinde farklı paydaş gruplarının, özellikle "kullanıcılar" ve "teknik topluluk" gibi grupların temsiliyle ilgili bazı önemli sorunlar gündeme gelmiştir. Kullanıcıların kim tarafından temsil edildiği ve teknik topluluğun özel sektör ve akademi ile olan potansiyel çakışmaları, temsilin çeşitliliği ve çıkarların çift temsili riskleri konusunda endişeleri artırmıştır. IETF toplantılarına katılanların analizi, teknik topluluğun sıklıkla özel

[26] Olson'un kolektif eylem teorisine göre, küçük gruplarda bireylerin her biri, grubun toplu çabalarından elde edilen faydalardan önemli bir pay alır. Bu, küçük gruplarda işbirliğini ve kolektif eylemi teşvik eder, çünkü her bireyin katkıları daha görünür ve faydaları doğrudan hissedilir. Büyük nüfuslarda ise bireylerin katkılarının toplam fayda üzerindeki etkisi azalır ve kolektif eylem için gerekli motivasyon zayıflar (1993, s. 567).

sektör ve akademik kurumlarla çakıştığını, bu durumun aynı ilgi alanlarının iki veya üç kat temsil edilmesi riskini doğurduğunu göstermiştir (Belli, 2015, s. 7).

Diğer yandan, yüksek katılım maliyetleri ve genellikle geniş bir kullanıcı kitlesine yayılan faydalar, bireysel ve küçük ölçekli katılımcıların sürece etkin bir şekilde dahil olmalarını zorlaştırır. Ancak siber uzay, birbirini etkileyebilen çok sayıda katılımcının olduğu bir ortamdır. Bu alan, doğası gereği şeffaftır ve kullanıcılar tarafından tanımlanır, genişletilir, kısıtlanır veya sansürlenir (Mihr, 2016, s. 316). Her bir aktörün, özellikle de bireylerin ve küçük örgütlerin, genel yönetişime katkıda bulunmasının maliyeti yüksektir, ancak faydaları genellikle tüm kullanıcılar arasında yayılır. Ancak NETmundial'in vurguladığı gibi, bu çok paydaşlı yaklaşım, her grubun eşsiz katkılarını tanıyarak ve her birinin önemini vurgulayarak, geniş bir katılımcı yelpazesinin dahil edilmesinin önemini ortaya koyar.

Sonuç olarak bireylerin ve küçük örgütlerin aktif katılımı ve katkıları olmadan, internet yönetişimi, toplumun geniş kesimlerinin ihtiyaçlarını ve beklentilerini yansıtmada eksik kalacaktır. Bu bağlamda bireylere, internetin nasıl şekillendirildiği ve geleceğinin nasıl inşa edileceği konusunda söz hakkı verilmelidir. Bu türden bir katılım, çeşitlilik, şeffaflık ve kapsayıcılık ilkelerine dayanan bir yönetişim yapısının oluşturulmasını sağlayarak, tüm toplum kesimlerinin seslerinin duyulmasına ve internetin evriminin kolektif bir vizyonla yönlendirilmesine olanak tanır. İnternetin son kullanıcıları - bireyler, işletmeler ve topluluklar- kendi ihtiyaçları, tercihleri ve davranışları ile internetin şekillendirilmesinde dolaylı bir role sahip olduğundan, kullanıcı katılımının sağlayacağı geri bildirim ve kamuoyu oluşumu, internet yönetişimi üzerinde etkili olacaktır.

1.3. Kuramsal Çerçeve: Normatif Bakış Açısını Kuramsallaştırma

Robert Cox, teoriyi şöyle tanımlar: "Teori gerçekliği takip eder. Aynı zamanda gerçeklikten önce gelir ve onu şekillendirir. Diğer bir deyişle, olayların gerçekleştiği gerçek bir tarihsel dünya vardır; ve teori, olanlar üzerine düşünülerek yapılır." (1992, s. 133). Bu perspektif, teorinin sadece mevcut olayları ve durumları açıklamakla kalmayıp, aynı zamanda gelecekteki eylemleri ve politikaları yönlendirme kapasitesine de sahip olduğunu belirtir. Bu bağlamda, teorik çerçeve oluşturmanın küresel internet yönetişimi için önemi, özellikle günümüzdeki hızla değişen teknolojik ve sosyo-politik koşullar altında daha da belirginleşmektedir. Küresel internet yönetişimi, çeşitli

aktörlerin katılımıyla internetin işleyişi, kaynaklarının dağıtımı ve erişim politikaları gibi konuları kapsayan karmaşık bir alanı ifade eder. Bu alanda kararların alınması, politikaların şekillendirilmesi ve uygulanması, geniş bir perspektifi ve derin bir anlayışı gerektirir. İşte bu noktada, kuramsal/teorik çerçeve devreye girer. Kuramsal çerçeve, küresel internet yönetişimiyle ilgili karşılaşılan sorunları anlama, analiz etme ve çözüm yolları üretme süreçlerinde kritik bir role sahiptir.

Küresel yönetişim üzerine yapılan araştırmalar, Soğuk Savaş'ın bitimiyle büyük bir çeşitliliğe sahne olmuştur. Uİ disiplininde, küresel yönetişimi açıklama girişiminde birçok teorik yaklaşım bulunmaktadır; bunlar arasında Realizm, Konstrüktivizm, Liberalizm ve Eleştirel Teori gibi teoriler öne çıkmaktadır (Schofield, 2019, s. 3). Uİ akademisyenleri, değişimi incelemek istediklerinde, sıklıkla Robert Gilpin'in (1981) "belirli bir sistem içindeki değişiklikler" ya da başka bir deyişle, kurumsal yapıdaki değişimleri tanımladığı sistemik değişikliklere odaklanırlar. Ancak sistem değişikliği, daha derin bir anlam taşır; bu, temel aktörler ve ilkelerde meydana gelen bir değişikliği ifade eder. Böyle bir değişimin bileşeni olarak küresel internet yönetişimi, internet araştırmalarında yeni teorilerin denenmesi için kritik bir alan olarak öne çıkmaktadır. Bu alan, devlet ve özel sektörün evrilen rolleri, büyük güçler arasındaki güvenlik dinamikleri ve küresel ekonomik ile kültürel entegrasyonun boyutları gibi geleneksel konuları barındırır (van Eeten & Mueller, 2013, ss. 1-2). Bu bağlamda, internet yönetişimi, Uİ teorileri açısından zengin bir inceleme sahası sunar, zira bu alanda devletlerin, uluslararası kuruluşların, özel sektörün ve sivil toplumun etkileşimleri, güç dengeleri ve işbirliği mekanizmaları açıkça gözlemlenebilir. Bu etkileşimler, Uİ'nin temel kavramlarını ve teorilerini, özellikle devlet egemenliği, güç dengesi ve küreselleşme süreçlerini yeniden değerlendirme fırsatı sunar.

Reardon ve Choucri (2012), siber uzay üzerine yapılmış çalışmaları teorik olarak sınıflandırdıkları bir çalışma yapmışlardır. Yapılan çalışmaları realizm, liberalizm, inşacılık ve hiçbir teoriyi benimsemeyen olmak üzere dört kategoride sınıflandırdıkları çalışmada, siber politika literatüründe konstrüktivizmin hâkim olduğunu ortaya koymuşlardır. Bu analizde yönetişimi ele alan üç ayrı çalışmaya değinmişlerdir: Realizm açısından, Drezner'in (2004) çalışması, devletlerin siber uzayın küresel yönetişiminde nasıl etkin roller üstlendiklerini ve bu süreçte devletlerin kendi çıkarlarını nasıl koruyup ilerletmeye çalıştıklarını ele almaktadır. Liberal perspektifi temsil eden Newman (2008), siber uzayın yönetişiminde transatlantik sivil haklar ve

kurumsal iş birliklerinin önemini vurgulayarak, çok paydaşlılığın ve bireysel hakların nasıl genişletildiğini analiz etmektedir. Konstrüktivist bakış açısından ise, Farrell (2003), e-ticaretin uluslararası temellerini inşa etme sürecinde normların ve anlaşmaların rolünü incelerken, devletlerarası iş birliklerinin yanı sıra sosyal ve kültürel yapıların bu süreçteki etkinliğini gözler önüne sermektedir.

Uİ'deki bu teorik çerçeveler, küresel yönetişimin ve uluslararası işbirliğinin nasıl şekillendirileceği konusunda farklı yaklaşımlar sunar. Liberal iyimserliğin zorluklarla karşılaşmasına rağmen, küresel yönetişim düzenlemelerinin bazılarının gerilemesiyle paralel olarak diğerlerinin derinleştiğini kabul etmek, uluslararası sistemin karmaşıklığını ve dinamizmini daha iyi anlamamıza yardımcı olur. Bu tartışmalar, Uİ teorisinin ve pratiğinin sürekli evrim geçirdiğini ve küresel sorunlara yanıt olarak farklı teorik yaklaşımların değerinin olduğunu göstermektedir.

Bu çalışma açısından kuramsal çerçeve; yukarıda sayılan tüm gerekçelere ek olarak; politika yapıcılar, araştırmacılar ve pratik uygulayıcılar için, internetin nasıl yönetilmesi gerektiğine dair kapsamlı bir bakış açısı sunması gerekçesiyle önem arz etmektedir. Bu çalışmada kuramsal çerçevenin görevi, internet yönetişiminin mevcut ve potansiyel sorunlarını ele alırken, sürdürülebilir, adil ve kapsayıcı yönetişim modelleri geliştirmek için gerekli olan normatif temelleri sağlamaktır. Bu bağlamda, çalışmanın en önemli savı olan çok paydaşlılık, adil ve eşit internet erişimi ve sağlam bir hukuki çerçevenin oluşturulması gibi konuları destekleyen normatif teori, kuramsal çerçevenin temelini oluşturmaktadır.

Bu çalışma, Uİ disiplini içerisinde sıklıkla ihmal edilen normatif teorinin, küresel internet yönetişimi sorunlarına "en iyi" rehberliği sunacak teori olduğunu öne sürer. Normatif teori, internet yönetişimi alanında etik ilkelerin ve değerlerin ön plana çıkarılmasını savunmaktadır. Bu teori, çok paydaşlı yaklaşımların gerekliliğini, internetin herkes için adil ve eşit bir şekilde erişilebilir olmasının önemini ve güçlü bir hukuki çerçevenin varlığını vurgular. Normatif teori, internet yönetişiminin sadece teknik bir mesele olmadığını, aynı zamanda sosyal adalet, eşitlik ve insan hakları gibi temel değerleri içerdiğini öne sürer. Bu yaklaşım, internetin küresel bir kamu malı olarak görülmesini ve bu nedenle yönetişiminin, tüm paydaşların katılımıyla ve geniş bir etik perspektiften ele alınmasını gerektirir.

Aşağıda, Normatif yaklaşımların yanı sıra, Realizm, Liberalizm ve Konstrüktivizm gibi diğer uluslararası ilişkiler teorilerine de yer verilecek, bu teorilerin küresel internet yönetişimi üzerindeki etkileri ve önemleri detaylı bir şekilde incelenecektir. Bu teorik çerçevelerin küresel internet yönetişimi üzerine yapılan tartışmalara nasıl ışık tuttuğu ve bu alanın gelecekteki gelişimini nasıl şekillendirebileceği üzerinde durulacaktır.

1.3.1. Realizm: Güç, Güvenlik ve Çıkar Odaklı Dijital Yönetişim

Uİ tarihinde devletlerin iç ve dış politikalarını şekillendiren temel ideolojiler ve teoriler, zaman içinde evrimleşmiş ve çeşitlenmiştir. Bu teorilerden biri olan realizm, uluslararası ilişkilerde devletlerin davranışlarını anlamak için güç ve çıkar kavramlarını merkeze alır. Realizm, devletlerin egemenliklerini koruma ve ulusal çıkarlarını maksimize etme eğiliminde olduklarını öne sürer. Bu çerçevede, Thomas Hobbes'un mutlak egemenlik anlayışından Hegel'in uluslararası hukuk görüşlerine, internet yönetişimi üzerine yapılan realist çalışmalardan günümüzün küresel yönetişim tartışmalarına kadar uzanan geniş bir spektrumda, devlet merkezli bir perspektif hakimdir. Bu perspektif, uluslararası sistemdeki anarşi kavramı ve güvenlik ikilemi gibi kavramlarla desteklenirken, aynı zamanda devlet dışı aktörlerin ve küresel sorunlara yönelik işbirliğinin önemini ve zorunluluğunu da tartışmaya açar (Tarhan, 2016, s. 15).

Westphalian devlet egemenliği anlayışı, küresel siber yönetişimde ulus-devletlere merkezi bir rol verir. Bu yaklaşım, internetin küresel bir alan olduğunu kabul etse de, ulusal devletlerin internet üzerinde egemenlik yetkisini koruması gerektiğini savunur. Bu, internetin nasıl yönetileceğine dair önemli bir tartışma başlatır ve farklı aktörler arasında güç dengesini etkiler. Bu yaklaşım, realist teoriye benzer şekilde, küresel siber alanın yönetişimi konusunda devlet merkezli bir perspektife işaret eder. Bu yaklaşım, devletin internet üzerindeki egemenliğini ve kontrolünü vurgularken, çok paydaşlı işbirliğinin ve diğer paydaşların seslerinin önemini ikinci plana atar (Budnitskiy, 2018, s. 87).

Küresel internet yönetişimi üzerine yapılan realist çalışmalar, devletlerin bu alandaki merkezi rolünü vurgulamakta ve internetin düzenlenmesinde ulusal yargı alanlarının önemini öne çıkarmaktadır. Bu nedenle internetin ilk zamanlarındaki özgürlükçü vizyon, Goldsmith (1998) gibi siber realistler tarafından eleştirilmiştir. Goldsmith, siber uzayın gerçek dünya ile olan bağlantısını ve yasal düzenlemelere açık olduğunu savunarak, siber uzayın ayrı bir alan olarak görülmesinin yanılsamalarını vurgulamıştır.

Lessig ise (2006), internetin sosyal normlar, piyasa dinamikleri ve kod mimarisi gibi çeşitli düzenleme biçimleri aracılığıyla etkin bir şekilde düzenlenebileceğini savunarak, siber özgürlükçülerin argümanlarını sorgulamışlardır. Bu düşünürler, internetin yalnızca bölgesel devletlerin müdahalesiyle etkili bir şekilde çalışabileceği ve bu tür bir kontrolün demokratik devletler tarafından sağlanabileceği görüşünü desteklemişlerdir (Watt, 2017, ss. 85-86). Bu çalışmalar, internetin küresel bir fenomen olmasına rağmen, yönetişim yapısının bölgesel karakterini koruduğunu ve uluslararası düzenlemelerin devletler arasında müzakere edildiğini belirtmektedir. ABD hükümetinin ICANN üzerinde uyguladığı kontrol, realistler tarafından önemli bir odak noktası olarak görülmektedir (Chenou & Radu, 2015, s. 38).

1970'lerin sonlarında Kenneth Waltz tarafından geliştirilen Neo-Realizm, küresel yönetişim konusunda karamsar bir perspektif sunar ve uluslararası sistemde iki veya tek bir devletin hakimiyeti gibi durumları analiz eder. Waltz'un şemasında sistemin yönetişimi için tek bir araç vardır: güç dengesi (Holsti, 1992, s. 32). Soğuk Savaş sonrası dönemde ABD'nin üstünlüğü, uluslararası sistemi tek kutuplu olarak tanımlama eğilimini güçlendirmiştir. Bu noktada neo-realizm, güvenlik konusunda neo-liberalizmden daha güçlü bir açıklama sunar. Neo-liberalizm, barış ve işbirliği vurgusuna rağmen, uluslararası politikanın daha çatışmacı ve rekabetçi yönlerini açıklamada yetersiz kalmıştır (Schofield, 2019, s. 5).

İnternetin tarihine bakıldığında, ABD'nin internet üzerindeki etkisi inkâr edilemez bir gerçektir. ABD şirketleri, çekirdek ağ teknolojilerinin kontrolünü elinde tutmuş, önemli çok uluslu internet kurumları ABD'de kayıtlı olmuş ve ABD şirketleri ile ABD hükümeti, küresel internet yönetişim sistemine uzun süre hâkim olmuştur. Bu hakimiyet, internetin yapısı ve yönetişiminin temelinde yatan konsensüs ve güç dengesi prensipleriyle birleştiğinde, internetin küresel bir kaynak olarak işleyişi ve yönetişimi için bir düzenin varlığını zorunlu kılmıştır. Özellikle, güç dengesi, internet yönetişimindeki düzenin oluşmasında itici bir güç haline gelmiştir. Bu durum, internetin küresel doğasının, tek bir ülkenin veya bir grup ülkenin egemenliği altında olamayacağını ve tüm ulusların çıkarlarını dikkate alması gerektiğini vurgulamaktadır. Çin gibi ülkeler, küresel internet yönetişim sistemine resmi olarak dahil olduklarında, yerel yönetimlerin internetin küresel yönetişimiyle nasıl bütünleşeceği ve diğer uluslararası topluluklarla işbirliğini nasıl güçlendireceği önemli bir mesele haline gelmiştir (Zhang vd., 2020, s. 2309).

Neo-realizme göre devletlerin çıkarları, uluslararası kurumlarla etkileşime girildiğinde yok olmaz ya da dağılmaz, sadece değişik şekiller alır. Bu teoriye göre devletler, uluslararası örgütlerle etkileşime girdiğinde bile, özünde bencil ve güç odaklıdırlar. Bu yaklaşıma göre devletlerin işbirliğine yönelik iki önemli engeli vardır: Birincisi, işbirliğinden elde edilecek olası kazançların adil bir şekilde paylaşılmayacağı ve daha çok başkalarına yarayacağı endişesi söz konusudur. Mutlak kazançların büyük olasılığı bile işbirliğini engelleyebilir, çünkü devletler, diğerlerinin artan güçlerini nasıl kullanacaklarından çekinirler. İkincisi, devletler, işbirliğinin daha fazla kırılganlığa yol açabileceği korkusuyla temkinli davranırlar. Bir ülke, ne kadar çok uluslararası iş bölümüyle bütünleşirse ve uzmanlaşma yoluyla ne kadar çok kazanç sağlarsa, o kadar savunmasız hale gelir (Cornett & Caporaso, 1992, ss. 229-230).

Siber alandaki işbirliğinde de benzer bir görünüm mevcuttur. Devletler, veri akışı ve gizlilik konularında uluslararası standartların oluşturulması için birlikte çalışmanın önemini kabul etmekle birlikte, veri paylaşımı konusunda birbirlerine karşı derin bir güvensizlik beslemektedirler. Bu güvensizlik, ulusal güvenlik ve egemenlik kaygılarından kaynaklanmaktadır. Örneğin ABD, AB'nin katı veri koruma yönetmeliklerini Amerikan şirketlerine karşı bir rekabet dezavantajı olarak eleştirmiştir. Bu durum, devletlerin kendi çıkarlarını koruma eğiliminde olduklarını ve işbirliği yaparken bile kendi ulusal çıkarlarını ön planda tuttuklarını göstermektedir. Aynı zamanda, siber güvenlik alanında işbirliği, siber saldırılara karşı kolektif bir savunma mekanizması oluşturma potansiyeline sahipken, devletlerin siber saldırıların kaynağını belirleme ve sorumluları üzerinde anlaşmaya varma konusundaki zorlukları, bu işbirliğini karmaşıklaştırmaktadır. Özellikle devletler, siber güvenlik alanındaki işbirliğinin kendi siber istihbarat toplama ve saldırı kapasitelerini kısıtlayabileceğinden endişe duymakta, Rusya ve Çin gibi ülkeler ABD'nin siber güvenlik çabalarını kendi internet egemenliklerine yönelik bir tehdit olarak algılamaktadır. Bu durum, uluslararası işbirliğinin karmaşıklığını ve devletlerin kendi güvenliklerini nasıl algıladıklarının önemini vurgulamaktadır.

Hirshleifer'in anarşi kavramı üzerine yaptığı analiz, ekonomik ve sosyal sistemlerin nasıl işlediğine dair derinlemesine bir bakış sunar. Anarşi, genellikle düzensizlik ve kaos ile özdeşleştirilse de, Hirshleifer'e göre kendiliğinden oluşan bir düzenin var olabileceğini ve bu düzenin belirli koşullar altında sürdürülebilir olabileceğini belirtir (1995, s. 26). Bu çerçeve, küresel internet yönetişimine uyarlandığında, internetin açık

ve merkezi olmayan yapısının nasıl işlediğini ve potansiyel zorlukları anlamak için faydalı bir metafor sağlayabilir. Küresel internet yönetişiminde "anarşi", devletler, şirketler, sivil toplum kuruluşları ve bireyler gibi çeşitli aktörlerin merkezi bir otorite olmaksızın etkileşime girdiği ve kaynakları (bilgi, bant genişliği, teknoloji) ele geçirdiği ve savunduğu bir sistem olarak görülebilir. Bu aktörler, kaynakları üretken bir şekilde kullanmak ve bu kaynakları korumak veya genişletmek için rekabet ederken, işbirliği ve çatışma arasında bir denge kurarlar. Ancak uluslararası sistemdeki anarşi, devletlerin ortak çıkarlarını gerçekleştirmelerini zorlaştıran bir güvenlik ikilemi yaratmaktadır. Bir devletin güvenliğini artıran politikalar diğerleri için tehdit olarak algılanabilir ve bu da karşılıklı güvensizlik ve silahlanma yarışı gibi istenmeyen sonuçlara yol açabilir (Jervis, 1978).

Realizm, özellikle güvenlik ikilemi kavramıyla, devletlerin güvenliklerini maksimize etme çabası içinde olduklarını ve bu süreçte diğer devletlerle rekabet halinde olduklarını öne sürer. Güvenlik ikilemi, bir devletin güvenliğini artırmaya yönelik herhangi bir adımının, diğer devletleri tehdit olarak algılamalarına ve karşılık olarak kendi güvenlik önlemlerini artırmalarına neden olabileceği bir durumu ifade eder. Senges ve Horner, bir devletin, ISS'lerin rakip iletişim şirketlerinin içeriğini engelleme politikası gibi karmaşık konuları ele alırken çeşitli ilkeleri dikkate alması gerektiğini vurgular. Bu ilkeler, ulusal mevzuat, düzenleyici prensipler ve uluslararası yönergeleri içerebilir. Ayrıca, politika yapıcıların bireysel değerleri de bu süreçte etkili olabilir. Genel ilkeler, özel bir konuya uygulanmak üzere politika ilkelerine dönüştürülmelidir. Örneğin; ağların tarafsız olması ve içerik engellemeye izin verilmemesi gibi (2009, s. 15). Realizmin güvenlik ikilemiyle ilgili olarak, internet yönetişimindeki bu tür düzenlemeler, uluslararası bir güvenlik ikilemi oluşturabilir. Bir ülkenin internet üzerindeki kontrolünü artırması, diğer ülkelerin benzer veya daha sıkı önlemler almasına, uluslararası internet yönetişimi alanında rekabetin ve gerilimin artmasına neden olabilir. Bu durum, ağların tarafsızlığı ve içerik engellemeye karşı olan genel ilkelerle çatışır ve internetin küresel doğasını koruma çabalarını zorlaştırır.

Jervis (1978) dört güvenlik biçiminden bahseder. İlki, hem sömürme cazibesi yüksek hem de savunma zor olduğunda, devletlerin rekabet etmeye ve silahlanmaya meyilli oldukları rekabetçi güvenliktir. Bu durum, uluslararası sistemde gerginlik ve çatışma riskini artırır. İkincisi, bir devletin diğerlerinden önemli ölçüde daha güçlü olduğu durumda, hegemonik istikrarın hâkim olduğu hegemonik güvenliktir. Güçlü devlet,

diğer devletler üzerinde caydırıcılık sağlayarak barışı ve düzeni korur. Üçüncüsü, sömürme cazibesi düşük ve savunma kolay olduğunda, devletlerin işbirliğine ve ortak çıkarlarını geliştirmeye meyilli oldukları işbirlikçi güvenliktir. Bu durum, uluslararası ticaret ve yatırım gibi alanlarda işbirliğine yol açar. Dördüncüsü ise, farklı devletlerin farklı stratejiler izlediği ve istikrarsız bir güç dengesinin hâkim olduğu karmaşık güvenliktir. Bu durum, öngörülemezliği ve belirsizliği artırır.

Karmaşık güvenlik, küresel internet yönetişiminin mevcut durumunu en iyi yansıtan modeldir. Çeşitli aktörlerin farklı ve bazen çelişen çıkarları ve stratejileri, yönetişim süreçlerinde öngörülemezliği ve belirsizliği artırır. Bu durum, işbirliğini ve uzlaşmayı zorlaştırırken, aynı zamanda dinamik ve esnek yönetişim yapılarının geliştirilmesi için fırsatlar sunar. Karmaşık bir güvenlik dünyasında, çok katmanlı ve esnek bir yönetişim modeli, değişen ihtiyaçlara ve tehditlere hızlı bir şekilde yanıt verebilir.

Hirshleifer'in "kararlılık parametresi" düşüncesi, internet üzerindeki kontrol ve yönetişimin sürdürülebilirliğine dair önemli bir içgörü sunar. Bu, mücadele çabalarının getirisi azaldığında, yani aktörler arasındaki rekabetin maliyeti gelirlerinden daha az olduğunda anarşinin sürdürülebilir olduğunu öne sürer (1995, s. 43). Siber alanda bu, siber güvenlik tehditlerine karşı koymak için işbirliğinin artırılması ve bilgi akışının serbestçe sürdürülmesi gibi koşullar altında gerçekleşebilir. Ancak, Hirshleifer'in de belirttiği gibi anarşi kırılgandır veya şekilsiz bir "amorfi"ye dönüşebilir ya da daha organize bir hiyerarşiye evrilebilir. İnternet yönetişiminde bu, düzenin çok fazla merkezi olmayan ve kontrolsüz kaldığında kaotik bir duruma dönüşebileceği veya aşırı düzenlemeler ve sıkı kontrol mekanizmaları ile daha merkeziyetçi bir yapıya evrilebileceği anlamına gelir. Bu dengenin sağlanması, küresel internetin sağlıklı bir şekilde işlemesi ve gelişmesi için kritik öneme sahiptir.

İnternet, insan yapımı bir yapı olarak, dış etkenlerden daha az etkilenme eğilimindedir. Bu durum, kuruluşların internet politikalarını belirlerken daha fazla esneklik sunar. Dolayısıyla internetin teknik özelliklerinin, kurumsal sınırların ötesindeki düzenlemelerin oluşumunu teşvik ettiği söylenebilir. Devletlerin internet politikaları oluştururken ulusal mevzuat, düzenleyici prensipler, uluslararası yönergeler ve bireysel değerler gibi çeşitli ilkeleri dikkate alması, güvenlik ve özgürlük arasında dengeli bir yaklaşım gerektirir. Bu noktada Rose'un neoklasik realizm yaklaşımı, uluslararası ilişkilerde bir devletin dış politikasının, göreli maddi gücü tarafından temel olarak

yönlendirildiği ancak bu gücün dış politika üzerindeki etkisinin karar vericilerin algıları, devlet yapısı ve sistemik baskılar gibi birim düzeyindeki değişkenler aracılığıyla dolaylı ve karmaşık bir şekilde etkilendiğini savunur (1998, s. 152).

Küresel siber yönetişim bağlamında bakıldığında devletlerin internet altyapısına yaptıkları yatırımlar ve bu altyapıyı kontrol etme kapasiteleri, onların küresel internet yönetişimindeki göreli maddi güçlerini yansıtır. Karar vericilerin teknoloji ve siber alanın potansiyelleri ve tehditleri hakkındaki algıları, ulusal internet politikalarının ve uluslararası internet yönetişimine katılımın şekillendirilmesinde kritik bir rol oynar. Bu algılar, bir ülkenin siber savunma stratejilerini, dijital ekonomiye yatırım yapma kararlarını ve internet özgürlüğü ile ilgili politikalarını etkiler. İç politik yapılar ve devlet mekanizmaları, internet yönetişimi ve politika yapım sürecinde önemli bir role sahiptir. Demokratik sistemlerde, politika yapım süreci genellikle daha şeffaf ve çok taraflı iken, otoriter rejimlerde tek taraflı ve merkeziyetçi olabilir. Bu farklılıklar, internet sansürü, veri koruma politikaları ve uluslararası internet yönetişimiyle ilgili kararlarda belirginleşir. Dolayısıyla küresel internet yönetişimi, devletlerin uluslararası normlar ve anlaşmalar çerçevesinde hareket etmelerini gerektirir.

Realist yaklaşım, devlet dışı aktörlerin ve özel otoritenin internet yönetişimindeki artan rolünü yeterince kabul etmese de; piyasa liberalizasyonu ve minimal devlet müdahalesi, internetin gelişimini önemli ölçüde kolaylaştırmıştır (Chenou & Radu, 2015, s. 38). Özetle realizm, küresel yönetişim konusunda eleştirilere de maruz kalmaktadır. Bu teori, uluslararası ilişkilerin değişen doğasını ve özellikle de küresel çapta ortaya çıkan yeni tehdit ve fırsatları yeterince hesaba katmamakla eleştirilir.

Diğer yandan realizmin güvenlik ikilemine odaklanması, negatif anlamda siber güvenlik yaklaşımlarını ön plana çıkarırken, açık ve erişilebilir bir internetin temel gerekliliği olan iyi yönetişim unsurlarının göz ardı edilmesine sebebiyet verir. Bu, özellikle siber alanın düzenlenmesi ve yönetilmesinde, işbirliğine dayalı ve kapsayıcı yaklaşımların gerekliliğinin küçümsenmesine yol açar. Son olarak, realizmin siber egemenlik ve ulusal yargı yetkileri üzerine yoğunlaşması, internetin küresel doğasıyla çelişir. İnternetin sınırların ötesindeki yapısı, ulusal düzenlemelerin ötesinde, küresel normlar ve standartlar gerektirir. Bu durum, uluslararası düzenlemelerin ve kurumların önemini artırırken, realizmin bu dinamikleri yeterince ele alamadığını gösterir.

Sonuç olarak realizmin uluslararası ilişkiler ve küresel internet yönetişimi konusundaki yaklaşımı, güç ve çıkarların merkeziyetçiliğine dayanan ve devlet merkezli bir perspektifi temsil eden bir çerçevedir. Bu yaklaşım, uluslararası sistemin anlaşılmasında ve devletlerin dış politikalarının şekillendirilmesinde zaman zaman hakimiyet kurabilen bir teori olsa da, küresel internet yönetişimi alanında realizmin bu geleneksel çerçevesinin hakimiyeti sınırlıdır. Bu sınırlılığın temel nedeni, internetin çok paydaşlı yapısının, devlet merkezli yaklaşımların ötesine geçen bir yönetişim modeli gerektirmesidir. Küresel internet yönetişiminin doğası -realizmin devlet merkezli anlayışına zıt bir şekilde- çeşitli aktörlerin katılımını zorunlu kılar. Bu çok paydaşlı yapı, tek bir aktör grubunun internet üzerinde tam bir kontrol veya hakimiyet kurmasını zorlaştırır. Özellikle bazı devletlerin ve özel sektör aktörlerinin internet üzerinde daha fazla kontrol ve egemenlik kurma çabaları, internetin açık ve sınır tanımayan yapısı nedeniyle başarısızlıkla sonuçlanır. Bu durum, küresel internet yönetişiminde normatif unsurların ve değerlerin önemini artırır. Dolayısıyla realizm, uluslararası ilişkilerdeki devlet davranışlarını anlamak için güçlü bir çerçeve sunsa da, modern dünyanın karmaşıklığı ve sürekli değişen dinamikleri karşısında sınırlılıklara sahiptir. Bu nedenle, küresel yönetişim konusunda daha kapsamlı ve esnek teorilere ihtiyaç duyulmaktadır.

1.3.2. Liberalizm: Özgürlükçü Yaklaşımlar

Uİ disiplininde liberalizm, devletlerarası işbirliğini ve çok taraflı kurumların önemini vurgulayan önemli bir teorik yaklaşımdır. Liberalizmin uluslararası sistemdeki devlet-dışı aktörleri de analiz düzeyine dahil etmiş olması, küresel internet yönetişimi konusunda önemli bir perspektif sunmasına yardımcı olur. Bu anlamda liberalizmin özgürlükçü yaklaşımları, siber uzayın karmaşık yapısını ve çok boyutlu aktörler arası etkileşimleri anlamak için kritik öneme sahiptir. 1990'ların başında başlayan ve devletler, akademisyenler, sivil toplum kuruluşları ve özel sektör temsilcileri arasında yoğunlaşan internet yönetişimi tartışmaları, bu alandaki liberal yaklaşımların temellerini atmıştır. İnternetin özgürlükçü doğası, ulusal sınırların ötesinde, kendi kendini düzenleyebilen bir alan olarak görülmesini sağlamış ve bu da internetin "yeni aklın yuvası" olarak tanımlanmasına yol açmıştır (Watt, 2017, s. 84).

İnternet özgürlüğünün retoriği, bilginin küresel akışının, liberal-demokratik değerlerle—özellikle ifade, toplanma ve seçim özgürlüğüyle—özdeşleştiğini varsayar.

Bu, Westphalian devlet egemenliği kavramlarının ve kurumlarının internet yönetişimi için uygun olmadığı anlamına gelir. İnternet özgürlüğü, "özgür", "açık", "küresel" ve "sınırsız" gibi metaforlar kullanarak, internetin yönetişiminde devletlerin merkezi bir rol oynamasının, internetin ulusal çizgiler boyunca parçalanmasına yol açabileceği tehdidini vurgular (Budnitskiy, 2018, s. 89).

John Perry Barlow ve benzeri "iyimserler" tarafından yapılan açıklamalar, büyük ölçüde reddedilmiş olsa da, bu tür görüşleri yüzeysel bir şekilde değerlendirip yanlış anlamak, eleştirenlerin düştüğü bir hata olarak görülür. Barlow, siber suçlar ve spam gibi sorunlar var olduğu için ütopik bir hayalperest olarak etiketlenmektedir. Bu durum, 1960'larda dünya nükleer savaş tehdidi altında iken, barışçıl bir gelecek hayal eden John Lennon'a yapılan eleştirileri hatırlatmaktadır. Oysa ki insan hakları gibi kavramlar, ihlallerine rağmen önemini korumaya devam ettiği gibi, toplumun bu değerlere tam anlamıyla saygı göstermemesi, bu ideallerin geçerliliğini veya ahlaki önemini azaltmaz. Bu bağlamda Barlow ve diğer iyimserler, erken internet dönemini, güvenlik ve meşruiyet adına getirilen kısıtlamaların etkinliğini sorgulama ve yeniden değerlendirme fırsatı olarak değerlendirmişlerdir (Andjelkovic, 2006, s. 18).

İnternet özgürlüğü yaklaşımı, daha çok internetin ilk dönemlerini kapsayan liberal yaklaşımlara yönelik bir analiz sunmaktadır. İlk dönemlerin liberal yaklaşımları, genellikle sınırsız ifade özgürlüğü ve düzenleme yapmama prensipleri üzerine kuruluydu. Günümüzün liberal yaklaşımlarında ise internet, teknik bir platformdan çok daha fazlasını temsil ettiği için küresel politika, sosyal etkileşim, ekonomi ve hukukun kesiştiği bir alan haline gelmiştir. Ancak bu bakış açısı, internetin getirdiği riskleri ve zorlukları, özellikle de dezenformasyon, kişisel gizliliğin ihlali ve siber güvenlik sorunları gibi günümüz problemlerini göz ardı etmektedir. Bu nedenle günümüzün liberal yaklaşımları, bu yeni gerçeklikleri dikkate alarak evrimleşmeye çalışmaktadır.

Bugün özel sektör dahi, serbest piyasa ilkelerine sadık kalarak, siber alanda insan haklarının korunmasına önem vermektedir. Bu yaklaşım, ulusal pazarlara erişim engellerini azaltmak ve bilgi akışını serbestleştirmek gibi kendi çıkarlarına da hizmet eder. Google ve Facebook gibi küresel teknoloji devlerinin stratejileri, bu yaklaşımın açık bir göstergesidir. Diğer yandan, kâr amacı gütmeyen dijital haklar savunuculuk grupları, mali teşviklerden ziyade bireylerin dijital haklarını korumaya ve ifade özgürlüğünü genişletmeye odaklanır. Bu gruplar, devletleri ve büyük teknoloji

şirketlerini kullanıcı haklarını ihlal etmekle sıkça eleştirir. Ayrıca, internet özgürlüğüne bağlı bireyler ve kuruluşlar, liberal ve liberal olmayan devletlerin internet yönetişimini eleştirerek, liberal demokrasilerin ve Batı merkezli olmayan devletlerin politikalarına karşı çıkar (Budnitskiy, 2018, s. 90). Sonuç olarak, internet özgürlüğü sadece bir bireysel hak meselesi değil, aynı zamanda küresel siber yönetişimin de temel bir unsurudur.

Liberalist kurumsalcı yaklaşım, uluslararası hukukun ve uluslararası kuruluşların hala önemli ve etkili olduğunu savunur. Bu perspektife göre son yirmi yılda uluslararası kurumların değişmiş olabileceği kabul edilse de, bu kurumlar genel ilgi alanlarını ve etkinliklerini kaybetmemişlerdir. Paris İklim Anlaşması gibi yeni anlaşmaların imzalanması ve uluslararası finans otoritelerinin krizlere müdahalesi, uluslararası kurumların zayıflamadığını, aksine belirli alanlarda daha da güçlendiğini göstermektedir (Zürn, 2018b). Mueller (2010) ve Denardis (2014), internet yönetişiminin yalnızca devletler, pazarlar veya bireysel kuruluşlar aracılığıyla anlaşılamayacağını, daha ziyade içsel gerilimleri ve birlikte çalışabilirliğin ve açıklığın vurgulandığı bir paydaş ekosistemi olarak ele alınması gerektiğini belirtmişlerdir. Bu karmaşık paydaş ekosistemi, ulus devlet egemenliğini tehdit eden ve siyasi katılımı güçlendiren çok paydaşlılık kavramını içerir. Liberal teori, uluslararası işbirliği ve küresel kurumların güçlenmesini vurgularken, bu yeni yönetişim modeli, sivil toplumun, özel sektörün ve devletlerin bir arada çalışarak küresel internetin yönlendirilmesindeki rollerini kabul etmektedir. Öte yandan, DeNardis'in çalışmalarındaki ekosistemik yaklaşım, konstrüktivist teorinin izlerini taşımakta, teknolojinin sosyal ve politik yapılar üzerindeki etkisini ve toplumsal normların ve değerlerin teknolojik düzenlemeler üzerindeki rolünü ön plana çıkarmaktadır.

Liberal teori, uluslararası işbirliği ve kurumların rolünü vurgular. AB'nin ve önemli Avrupa güçlerinin kullanıcı haklarını koruma ve internet özgürlüğünün temel değerlerini muhafaza etme yönündeki talepleri, liberalizmin çok paydaşlı kurumlar aracılığıyla kolektif çıkarların teşvik edilmesine verdiği önemi yansıtır. Özellikle, Avrupa'nın devletler için daha büyük bir rol talebi ve organizasyonel değişikliklere açıklığı, liberalizmin normlar, kurallar ve kurumsal reformlar üzerinden uluslararası işbirliğini ve düzenlemeyi nasıl desteklediğinin bir göstergesidir. Bu iki yaklaşım, internet yönetişiminde bir güç mücadelesi ve normatif bir değerler çatışması olarak yorumlanabilir. ABD'nin mevcut düzeni koruma eğilimi ve Avrupa'nın daha reformist

tutumu, siber uzayın geleceği üzerinde etkili olabilecek uluslararası bir diyalogun başlangıcı olarak değerlendirilebilir. Bu durum, siber uzayın yönetişimindeki mevcut yapısal düzenlemelerin korunması ve evrimleşmesi arasındaki dinamik bir dengeyi temsil etmektedir (Budnitskiy, 2018, s. 92).

Özetle liberal teorinin temelinde, bireylerin ve grupların serbestçe hareket edebileceği, ifade özgürlüğü, bilgi akışının serbestliği ve çok taraflı kurumların önemli olduğu bir uluslararası sistem vizyonu yatar. Bu, liberalizmin özgürlükçü yaklaşımlara ve devlet-dışı aktörlerin analizine büyük önem vermesinin temel nedenidir. Bunun yanında, özgürlükçü yaklaşımlar ile düzenleyici mekanizmaların varlığı arasındaki dengeyi de ihmal etmez. Ancak bu özgürlükçü ve çok aktörlü yaklaşımın, internetin yönetişimi ve düzenlenmesi konusunda normatif ilkeleri göz ardı ettiği görülmektedir. Dolayısıyla liberal teorinin eleştirilebileceği noktalardan biri, siber uzayın doğası ve yönetişimi konusunda çok aktörlü ve özgürlükçü yaklaşımlar sunarken, bu normatif ilkelerin nasıl entegre edileceği veya korunacağı konusunda derinlemesine bir çerçeve sunmamasıdır. Örneğin, özgür ve açık bir internetin savunulması, bireysel mahremiyet ve veri koruma gibi normatif değerlerle nasıl dengeleneceği konusunda açık bir yol göstermez. Ayrıca, devletlerin ve büyük teknoloji şirketlerinin eylemleri karşısında bireylerin ve küçük grupların haklarını nasıl koruyacağı konusunda somut politika önerileri sunmaktan kaçınır. Bu, liberal teorinin, özgürlük ve işbirliğinin yanı sıra, siber uzayın yönetişiminde adalet, eşitlik ve bireysel haklar gibi normatif unsurları da entegre edecek şekilde genişletilmesi gerektiğini gösterir. Böylece, liberal teori, sadece neyin mümkün olduğunu değil, aynı zamanda neyin olması gerektiğini de kapsayacak şekilde daha kapsamlı bir çerçeve sunabilir.

1.3.3. İnşacılık: Dijital Yönetişim İnşa Edilebilir Mi?

İnternetin nasıl yönetileceği konusundaki tartışmalar, teknolojik gelişmelerin yanı sıra sosyal, politik ve kültürel dinamiklerle de iç içe geçmiştir. Bu bağlamda, Alexander Wendt'in sosyal inşacılık teorisi, Uİ alanında devletlerin birbirleriyle olan etkileşimlerini ve bu etkileşimlerin sosyal yapıları nasıl şekillendirdiğini inceleyerek önemli bir perspektif sunar. Wendt'in yaklaşımı, devletler arası ilişkilerin ve dolayısıyla uluslararası sistemin, yalnızca güç ve çıkarlar üzerine değil, aynı zamanda aktörler arası etkileşimlerle oluşan kimlikler ve normlar üzerine de inşa edildiğini öne sürer. Bu

teorik çerçeve, internet yönetişimi gibi karmaşık ve çok boyutlu bir alanı anlamak için de önemli bir çerçeve sunar.

Alexander Wendt'in sosyal inşacılık kuramı, uluslararası ilişkilerde devletlerin birbirleriyle olan etkileşimlerinin nasıl sürekli olarak kendilerini ve birbirlerini yeniden tanımlayabileceğini inceler. Wendt'in yaklaşımı, devletlerarası ilişkilerin sadece güç ve çıkarlar üzerine kurulu olmadığını, aynı zamanda sosyal yapılar ve aktörler arası etkileşimlerle şekillenen kimlikler ve normlar üzerine de inşa edildiğini savunur. Bu perspektif, küresel internet yönetişimine uygulandığında, devletler ve diğer aktörlerin internet politikaları ve uygulamaları aracılığıyla nasıl birbirleriyle etkileşime girdiklerini ve bu sürecin internetin sosyal yapısını nasıl şekillendirdiğini anlamamıza yardımcı olabilir.

Alexander Wendt'in (1992) *Anarşi, Devletlerin Yaptığı Şeydir: Güç Politikasının Sosyal İnşası* adlı eserinde kurumlar, kimlikleri ve çıkarları bir araya getiren yapılar olarak tanımlanır. Bu yapılar, aktörlerin sosyalleşmesini ve kolektif bilgiye katılımını sağlayarak karşılıklı anlaşılmayı ve işbirliğini teşvik eder. Wendt'in kurumlar ve kimlik inşası hakkındaki teorisi, internet yönetişimi için önemli bir çerçeve sunmaktadır. Bu çerçeve, internetin tüm kullanıcılar için faydalı bir platform olarak gelişmesini ve korunmasını sağlamak için gerekli olan diyalog ve işbirliğini teşvik etmeye yardımcı olabilir. Wendt'e göre, eylemler ve kimliklerin oluşumu sürekli bir süreçtir ve yalnızca aktörlerin uygulamaları nedeniyle var olur ve gelişir (1999, s. 36). Bu bağlamda küresel internet yönetişimi, devletlerin ve diğer aktörlerin birbirleriyle olan etkileşimlerinin, internetin sosyal yapısını ve bu yapının nasıl geliştiğini şekillendirdiği bir alan olarak görülebilir.

Küresel internet yönetişiminde devletler ve diğer aktörler arasındaki etkileşimler, Wendt'in "Ego" ve "Alter"[27] kavramlarıyla benzer şekilde, karşılıklı roller ve beklentiler aracılığıyla şekillenir (Copeland, 2000, s. 193). Örneğin, bir devletin internet üzerinde sıkı kontrol politikaları uygulaması, diğer devletler tarafından

[27] Alexander Wendt'in inşacılık teorisinde "Alter" ve "Ego", devletlerarası etkileşimleri anlamak için kullanılan temel kavramlardır. "Ego", bir devletin kendisi hakkındaki algısı ve kimliğini ifade ederken, "Alter" diğer devletleri ve aktörleri temsil eder. Ego, bir devletin kendisi veya "ben" anlayışını ifade eder. Ego, kendi kimliğini, çıkarlarını ve davranışlarını nasıl algıladığı ile ilgilidir. Alter ise, "diğer" veya başka bir devleti temsil eder. Ego'nun perspektifinden Alter, dış dünyada, yani diğer devletlerde, uluslararası kuruluşlarda veya aktörlerde bir "öteki" olarak algılanır. Ego'nun Alter ile olan etkileşimi, Ego'nun kendi kimliğini, çıkarlarını ve davranışlarını nasıl anladığı ve uyarladığı üzerinde önemli etkilere sahiptir.

güvensizlik ve rekabetçi bir tutum olarak algılanabilir, bu da karşılıklı egoist ve militarist benlik anlayışlarının yeniden üretilmesine yol açabilir. Ancak aynı zamanda, internetin açık ve özgür bir alan olarak korunmasını teşvik eden uluslararası iş birlikleri ve normlar, devletlerin ve diğer aktörlerin birbirlerine karşı daha işbirlikçi ve diğerlerini dikkate alan bir tutum benimsemelerine yol açabilir. Nihayetinde bu durum, paylaşılan düşünce yapısının daha kolektif ve ötekiyle ilgili bir yapıya dönüşmesine neden olabilir.

Siyasi otoritenin bir yapısı olarak anlaşılan devlet, "çatışmanın ele alındığı, toplumun yönetildiği ve sosyal ilişkilerin yönetildiği" normlar, kurallar ve ilkeler tarafından oluşturulur (Wendt, 1999, s. 202). İnternet, uluslararası bir alan olarak çatışmaların yönetilmesi, toplumların düzenlenmesi ve sosyal ilişkilerin yönlendirilmesi için benzer bir normatif yapıya ihtiyaç duyar. Bu yapı, farklı ülkelerin devletleri, uluslararası kuruluşlar, çokuluslu şirketler, sivil toplum kuruluşları ve bireyler gibi çeşitli aktörler arasında işbirliğini ve koordinasyonu sağlamak üzere tasarlanmıştır. Küresel internet yönetişiminde normlar ve kurallar, online gizlilik, veri koruma, siber güvenlik, içerik yönetişimi ve internet erişimi gibi konularda rehberlik eder.

Bu çok paydaşlı ve çok boyutlu yönetişim anlayışı, hem devletler hem de çok sayıda uluslararası aktörün etkileşimlerine dayanan bir düzeni temsil etmektedir. Gelişmekte olan bu düzen, siber uzayın yönetişiminin geleneksel ulusal sınırların ötesine geçen bir fenomen olduğunu ve artık küresel diyalogların ve anlaşmaların ürünü olduğunu göstermektedir. Ağın küreselleşmesi, ulus devletlerin egemenlik iddiaları ile bireysel hakların ve toplulukların çıkarlarını koruma arayışları arasında karmaşık bir gerilim yaratmaktadır. Bu yeni yönetişim modeli, teknik bir güç mücadelesinden ziyade, insanların ne yaptığına, ne söylediğine ve nasıl bir toplumsal yapı inşa ettiklerine dair dinamik ve bireysel düzeyde toplanan verileri içeren bir yapıya evrilmiştir (Couldry & Powell, 2014, s. 1).

Deibert, iletişim ortamlarını doğal ortamlara benzetmektedir. Doğal ortamlar, belirli türlerin üremesini ve hayatta kalmasını kolaylaştırırken, diğer türlerin üremesini ve hayatta kalmasını zorlaştırır. İletişim ortamları da benzer şekilde, belirli sosyal güçlerin ve fikirlerin üremesini ve hayatta kalmasını kolaylaştırırken, diğerlerinin üremesini ve hayatta kalmasını zorlaştırır (2002, s. 117). Bu bağlamda internet de, çeşitli sosyal güçlerin, fikirlerin ve kültürlerin bir araya geldiği, interaktif ve dinamik bir ekosistem

olarak düşünülebilir. Bu dijital ortam, bazı sosyal güçlerin ve fikirlerin gelişimini kolaylaştırırken, diğerlerini sınırlandırabilir veya bastırabilir. Bu anlamda küresel internet yönetişimi, internetin doğal bir ortam olarak işlev görmesini sağlayan kurallar, politikalar ve standartlar bütünü olarak hareket eder. Bu yönetişim, çeşitli aktörlerin etkileşimiyle şekillenir.

Alexander Wendt'in sosyal inşacılık teorisi, uluslararası ilişkilerin sosyal yapılar ve aktörler arası etkileşimlerle nasıl şekillendirildiğini vurgulayarak, internet yönetişimi gibi karmaşık alanları anlamak için değerli bir çerçeve sunmaktadır. Bu teorik yaklaşım, devletler ve diğer aktörlerin internet üzerindeki politikaları ve uygulamaları aracılığıyla birbirleriyle nasıl etkileşime girdiğini ve bu sürecin internetin sosyal yapısını nasıl şekillendirdiğini daha iyi kavramamızı sağlar. İnşacılığın, internet yönetişimindeki sosyal, politik ve kültürel dinamikleri tanıması ve bunların teknolojik gelişmelerle nasıl iç içe geçtiğini vurgulaması, bu teorik çerçevenin en güçlü yanlarından biridir. Bu yaklaşım, internetin sadece teknik bir altyapı olmadığını, aynı zamanda toplumsal değerler, kültürel normlar ve bireylerin eylemleri arasındaki etkileşimlerin bir sonucu olarak şekillendiğini gösterir.

Ancak inşacılık, sosyal yapılar ve aktörler arası etkileşimlere odaklanırken, teknolojik determinizmin rolünü göz ardı edebilir. İnternet teknolojilerinin kendine has özellikleri ve bu teknolojilerin toplumsal yapılar üzerindeki etkileri, inşacılık teorisi içinde yeterince ele alınmaz. Dolayısıyla inşacılık, internet yönetişiminin anlaşılmasında değerli bir çerçeve sunarken, uygulanabilirlik ve teknolojik faktörlerin yeterince dikkate alınmaması gibi zorlukları da beraberinde getirir. Bu durum, inşacılık teorisinin internet yönetişimi üzerine uygulanışının, gerçek dünya pratikleri ve çatışmalarıyla nasıl uyum sağlayabileceği üzerine daha fazla düşünülmesi gerektiğini gösterir.

1.3.4. Eleştirel Bir Teori: Normatif Teori

Normatif teori, uluslararası ilişkilerin ahlaki boyutunu ve daha geniş olarak Uİ disiplininin ürettiği anlam ve yorumları inceleyen bir çalışma alanıdır (Brown, 1992, s. 3). Normatif teori, etik ilkeleri, ahlaki yükümlülükleri ve uluslararası ilişkilerde adalet arayışını vurgulayarak küresel yönetişim tartışmalarına önemli katkılarda bulunmaktadır. Normatif teori, küresel yönetişim kavramını değerlendirirken, etik ilkeler, adalet, eşitlik ve katılımcılık gibi değerleri merkeze alırken; küresel yönetişimin yalnızca etkili ve verimli karar alma ve problem çözme süreçlerinden ibaret olmadığını,

aynı zamanda bu süreçlerin demokratik meşruiyetle desteklenmesi gerektiğini savunur. Küresel yönetişimde normatif ilkelerin rolü, çeşitli çalışmalarda incelenmiştir.

Teorinin kökenleri klasik siyasal felsefeye kadar uzanmaktadır. Platon ve Aristoteles gibi antik Yunan filozofları, adalet, siyasetin amacı ve iyi bir toplumun nasıl olması gerektiği gibi konularda düşünceleriyle normatif teorinin temelini oluşturmuşlardır. Ortaçağ'da Aziz Augustine ve Thomas Aquinas gibi filozoflar, doğal hukuk ve ilahiyat kavramlarını kullanarak normatif teorinin gelişimine katkıda bulunmuşlardır. Aydınlanma döneminde Hobbes, Locke ve Rousseau gibi filozoflar, toplumsal sözleşme ve doğal haklar gibi kavramlar üzerinden normatif teoriyi geliştirmişlerdir. Immanuel Kant ve John Stuart Mill gibi modern filozoflar ise ahlak, özgürlük ve adalet gibi kavramlar üzerine yaptıkları çalışmalarla normatif teorinin temelini sağlamlaştırmışlardır.

Normatif teori, uluslararası politikanın etik, moral ve normatif temellerine odaklanan bir alan olarak, ahlak felsefesi, siyaset teorisi ve genel Uİ disiplininden beslenir. Bu teori, etik değerlendirmelerin temelini, ahlaki ilkelerin kaynaklarını ve bu ilkelerin küresel siyaset bağlamında nasıl değerlendirilip gözden geçirileceğini inceler. Bu alanın gelişimi, 1980'ler ve 1990'lar boyunca Hoffmann, Linklater, Nardin, Frost ve Brown gibi isimlerin öncülük ettiği çalışmalarla belirginleşmiştir. Uluslararası Çalışmalar Derneği içinde Uluslararası Etik Bölümü'nün kurulması, normatif sorgulamaların Uİ teorisinde önemli bir yere sahip olduğunun bir işaretidir. Gelişim sürecinde, uluslararası düzeyde ahlaki beklentileri, kararları ve dilemmaları keşfetmeyi amaçlayan çeşitli bakış açıları, bu alana dahil olmuştur. Siyaset teorisi, adalet, görev ve haklar gibi kavramları içerirken, ahlak felsefesi deontoloji ve sonuçsalcılık gibi yaklaşımları sunar. Bu temel kavramlar, komüniteryanizm ve kozmopolitanizm gibi siyaset teorisi kategorileri aracılığıyla uluslararası ve küresel seviyelere taşınmıştır (Dunne & Kurki & Smith, 2013).

Normatif Uİ teorisi, uluslararası ilişkilerin etik boyutlarına odaklanarak, ahlaki soruları ve küresel politikada ahlaki normların ve değerlerin rolünü derinlemesine inceler. Bu yaklaşım, devletler, ulusötesi şirketler ve uluslararası örgütler gibi uluslararası sistemde faaliyet gösteren çeşitli aktörlerin, ahlaki sorumlulukları ve etik davranışlarını merkeze alır. Bu teori, normatif teorinin iç çeşitliliğini ve genel Uİ disipliniyle olan bağlantısını kabul ederek, küresel zorlukların anlaşılması ve çözümünde etik meselelerin önemini

vurgular. Etik ilkelerin uluslararası politikada nasıl şekil aldığını ortaya koyarak, daha adil ve sorumlu bir küresel düzenin oluşturulmasına katkıda bulunmayı amaçlar.

Siber alanın yönetilmesi, normatif teori açısından, internetin açık, özgür ve güvenli bir şekilde kullanımını destekleyen yönetişim modellerini ve politikalarını geliştirmeyi gerektirir. Bu süreç, siber etiğin, hukukun ve politikanın entegrasyonunu içerir ve siber alanın yönetilmesinin sadece teknik bir mesele olmadığını, aynı zamanda etik, sosyal ve politik boyutları da olduğunu vurgular. Öyle ki, küresel internet yönetişiminin normatif anlatılar tarafından yapılandırıldığını düşünen akademisyenler dahi vardır (Cheneu, 2014; Pohle vd., 2016). Bu çerçeve, erişim hakkı, ifade özgürlüğü, güvenlik, gizlilik, katılımcılık ve şeffaflık gibi ilkeler etrafında şekillenir.

Normatif teori, adil savaş, insani müdahale, siyasal yapılanma, demokratik barış ve koruma sorumluluğu gibi çeşitli siyasi konuları inceler. Ancak bu çalışma, özellikle norm, adalet, hukuk ve düzen kavramlarının önemine odaklanır. Bu bağlamda küresel internet yönetişimini öne çıkan bir sorun olarak ele alır ve bu alanın karşılaştığı zorlukların norm temelli boyutları göz önünde bulundurularak düzenlenmesi gerektiğini belirtir. Bunun yanında, normatif teorinin öne sürdüğü "hukukun düzenleyici rolü" çalışma açısından bir sorun alanı olarak kabul edilen "hukuki mekanizmanın olmaması durumunu" yansıtmaktadır. Bu nedenle, bu öğeler aşağıda detaylı bir şekilde ele alınacaktır.

1.3.4.1. Norm

Normatif teori, uluslararası ilişkilerde normların nasıl ortaya çıktığını, yayıldığını ve uygulandığını inceleyen bir teoridir. Bu teoriye göre, normlar, devletlerin ve diğer aktörlerin davranışlarını yönlendiren ve düzenleyen kurallardır. Normlar resmi (yasalar, antlaşmalar) veya gayri resmi (örf ve adetler, ahlaki ilkeler) olabilmektedir. Bu yönüyle normlar, uluslararası ilişkilerdeki aktörlerin davranışlarını şekillendiren temel unsurlar olarak kabul edilmektedir.

Ulusların kendi kendine yeten birimler olarak algılandığı küresel doğa durumu, devletlerarasındaki ilişkilerde ahlaki normların zayıflığını gösterir. Machiavelli, Hobbes ve Rodin gibi geleneksel teorisyenler, uluslararası ilişkilerde evrensel bir kuralın varlığını reddederek, varlık nedenini en yüksek norm olarak kabul etmişlerdir. Uluslararası hukuk gibi ahlaki bağlar kabul edilse bile, ulus-üstü otoritenin yokluğu nedeniyle ulus-içi ahlaki bağlardan daha zayıf olduğu savunulmuştur. Bu düşünürler

için uluslararası ilişkilerde teorik ilgi gören tek konu, savaşın meşrulaştırılması ve önlenmesidir. Ancak küreselleşme sürecinin başlamasını müteakip bu ihmal, sorgulanmayı gerektirmiştir (Beitz, 1999, s. 3). Zira küreselleşme, ulus devlet sınırlarını aşan ve uluslararası normatif teorinin kapsamına giren etik sorunların sayısını ve karmaşıklığını artırmıştır.

Devletlerin kendi kendine yeten siyasi düzenler olarak görülmemesi gerektiğinin anlaşılması, uluslararası ilişkilerdeki normatif teorinin, devletlerin ötesindeki aktörleri ve küresel yönetişim mekanizmalarını da dikkate alması gerektiğini gösterir. Normatif teori, Westphalia sonrası dönemde uluslararası ilişkilerde devlet merkezli bir bakış açısının ötesine geçmenin önemini vurgulamaktadır. Bu teoriye göre uluslararası örgütler, sivil toplum kuruluşları ve uluslararası kamusal alanlar gibi kurumsal mekanizmalar ve küresel yönetişimin diğer biçimleri dikkate alınmalıdır. Bu bağlantılar, uluslararası ilişkilerdeki normatif teorinin bireyler ve devletler arasındaki ilişkilere odaklanmak yerine daha geniş bir çerçevede düşünmesini sağlayabilir. Bu bağlamda normatif teori, daha geniş ahlaki taahhütlerin oluşturulması ve geliştirilmesini önemli bir "görev" olarak görür (Cochran, 2004, ss. 116-117). Küreselleşme ve artan karşılıklı bağımlılık, devletler ve uluslararası alandaki diğer aktörler arasındaki karmaşık bir ilişki ağı yaratmıştır. Bu durum, geleneksel "küresel doğa durumu" imajının artık geçerli olmadığını ve uluslararası ilişkilerin ahlaki boyutunu göz ardı etmenin imkânsız hale geldiğini göstermektedir (Beitz, 1999, s. 4).

Küreselleşme, farklı kültürler arasındaki etkileşimi hızlandırmış ve bu durum internet yönetişiminde dikkate alınması gereken “karmaşık bir değerler manzarası” ortaya çıkarmıştır (Senges & Horner, 2009, s. 11). Normların, bu karmaşık değerler mekanizmasını kontrol etme ve uluslararası sistemde istikrarı teşvik etme gibi antlaşmaların sağladığı bazı amaçları yerine getirebilecek kapasitesi vardır. Teknolojideki hızlı değişimlere ayak uydurabilme potansiyelleri ile normlar, uluslararası hukukun geliştirilmesine de katkıda bulunabilir. Özellikle, siber olaylara müdahalede devlet uygulamaları, gelecekte benzer olaylara nasıl yaklaşılacağını belirlemeye yardımcı olabilir.

Küresel internet üzerinde bir yönetişim rejiminin oluşturulmasının zorunlu olduğu ancak geniş kapsamlı bir antlaşmanın mümkün olmadığı durumlarda dahi, davranışı yönlendirmek için normların geliştirilmesi ön plana çıkar. Normlar, müzakere edilmiş

antlaşma metinlerinden farklı olarak, kesin kurallardan ziyade genel ilkeler olarak işlev görür. Bu esneklik, normların oluşturulmasını, geniş çaplı antlaşmaların zorluklarına bir alternatif olarak cazip kılar. Devletler ve diğer aktörler, normları tek taraflı politika bildirimleri, ikili veya çok taraflı bildirimler ve hatta pratik eylemler yoluyla geliştirebilir. Örneğin, NATO'nun Siber Savunma Politikası ve BM Kamu Uzmanları Grubu'nun siber uzayın uluslararası hukuka tabi olduğunu belirten bildirisi, normların siber yönetişimi nasıl şekillendirilebileceğini gösterir. Eichensehr'ın örneklerinde görüldüğü gibi, devletler ve diğer aktörler tarafından geliştirilen normlar, geniş çaplı antlaşmaların yerini alarak, siber olaylara müdahalede ve uluslararası hukukun geliştirilmesinde önemli bir rol oynayabilir (2015, s. 361).

Devletlerin artık geleneksel anlaşmalar yapmak ya da kurallar belirlemek yerine, siber güvenlik gibi özel alanlarda uluslararası hukukun geleneksel çerçevesinin dışında kalan normatif unsurlara yöneldiği görülmektedir. Bu eğilim, "uluslararası norm oluşturmanın çeşitliliği" olarak bilinen bir kavramla açıklanabilir. Bu durum, günümüzde uluslararası alanda kamu gücünün uygulanmasının büyük bir kısmının, geleneksel uluslararası hukuk normları oluşturma yöntemlerinden farklı olduğunu ortaya koymaktadır (Mačák, 2017, s. 8).

Sonuç olarak, geniş kapsamlı bir antlaşmanın olasılık dışı olduğu bir durumda normlar, devletlerin ve diğer aktörlerin siber uzaydaki davranışlarını düzenlemek için en umut verici araçlardan biri haline gelir. Bu, siber uzaydaki askeri gücün kullanımı gibi en tehlikeli anlaşmazlık alanlarında bile, benzer düşünen devlet gruplarının ve müzakere edilen dar kapsamlı anlaşmaların ortaya çıkabileceği bir çerçeveyi sunmaktadır.

1.3.4.2. Düzen

"Düzen, yönetişim olmadan da var olabilir, ancak yönetişim bir tür düzen gerektirir." (Biersteker, 1992, s. 102). Küresel düzenin[28] normatif boyutları yaygın ve kaçınılmazdır. Normatif teorisyenler, küresel düzenin nasıl olması gerektiğine dair fikirler üretirler (Roseanu, 1992, ss. 11-12). Bu fikirler, adalet, eşitlik ve insan hakları gibi kavramlara dayanır. Normatif teorisyenler, küresel düzenin mevcut durumunu eleştirir ve onu daha iyi hale getirmek için önerilerde bulunurlar. Normatif

[28] Devletler arasındaki ilişkilere dayanan uluslararası düzen fikrinin aksine, küresel düzen fikri imparatorluk, federasyon, bölgesel işbirliği veya ulus ötesi ilişkilere ve gayri resmi küresel yönetişime dayalı devletsiz bir düzen gibi diğer olası düzenlemeleri önermektedir (Nardin, 2022).

teorisyenlerin adalet, eşitlik ve insan haklarına dayalı önerileri, küresel düzenin sadece var olanı değil, aynı zamanda nasıl olması gerektiğini de şekillendirir.

Normatif teorisyenlerin önerileri, küresel düzenin mevcut durumunu eleştirir ve onu daha iyi hale getirmeye yönelik bir çerçeve sunar. Teori, açıklayıcı teorileştirmeyi ahlaki ve politik kaygılara, küreselleşmenin ortaya çıkardığı sorunlara ve kökleri farklı medeniyetlere dayanan uluslararası düzen hakkındaki fikirlere bağlar (Nardin, 2022). Bu teori, uluslararası düzenin nasıl olması gerektiği ve devletlerin nasıl davranması gerektiği gibi normatif sorulara cevaplar arar. Devletlerin egemenliği, insan hakları, adil savaş, insani müdahale, mülteciler, küresel adalet, çevre gibi birçok önemli konuda normatif çerçeveler ve ilkeler geliştirmeye çalışır (Bakan, 2002, s. 437). Bu normatif çerçeveler, uluslararası ilişkilerin kozmopolitanizm ve komüniteryenizm gibi iki temel perspektiften nasıl ele alınabileceğine ışık tutar.

Komüniteryen yaklaşım, devlet egemenliğini ve ulusal kimliği öne çıkarır, egemenliğin devlete ait olduğunu ve ulusal adaletin küresel adalete göre öncelikli olduğunu savunur. Bu görüşte, uluslararası toplumda devletler merkezi bir yer tutar ve bireylerin hakları öncelikle kendi devletleri tarafından korunur. Buna karşılık, kozmopolitan yaklaşım, evrensel insan haklarının devlet egemenliğinden üstün olduğunu, sınırların ve egemenliğin insan refahını artırmak için yeniden değerlendirilebileceğini öne sürer. Bu yaklaşım, küresel bir siyasi ve ahlaki düzeni, uluslararası kurumların ve sivil toplumun aktif rolünü ve küresel adalet ile eşitliği savunur (Bakan, 2002, s. 438-439). Kozmopolitan görüşü temsil eden önemli düşünürler arasında Immanuel Kant, John Rawls, Martha Nussbaum ve David Held bulunurken; komüniteryen görüş Michael Walzer, Charles Taylor, Alasdair MacIntyre ve Amitai Etzioni tarafından savunulmaktadır. Her iki yaklaşım da, devlet egemenliği, insan hakları, adaletin dağılımı, insani müdahaleler ve çevre gibi konularda farklı öncelikler ve çözüm yolları önerir.

Kozmopolitanizm ve komüniteryenizmin sunduğu çerçeveler, küresel yönetişimde meşruiyetin ve demokrasiye dayalı yaklaşımların değerlendirilmesi için önemli bir temel oluşturur. Macdonald (2019), hem enternasyonalist hem de kozmopolit modellerin, meşruiyeti "kapalı" topluluklarda rasyonel siyasi eyleme dayandırdığını ifade ederek devletçi paradigmanın ötesine geçen "çoğulcu" bir dünya düzeni tahayyülü sunar. Bu tahayyülde meşruiyet, "açık" topluluklarda yaratıcı siyasi eyleme dayanır. Bu

topluluklar, farklı ve akışkan çıkarlara ve kimliklere sahip çok sayıda aktörden oluşur ve sürekli bir dönüşüm halindedir. Dolayısıyla çoğulcu model, küresel yönetişimde meşruiyeti güçlendirmek için önemli bir çerçeve sunar. Bu model, rasyonellik ve hesap verebilirlik ilkelerini göz ardı etmeden, farklı seslerin ve bakış açılarının dahil edilmesine imkân tanır.

Koenig-Archibugi'ye göre (2011) normatif yaklaşımlar, küresel yönetişimin meşruiyetini demokrasiye dayalı çeşitli perspektiflerden değerlendirmenin önemini vurgular. Bu bağlamda, iki temel yaklaşım öne çıkar: demokratik hükümetlerarasıcılık ve demokratik kozmopolitlik. Demokratik hükümetlerarasıcılığa göre küresel yönetişim, doğrudan demokratik meşruiyetten yoksundur ve meşruiyetini demokratik olarak seçilmiş hükümetlerin küresel politika oluşturma sürecine katılımları yoluyla dolaylı olarak kazanır. Bu yaklaşım, demokrasinin bir kamusal alan gerektirdiği ve ulusötesi bir kamusal alanın henüz mevcut olmadığı görüşüne dayanır. Demokratik müzakerenin, dil engelleri ve eğitimli seçkinlerin müzakereleri tekelleştirmesi gibi zorluklar nedeniyle küresel düzeyde zorlaşacağını savunur. Ayrıca, ulusal düzeyin ötesinde kolektif kararların kabulü için gerekli olan dayanışma ve aidiyet duygusunun zayıflığına dikkat çeker. Öte yandan, demokratik kozmopolitlik, demokratik meşruiyetin, küresel yönetişimin çoğulcu doğasına uygun olarak, birden fazla kanaldan sağlanabileceğini ve sağlanması gerektiğini önerir. Bu yaklaşım, uluslararası kurumların demokratikleşmesinin bireylerin ve grupların ilgisini ve sadakatini ulusal boyutun ötesine taşıyabileceğini ve bu şekilde demokratik yeniden yapılanmanın karşılıklı olarak birbirini güçlendiren bir süreç olduğunu savunur (Hirst vd., 2009, ss. 322-323).

Küresel internet yönetişimi ve diğer küresel sorunlar üzerine yapılan normatif tartışmalar, uluslararası toplumun sürekli değişen yapısına ve yeni zorluklara nasıl yanıt verilebileceğini gösterir. Küresel dönüşümlerin dinamikleri, analitik bir kavram olarak "düzen" ile normatif bir kural olarak "düzen" arasındaki ayrımı netleştirmeye yardımcı olur. Değişim belirsizliği besler ve değişim süreçleri ne kadar dinamik olursa, belirsizlik de o kadar artar. İnsanlar değişim öncesi istikrarın kaybından endişe duyar ve değişimin kurumları ve koşulları daha öncekinden daha az tatmin edici hale getireceğinden korkabilirler. Bu nedenle, dönüştürücü dinamikler, endişeleri yeni ortaya çıkan küresel düzenlemelerin, yerini aldıkları düzenlemelere kıyasla arzu edilirliği etrafında odaklayacaktır. Küresel düzene (çatışmalarla başa çıkma ve

hedeflere ilerlemeyi amaçlayan temel düzenlemelere ilişkin) dair sorunlar siyasi arenada yüzeye çıktıkça, normatif kaygıların yoğunlaşması kaçınılmazdır (Rosenau, 1992, ss. 9-10).

Küresel dönüşümlerin getirdiği belirsizlikler ve değişim süreçlerinin artan dinamikleri, normatif teori ve pratikteki "düzen" kavramının önemini vurgular. Normatif teorinin uluslararası toplumdaki değişimlere ayak uydurma ve küresel düzeni daha iyi hale getirme kapasitesi vardır (Hurrell, 2002, s. 191). Uluslararası toplum, zamanla değişen bir yapıya sahiptir. Yeni devletler ortaya çıkıyor, yeni teknolojiler geliştiriliyor ve küresel sorunlar artıyor. Normatif teori, bu değişimlere ayak uydurabilir ve yeni koşullara uygun yeni ilkeler ve standartlar ortaya koyabilir. Bu sayede normatif teori, küresel düzeni daha adil, barışçıl ve sürdürülebilir hale getirmeye yardımcı olabilir.

1.3.4.3. Hukuk

Küreselleşme ve teknolojinin hızlı gelişimi, uluslararası hukuk ve normatif teorilerin önemini artırmıştır. Uluslararası hukuk; hükümetlerarası örgütler, siyasi işbirliği ve uluslararası rejimler gibi kurumsal değerler ve normatif sistemler aracılığıyla, uluslararası ilişkilerde istikrar ve düzeni sağlamada kritik bir role sahiptir (Dyer, 1997, s. 179). Normatif teori ve uluslararası hukuk konuları, bugünkü uluslararası düzende devletlerin ve uluslararası aktörlerin karşılaştığı zorluklara çözüm bulma çabalarında merkezi bir rol oynar. Bu bağlamda, uluslararası ilişkiler ve hukukun nasıl şekillendirildiğini anlamak, küresel adaleti sağlama ve siber güvenlik gibi çağdaş sorunlara etkili çözümler üretme konusunda yol göstericidir.

Küresel adaleti sağlamanın en iyi yolu, uluslararası hukukun güçlendirilmesi mi yoksa ulus devletlerin yerine geçen uluslarüstü kurumların oluşturulması mıdır sorusu uzun süredir devam eden bir tartışmadır. Uluslararası hukukun küresel adaleti sağlamada önemli bir rol oynayabileceği savunulmaktadır. Bu görüşe göre adil bir uluslararası düzenin temelini oluşturabilecek evrensel hukuk normları ve ilkeleri geliştirilebilir. Bu normlar ve ilkeler, insan hakları, çevre koruma, küresel ticaret ve kalkınma gibi alanlarda adil ve eşitlikçi bir düzenin kurulmasına yardımcı olabilir (Nardin, 2022).

Küresel adaletin sağlanması konusunda, etik ilkelerin yaptırım gücü olmadan zayıf kalabileceği belirtilmektedir. Uluslararası hukukun araçsal değerlendirmeleri ve emirleri, müdahale için zorlayıcı nedenler sağlamada etiğe göre daha donanımlıdır (Cochran, 2004, s. 254). Etik, gücü onaylayabilir veya meşrulaştırabilir. Ancak etik

ilkelerin evrensel olarak kabul görmemesi bu meşrulaştırmayı zayıflatır. Bu nedenle etik ilkelerin somut ve evrensel bir temele oturması gerekir. Bununla birlikte Nardin (2022), uluslararası hukukun temel alındığı küresel bir düzende devletlerin rolünün de hesaba katılması gerektiğini belirtmiştir. Her ne kadar küreselleşme, devletlerin egemenliğini aşındırmış olsa da, devletler hala sadık varlıklar olarak kabul edilmiştir. Devlet idaresine duyulan ihtiyaç daha karmaşık hale gelmiştir, ancak ortadan kalkmamıştır. Uluslararası hukuk da devletlerin dahil olduğu bir dünya düzenini kurmak için bir çerçeve sağlamaktadır. Bu nedenle, küresel düzen teorisinin devletlerin rolünü de hesaba katması gerektiği ifade edilmiştir. Kant'tan Rawls'a kadar birçok teorisyenin hayal ettiği gibi, hukukun üstünlüğüne sahip devletlerin genişleyen bir konfederasyonunun küresel bir hukuk düzeni için bir model teşkil edebileceği belirtilmiştir. AB, Brexit ve diğer güncel sorunlara rağmen bu konuda örnek olarak gösterilmiştir.

ABD'nin fikri mülkiyet hırsızlığına karşı hukukun üstünlüğü normlarını savunması ve Budapeşte Sözleşmesine bağlılığın desteklenmesi, devletlerin kabul edilebilir davranışlar konusunda zamanla ortak bir anlayışa varabileceğini gösterir. ABD, AB ve Çin gibi büyük aktörler tarafından getirilen düzenlemeler, uluslararası düzeyde istikrar sağlama potansiyeline sahiptir. ABD, fikri mülkiyet hırsızlığı ve siber alanda gerçekleştirilen diğer yasa dışı faaliyetlere karşı durmakta ve hukukun üstünlüğü ilkelerini savunmaktadır. Bu çerçevede, Budapeşte Sözleşmesi'ne olan geniş çaplı desteğini de vurgulamaktadır. Siber altyapıya ve yeniliklere giderek daha fazla bağımlı hale gelen Çin, Rusya ve diğer ülkeler, siber saldırılar ve siber suçlardan kaynaklanan hasarlar nedeniyle ABD'nin siber hukukun üstünlüğüne yönelik tutumunu benimsemeye yönlendirilebilirler. Devletlerin normları keşfetmesi, gelecekte resmi anlaşmalara zemin hazırlayabilir (Eichensehr, 2015a, ss. 362-363).

ABD, AB ve Çin gibi büyük aktörler tarafından getirilen düzenlemeler, uluslararası düzeyde istikrar sağlama potansiyeline sahiptir. Ancak, yasal düzenlemelerin etkinliği konusunda, bu araçların yasal olmayan eylemleri meşrulaştırma eğilimine sahip olması şüpheye mahal vermektedir. Bu nedenle, siber alanda etik yaklaşımların önemi vurgulanmaktadır. Adil savaş teorisinden alınan ilhamla, sivillere zarar verme niyeti taşıyan ve orantısız eylemlerin kınanması gerektiği belirtilmektedir (Valeriano & Maness, 2017, s. 269). Adil savaş teorisi, sivillere zarar verme niyetinde olan ve orantısız eylemlerin reddedilmesi gerektiğine dair yöntemler sunar. Siber güvenlik

tartışmasının merkezinde, siber uzayda sivil ve askeri hedefler arasında net bir ayrım olmaması gerçeği yatar.

Siber altyapıya ve yeniliklere giderek daha fazla bağımlı hale gelen ülkeler, siber saldırılar ve siber suçlardan kaynaklanan hasarlar nedeniyle ABD'nin siber hukukun üstünlüğüne yönelik tutumunu benimsemeye yönlendirilebilirler. Devletlerin normları keşfetmesi, gelecekte resmi anlaşmalara zemin hazırlayabilir (Eichensehr, 2015a, ss. 362-363). Deibert ve Rohozinski, siber uzay kontrolünü üç nesil olarak tanımlayarak farklı evrelerdeki kontrol stratejilerini açıklamaktadır. Birinci nesil kontrol, internet kaynaklarına erişimi engellemeye yönelik basit önlemler alırken; ikinci nesil kontrol, bilgiye erişimi engellemeyi yasallaştıran hukuki ve normatif bir alanın oluşturulmasını içerir. Üçüncü nesil kontrol ise, bilginin manipülasyonu ve geniş kapsamlı gözetim gibi daha karmaşık stratejileri barındırır. Bu, bilgi üzerinde daha sofistike ve karmaşık bir kontrol anlayışını ifade eder.

Sonuç olarak normatif teorinin hukuk anlayışı, evrensel değerler ve ilkeler üzerine kuruludur. Küreselleşme ve teknolojinin hızlı gelişimi, uluslararası ilişkilerde istikrar ve düzeni sağlamada uluslararası hukukun rolünü artırmıştır. Bu bağlamda, uluslararası hukuk ve normatif teoriler, devletlerin ve uluslararası aktörlerin karşılaştığı zorluklara çözüm bulma çabalarında merkezi bir rol oynar. Küresel internet yönetişimi, siber güvenlik, fikri mülkiyet hırsızlığı, veri koruma ve internetin serbest akışı gibi konuları kapsar. Normatif teorinin bu alanda uygun olup olmadığı, bu teorinin küresel sorunlara etkili çözümler üretebilme kapasitesine bağlıdır.

1.3.4.4. Adalet

Pogge, çağdaş dünyada insanların yaşamının ticaret, diplomasi gibi alanlarda ve aynı zamanda küresel yönetişim kuralları tarafından büyük ölçüde etkilendiğini belirtir. Bu küresel kurumların nasıl şekillendirileceği konusunda her zaman genel bir mutabakat sağlanması zordur. Ancak, bu kurumların dünya genelindeki insanlar tarafından adil bulunmasını sağlamak ve değişen koşullar ışığında nasıl düzenlenmesi gerektiğine dair uzlaşıya varabilmek için, herkesin kabul edebileceği bir küresel adalet[29] ölçütüne ihtiyaç duyulmaktadır (2002, s. 33).

[29] Uluslar arasında adalet olarak uluslararası adaletin aksine, küresel adalet haklara saygı gösterilmesi veya malların uluslar ötesi dağıtımı konusunda adalettir. Küresel adaleti savunanlar sınırların ötesinde bir adaletten bahseder ve devletlerin daha az belirgin bir rol oynadığı bir dünya topluluğu hayal ederler (Nardin, 2022).

Pogge'nin (2002) küresel adalet ölçütü, küresel düzen ve diğer önemli uluslararası etkileri olan toplumsal kurumlar hakkında ahlaki yargıların temelini oluşturmayı öngörür. Küresel internet yönetişimi bağlamında adalet anlayışı; yönetişimde eşitliği, gelişmiş ve gelişmemiş ülkeler arasındaki dijital uçurumu ve ahlaki değerleri ele almayı gerektirir. Bu, siber uzayın yönetişiminde tüm aktörler için adil ve kapsayıcı bir çerçevenin oluşturulmasına yönelik bir gereksinimdir. Böylece dijital bölünme azaltılabilir ve siber güvenlik normları herkesin yararına olacak şekilde şekillendirilebilir.

Adler ve Bernstein, iyi (ahlaki) küresel yönetişimin mümkün koşullarını belirlemeye çalıştıkları çalışmalarında küresel yönetişimin meşruiyet ve adalete dayanması gerektiğinin altını çizmişlerdir. Bu unsurlar olmadan ahlaki bir yönetişimden bahsedilemeyeceğini öne sürmüşlerdir (2004, s. 294). Diğer yandan "siber adalet" kavramını ele alan Mihr'e göre siber adalet, siber alanda insan hakları normlarına dayalı iyi yönetişimi teşvik etmek için uygulanabilir bir yaklaşımdır. Mihr, siber alanda insan haklarının korunması için de bir yaklaşım önerir. Bu yaklaşıma göre siber uzaya kamusal alan olarak bakılmalıdır. İnternet ise, bu kamusal alanda iletişim ve etkileşim için kullanılan bir araçtır. Mihr, bu bağlamda, siber uzayın giderek daha fazla hem sanal hem de fiziksel hayatlarımızın bir parçası haline geldiğini vurgular ancak siber alan ile fiziksel alan arasındaki farka dikkat çeker. İnternette hizmet veren aktörler ve kurumların, fiziksel alanda olduğu gibi adalete hesap verme zorunluluğuna sahip olmadığını belirtir. Zira insan haklarının siber ortamda da geçerli olduğu kabul edilse de, bu hakların internet kullanımı ve sunduğu hizmetler bağlamında nasıl uygulanacağı halen tartışmalıdır. (2016, ss. 314-315).

Öte yandan, siber alandaki adalet ve yönetişim ilkeleri, uluslararası düzeyde devletlerin eylemlerini ve normları benimseme süreçlerini de etkileyebilir. Zira devletlerin uluslararası toplumun bir üyesi olarak kabul edilme arzusu, yeni normları benimsemelerinde önemli bir rol oynar. Bu normlar, devletlerin uluslararası alanda kimliklerini kanıtlamalarına, meşruiyet kazanmalarına ve saygınlık görmelerine yardımcı olur. Uluslararası normlar, aynı zamanda devletlerin hangi gruba ait olduğunu belirlemede de önemli bir rol oynar (Bakan, 2002, s. 235).

Zürn (2018a), normatif ilkeler ile otorite ilişkileri üzerinden meşruiyet okuması yaptığı çalışmasında, mevcut küresel yönetişim sisteminin içsel özelliklerinin, uluslararası

otoritelerin siyasallaşmasını ve karşı-kurumsallaşmasını tetiklediğini öne sürer. Sistemin iç gerilimleri, meşrulaştırma sorunlarını ve değişim taleplerini körükler. Bazı durumlarda değişim taleplerine karşılık derinleşmenin meydana gelmesi, meşruiyet kaygısıyla alınan kararların etkili ve kapsayıcı sonuçlar doğurmasını sağlayabilir. Bu durum, Buchanan ve Keohane'nin "meşruiyeti adaletle karıştırmak, en iyiyi iyinin düşmanı haline getirmektir"[30] sözünü hatırlatır (2006, s. 412). Zira küresel internet yönetişiminde aktif rol oynayan aktörler -özellikle özel sektör ve devletler- konuya dair normatif vizyonlarını çoğunlukla küresel adalet saikiyle değil, meşruiyet amacıyla gerçekleştirmektedir. Ama yürüttükleri politikanın amacı her ne kadar çıkar amaçlı ve/veya meşruiyet odaklı olsa da, nihayetinde normatif bir sonuç doğurmaktadır. Dolayısıyla meşruiyet çabaları normatif adalet ilkeleri doğuracaksa, bundan maksimum faydanın elde edilmesi için çabalanması gerekmektedir. Önceki alt başlıklarda değinilen büyük teknoloji şirketlerinin çabaları buna örnek olarak gösterilebilir. Facebook gibi büyük bir teknoloji şirketinin içerik yönetimi ve karar verme süreçlerinde güttüğü meşruiyet kaygısı bunun önemli bir örneğini temsil etmiştir (Pigatto vd., 2021, s. 8). Bu bağlamda meşruiyet ve adalet arayışı yalnızca normatif sonuçlar üretmekle kalmaz, aynı zamanda Habermas'ın adalet teorisinde vurguladığı gibi, özgür ve eşit bir iletişim sürecinin temelini de oluşturur (Floomkin, 2003, s. 752).

Sonuç olarak, normatif teorinin adalet anlayışı, küresel internet yönetişimi bağlamında hem mevcut zorluklara çözüm sunabilecek hem de eşitlik, insan hakları ve demokratik iletişim süreçlerinin güçlendirilmesi yoluyla adil bir siber ortamın oluşturulmasına katkıda bulunabilecek bir çerçeve sunar. Dolayısıyla, normatif teorinin adalet anlayışının, küresel internet yönetişimiyle uyumlu olduğu ve bu alanda önemli bir rehber olabileceği sonucuna varılabilir.

[30] Bu ifade, "mükemmeliyetçiliğin, iyi olanı engellemesi" anlamını taşır. Yani, meşruiyet ve adalet kavramlarını birbiriyle karıştırmak, ideal olanı ararken gerçekten iyi olanı göz ardı etmek anlamına gelir. Burada vurgulanan, bazen en iyi olana ulaşmaya çalışırken, gerçekte iyi olanı ve uygulanabilir olanı gözden kaçırabileceğimizdir. Bu durum, pratikte iyi sonuçlar elde etmek için uygulanabilir ve adaletli çözümleri göz ardı etmememiz gerektiğini hatırlatır. Zira meşruiyet ve adalet arasındaki dengeyi korumak, gerçekçi ve adil sonuçlar elde etmenin anahtarıdır.

Değerlendirme

Çalışmanın birinci bölümü, küresel internet yönetişiminin kavramsal ve kuramsal çerçevesini detaylı bir şekilde incelemiştir. Bu inceleme, yönetişimin tarihçesinden başlayarak, internetin ortaya çıkışı ve küreselleşmesi süreçleri üzerinden günümüzde karşılaşılan dijital yönetişim zorluklarına ve çeşitli teorik yaklaşımların bu zorluklara sunduğu çözümlere kadar geniş bir yelpazeyi kapsamaktadır. Bu kapsamda yönetişimin tanımı ve önemi, küreselleşme ile değişen yönetişim dinamikleri ve dijital çağda yönetişimin karşı karşıya kaldığı spesifik sorunlar ve bu sorunlarla başa çıkmak için önerilen teorik çerçeveler ele alınmıştır.

1990'ların ortalarından itibaren internetin ticarileşmesinin de etkisiyle öneminin artması, internete yönelik teknik bakış açısının yeterli olmadığını göstermiştir. Zira 1990'ların ortalarını takip eden birkaç on yıl içinde internet, yalnızca teknik topluluk için değil, bütün aktörler için önemli bir ağ haline gelmiştir. Bugün ise internet, en etkili iletişim aracı ve en büyük küresel pazar olarak anılmaktadır. Öte yandan, bugüne kadar tasarlanmış en büyük kitlesel gözetim aracı olmuş ve bu yönüyle tek bir devletin (ABD) yetki alanından çıkarak küresel bir mahiyet kazanmıştır. Bu bağlamda internetin artık "küresel bir güç alanı" olduğunu söylemek yanlış olmayacaktır.

Yönetişim kavramının evrimi, geniş bir aktör yelpazesinin katılımıyla, hiyerarşi ve zorunluluğa dayanmayan bir sosyal yönlendirme biçimi olarak ortaya çıkmıştır. Bu evrim, yönetişimin sadece devletlerin değil, sivil toplum, özel sektör, ve uluslararası kuruluşlar gibi çok sayıda aktörün etkileşimi ile şekillendiğini vurgulamaktadır. Küreselleşme ile birlikte yönetişimin uluslararası bir boyut kazandığı, ekonomik küreselleşme, teknolojik ilerleme ve çevresel sorunlar gibi faktörlerin bu yeni yönetişim modelini desteklediği gözlemlenmiştir. Diğer yandan internetin ortaya çıkışı ve hızla küreselleşmesi, bilgiye erişim, iletişim biçimleri ve sosyal etkileşimler üzerinde devrim yaratmıştır. Ancak bu devrim, yönetişim, güvenlik, gizlilik ve erişim gibi bir dizi karmaşık sorunları da beraberinde getirmiştir. Bu sorunların ele alınması, teknolojik çözümlerin ötesine geçerek, sosyal, politik ve etik boyutları kapsayan geniş bir perspektifi gerektirir.

İnternetin küreselleşmesiyle birlikte ortaya çıkan dijital yönetişim tartışmaları, ulusal yasaların ve düzenlemelerin ötesinde, küresel bir işbirliği ve koordinasyon ihtiyacını vurgulamıştır. Bu durum, geleneksel ulus-devlet modelinin sınırlarını zorlayarak

küresel sorunlara küresel çözümler üretme gerekliliğini öne çıkarmıştır. Küresel iyi yönetişim kavramı, yönetişimin amacının kontrol ve düzenleme olmadığını; işbirliği, şeffaflık ve katılımcılığı teşvik ederek daha adil ve sürdürülebilir bir düzen oluşturmayı hedeflediğini belirtir. Bu, çok paydaşlı işbirliği modellerinin önemini artırırken, yönetişimin çeşitli çıkarları, değerleri ve güç dinamiklerini dengede tutmayı amaçladığını gösterir.

Teknik ve politik yaklaşımlar, internet yönetişiminin temel boyutlarını oluştururken, her iki perspektifin bütüncül bir anlayış geliştirilmesi için hayati olduğunu ortaya koyar. Bu karmaşık süreç, çeşitli teorik yaklaşımların ve çok sayıda aktörün katkılarının entegre edilmesini zorunlu kılar. İnternet yönetişiminin aktörleri arasında devletler, hükümetlerarası ve uluslararası kuruluşlar, özel sektör, sivil toplum ve bireyler yer alır. Bu çok katmanlı yapı, yönetişimin daha kapsayıcı ve demokratik hale gelmesine olanak tanırken, süreçleri daha karmaşık hale getirir.

Öte yandan realizm, liberalizm, inşacılık, ve normatif teori gibi çeşitli teorik yaklaşımlar, dijital yönetişim zorluklarını farklı perspektiflerden ele almakta ve potansiyel çözüm yolları sunmaktadır. Realizm, güç ve güvenlik meselelerine odaklanarak devletlerin dijital alanda nasıl dominant bir rol oynayabileceğini tartışırken, liberalizm, işbirliği ve uluslararası kuruluşların rolünü vurgulayarak, açık ve bağlantılı bir internet için çerçeveler önerir. İnşacılık, dijital yönetişim anlayışlarının ve politikalarının sosyal yapılar ve normlar tarafından nasıl şekillendirildiğini inceler. Normatif teori ise, adil ve etik bir dijital düzenin nasıl oluşturulabileceği üzerine odaklanır, dijital çağda adalet, haklar ve özgürlüklerin korunmasına yönelik normatif çerçeveleri ön plana çıkarır. Bu teorik yaklaşımlar, dijital yönetişim zorluklarını ele alırken, her birinin farklı boyutları vurguladığı ve bu nedenle, etkili bir dijital yönetişim stratejisinin çok yönlü bir yaklaşımı gerektirdiği görülmüştür.

Yine de, normatif teorinin norm, hukuk, düzen, ve adalet üzerine geliştirdiği argümanlar, küresel internet yönetişimine en uygun teori olduğunu söylemek gerekmektedir. Zira normatif teorinin küresel internet yönetişimiyle ilgili sorunları ele alış biçimi, özellikle etkin bir hukuk mekanizmasının eksikliği gibi çeşitli sorun alanlarını kapsar. Bu teori, normların, hukukun, düzenin ve adaletin uluslararası ilişkilerde nasıl işlediğini inceler. Devletlerin ve diğer aktörlerin davranışlarını yönlendiren ve düzenleyen kuralların nasıl oluşturulduğu, yayıldığı ve uygulandığına

dair bir çerçeve sunar. Bu, internet yönetişimi gibi teknolojik ve hızla gelişen alanlarda, uyum sağlama ve yenilikçi çözümler geliştirme kapasitesi açısından kritik öneme sahiptir. Özellikle, siber güvenlik, veri koruma ve internetin özgür kullanımı gibi konularda, yeni normların oluşturulması ve uygulanmasına rehberlik edebilir.

Sonuç olarak, bu bölümde yapılan analizler, küresel internet yönetişiminin, çok katmanlı ve çok aktörlü bir yapıya sahip olduğunu ve bu alanda etkili politikalar geliştirebilmek için çeşitli teorik yaklaşımların ve aktörlerin katkılarının entegre edilmesi gerektiğini göstermektedir. İnternet yönetişimi, sadece teknik bir alan olmanın ötesinde, güç, güvenlik, özgürlük, adalet ve hukuk gibi temel kavramlar etrafında şekillenen derinlemesine bir politik ve sosyal etkileşim alanıdır. Bu nedenle, etkili bir küresel internet yönetişimi yapısının oluşturulabilmesi için, normatif teorinin sunduğu ahlaki ve etik değerlere dayalı yaklaşımların, teknik ve politik çözüm önerileriyle birleştirilmesi büyük önem taşımaktadır. Bu bütüncül yaklaşım, dijital çağın getirdiği zorluklarla başa çıkmak ve küresel internet yönetişiminin geleceğini şekillendirmek için gereklidir.

BÖLÜM II: BİR SORUN OLARAK KÜRESEL DİJİTAL YÖNETİŞİM

Çalışmanın bu bölümünde, çeşitli teknik gruplarda ve internet yönetişimi ile ilgili forumlarda küresel olarak ele alınan ve tartışılan internet yönetişiminin politik ve teknik sorunları ve bunların yarattığı sonuçlar ele alınacaktır. Sorunlar birbiriyle ilişkili ve birden fazla boyuta sahip olduğu için saf bir sınıflandırma mümkün olmamıştır. Bu nedenle internet yönetişimi ile yakından ilgili olan politik konuların tartışılmasına dikkat edilmiştir. Diğer yandan, siber uzayın yönetilebilir olup olmadığı, negatif ve pozitif boyutlarla incelenmiştir. İlk olarak, siber uzayın yönetilmesinin önündeki engellerin yönetişime negatif yansımaları incelenmiş, daha sonra iyi bir yönetişim anlayışının olasılıkları pozitif bir vurguyla değerlendirilmiştir.

2.1. Sorun Alanlarının Belirlenmesi

Siber yönetişim konuları ele alınırken ilk olarak bu konuların sınıflandırılması gerekmektedir. Zira neyin yönetilmeye çalışıldığı ancak anlaşılır bir kategorizasyonla mümkün olabilecektir. Sınıflandırmanın ardından hangi konuların hangi kategoride yer alacağı belirlenmelidir. Esasında bu da bir sorundur çünkü siber yönetişim konuları çok disiplinli olduğundan bütün konular iç içe geçmiştir. Ancak genel bir kategorizasyon, sorunun ne olduğu konusunda daha net bilgi verebilir. Örneğin, siber suç, suç biçimlerine karşı mücadele ile ilgilendiği için bu bir siber güvenlik konusudur. Ancak siber suçluların yargılanması konusu, bir yargı meselesidir. Dolayısıyla konular arasındaki geçişler daha esnek olduğu için, sınıflandırmada keskin bir ayrımdan söz edilemez (Kurbalija, 2015, s. 94).

İnternet yönetişimi alanında küresel kapasiteyi geliştirmek amacıyla kurulan Diplo, internet yönetişimi konularını sınıflandırırken “sepet” terimini kullanmıştır. Diplo'nun internet yönetişimi sınıflandırması, 40 ana konuyu yedi kategoride veya "sepette" gruplandırmıştır. Bu kullanım, AGİT müzakereleri sırasında benimsenmiş ve kullanılmaya başlanmıştır. İlk olarak 1997 yılında yapılan sınıflandırmada beş sepet tanıtılmıştır. Bunlar; a) Altyapı ve standardizasyon b) Hukuki c) Ekonomik d) Kalkınma e) Sosyokültürel. Ancak internet yönetişimi meselelerinin genişlemesiyle birlikte 2014 yılında iki sepet daha eklenmiştir. Bunlar; f) Güvenlik (daha önce siber güvenlik olarak altyapı ve standardizasyon sepetinin bir parçasıydı) g) İnsan hakları

(önceden sosyokültürel sepetin bir parçasıydı) (Kurbalija, 2015, s. 94). Bu sınıflandırma, ilk olarak 1997'de Jovan Kurbalija tarafından geliştirilmiş ve daha sonra *İnternet Yönetişimine Giriş* adlı kitabında tanıtılmıştır. Sınıflandırma, siber alanın dinamik yapısına ayak uydurmak amacıyla sürekli güncellenmektedir (DiploFoundation, t.y.).

WSIS de siber yönetişim sorunlarını genel internet yönetişiminin tanımına eklemlemiştir. Zira bu tanım, siber yönetişimin teknik konularını ve kamu politikası konularını içerir. Tanım, Aralık 2003'teki ilk WSIS toplantısında yayımlanan Cenevre İlkeler Bildirgesi tarafından kabul edilmiş ve onaylanmıştır. Bildirgenin 56. Paragrafı, özellikle kamu politikası konularına dikkat çekilmesi gerektiğinin altını çizmiştir (UNGA, 2016, s. 12). 2005'teki ikinci WSIS toplantısından sonra yayınlanan raporun 17. Paragrafında ise bu konular dört geniş kategoriye ayrılmıştır: Bunlar şu şekilde sıralanmıştır:

(i) Kritik internet kaynaklarının yönetimi ile ilgili sorunlar (DNS, IP ve kök bölge yönetimi gibi),
(ii) İnternet kullanımıyla ilgili sorunlar (spam, ağ güvenliği ve siber suçlar gibi),
(iii) Sorunlardan sorumlu olan mevcut kuruluşların bulunduğu, internet ile ilgili ancak internetten çok daha geniş bir etkiye sahip olan konular (fikri mülkiyet hakları veya uluslararası ticaret gibi),
(iv) İnternet yönetişiminin gelişimsel yönleriyle ilgili konular (özellikle gelişmekte olan ülkelerde kapasite geliştirme gibi) (ITU, 2005c, s. 27).

Görüldüğü üzere siber yönetişim sorunlarının ele alınmasında birçok konuyu içeren farklı sınıflandırmalar yapılmıştır. Bu çalışmada, bu sınıflandırmalar dikkate alınmış ancak çalışmanın sınırlılıkları nedeniyle belirli konular ön plana çıkarılmıştır. Çalışmanın "sorun" odaklı olması gerekçesiyle "konuların" açıklanmasından ziyade daha geniş anlamda tartışılabilecek "sorunlara" yer verilmiştir. Bu bağlamda çalışmada 4 ana sorun alanı belirlenmiş ve bu sorunlara dahil olan belirli konular incelenmiştir. Bu konular şu şekilde sınıflandırılmıştır:

(i) Teknik Sorunlar: TCP/IP, DNS, Kök Bölge, World Wide Web, Blok Zinciri, Yükselen Sorunlar

(ii) Güvenlik Sorunları: Siber Güvenlik, Siber Güvenlikleştirme, Siber Suçlar

(iii) İnsan Hakları Sorunları: Veri Koruma ve Gizlilik, Online Özgürlük, İfade Özgürlüğü, Unutulma Hakkı

(iv) Diğer Sosyo-Politik Sorunlar: Erişim, Kalkınma ve Dijital Bölünme

Hukuki boyut için ise ayrıca bir parantez açmak gerekir. Zira çalışmada siber yönetişimin hukuki boyutu üçüncü bölümde detaylı bir şekilde analiz edileceği için bu bölümde yer verilmemiştir. Nitekim hukuk sorunu, çalışmanın bağlamını temsil etmekte ve küresel dijital yönetişim sorununun önemli bir parçası olarak kabul edilmektedir. Bu çerçevede üçüncü bölümde, siber uzaya uyarlanabilecek bir hukuk mekanizmasının olasılıkları mevcut hukuk yaklaşımları üzerinden değerlendirilecektir.

2.1.1. Teknik Sorun Alanları

İnternetin teknik sorunları genellikle internetin çalıştırılmasıyla ilgili temel ve teknik konuları içeren altyapı ve standardizasyon ile ilgilidir. Dolayısıyla bu kategoriye eklenen konular da genellikle teknik veya temel işlevleri içeren konulardır. Tüm internet trafiğinin temeli olan telekomünikasyon altyapısı, TCP/IP ve DNS gibi internetin çalışmasını sağlayan teknik standartlar ve hizmetler, World Wide Web'i ve diğer internet uygulamalarını ve hizmetlerini etkinleştiren HTML ve XML gibi uygulama/içerik standartları gibi konular buna dahil edilebilir (Kurbalija, 2015, s. 102).

2005'te yayınlanan WGIG Raporu, altyapı ve standardizasyon sepetindeki ana konuları; telekomünikasyon altyapısı, teknik ve web standartları, internet protokol numaraları, alan adı sistemi, kök bölge ve yakınsama olarak kabul etmişti (Kurbalija, 2015, s. 102). Ancak WGIG Raporu'nun yayınlanmasından bu yana, politik tartışmalarda üç yeni internet yönetişimi sorunu ortaya çıkmıştır. Bunlar; ağ tarafsızlığı, bulut bilişim ve nesnelerin internetidir (Kurbalija, 2015, s. 103). Aşağıda bu teknik sorunlar ele alınacaktır.

2.1.1.1.TCP/IP

ABD Savunma Bakanlığı'nın araştırma kolu olan DARPA, TCP/IP modelini 1970'lerde internetten önceki geniş alan ağı olan ARPANET'te kullanılmak üzere yarattı. TCP/IP ilk olarak *Unix* işletim sistemi için tasarlanmış ve kendisinden sonra gelen tüm işletim sistemlerine yerleştirilmiştir (Shacklett & Novotny & Gerwig, 2021). En önemli teknik standart, internet trafiğinin yönlendirilmesi ve adresinin tanımlanması için temel olan İnternet Protokolü'dür (IP) (UNCTAD, 2015, s. 10). İnternete bağlı her nesne,

geleneksel olarak bir IP adresi olan bir sanal tanımlayıcı gerektirir (DeNardis & Raymond, 2017, s. 480). Bir konu, TCP/IP'nin geliştirilmesi, bakımı veya yönetimi ile ilgiliyse, internet yönetişimi içinde sınıflandırılabilir. Ayrıca, TCP/IP tabanlı ağ faaliyetlerine bağlı olan tüm sorunlar da internet yönetişiminin bir parçası olacaktır. IP numaraları, internete bağlı bilgisayarları ve diğer cihazları tanımlamak için kullanılan sayısal adreslerdir. TCP/IP'nin tasarlanmasının esas amacı, fiziksel ağlar üzerinden küresel iletişim hizmetleri sağlayan ağların ara bağlantısını oluşturmaktı. Bu sayede farklı coğrafyalardaki ağlar ile ana bilgisayarlar arasında iletişim sağlanmıştır (IBM, 2006, s. 4). Bunun yanında TCP/IP internetin güçlü yönlerinden birini oluşturmaktadır. Zira TCP/IP gibi teknik standartların telekomünikasyon altyapısından ve uygulama standartlarından bağımsız kalması interneti güçlendirmektedir. Bu bağımsızlık aynı zamanda interneti esnek hale getirmektedir (Kurbalija, 2015, s. 102).

İnternet özellikli cihazların (cep telefonları, kişisel düzenleyiciler, tabletler ve ev aletleri dahil) sayısındaki hızlı artış, IP numaralarına olan talebi artırmıştır. Bu doğrultuda, IP sürüm 6 (IPv6), IP sürüm 4'ün (IPv4) sınırlı sayı havuzunun üstesinden gelmek için oluşturulmuştur (IBM, 2021). Şu anda aktif olarak kullanılan iki tür IP adresi vardır: IPv4 ve IPv6. IPv4 ilk olarak 1 Ocak 1983'te dağıtılmış ve halen en yaygın kullanılan sürümdür. IPv4 adresleri, genellikle 32 bitlik sayılardır (örn; *192.0.2.53*). IPv6 protokolünün dağıtımı ise 1999 yılında başlamıştır. IPv6 adresleri 128 bitlik sayılardır (*2001:0db8:582:ae33::29*) (IANA, t.y.d).

Aşağıdaki bölümlerde daha detaylı olarak inceleyeceğimiz üzere IP numaralarının yönetişimi, IANA tarafından koordine edilirken; TCP'nin kontrolü IETF tarafından yapılmaktadır. IANA, IP numarası bloklarını beş Bölgesel İnternet Tesciline (RIR's) dağıtır. RIR's, IP numaralarını Yerel İnternet Kayıtlarına (LIR's) dağıtır. LIR's ise bu numaraları daha küçük İnternet Servis Sağlayıcılarına (ISP's), şirketlere ve bireylere dağıtır (IANA, t.y.d). 2003 yılında kurulan Sayı Kaynak Organizasyonu (NRO), beş RIR'ın[31] çalışmalarını koordine eder. Adres Destekleme Kuruluşu (ASO) ise, küresel IP adresi politikasını geliştirir ve ICANN Yönetim Kurulu'na tavsiyelerde bulunur (ICANN, t.y.a).

TCP/IP protokolü geniş kabul görmesine rağmen, güvenlik zafiyetleri nedeniyle eleştirilmekte ve bu zafiyetlerin giderilmesi etkin çözüm önerilerini gerektirmektedir.

[31] RIR bölgeleri sırayla; AFRIC, APNIC, ARIN, LACNIC ve RIPE NCC şeklindedir. Ayrıntılı bilgi için bkz: IANA (t.y.). Number Resources. https://www.iana.org/numbers (20.04.2021).

Zira TCP/IP protokolleri, güvenliksiz bir ortamda iletişimi korumak için gerekli olan kimlik doğrulama, bütünlük ve gizlilik mekanizmalarını sağlayamamaktadır. Buna ek olarak, ağları TCP/IP tabanlı saldırılardan korumak için *ad hoc* teknikler geliştirilmiştir. Bu nedenle, TCP/IP güvenliğine yönelik resmi bir yaklaşım eksikliği söz konusudur (Vigna, 2003, s. 914; Pai-zhang, 2010). Bu güvenlik sorunlarını çözmek için TCP/IP'nin üzerine yeni protokoller uygulanması gerekmektedir.

Mevcut IP, geleneksel internet için oldukça uygun olsa da, 5G ve B5G gibi yeni nesil ağlar, robot tabanlı otomasyon, bulut destekli sürüş gibi yeni uygulamalar, IP'nin sunabileceğinden daha fazla veri düzlemi yeteneği gerektirmektedir. Bu nedenle bu ağ teknolojileri için bir değişiklik gereklidir (Li & Makhijani & Dong, 2020, s. 1). Örneğin, IP tabanlı iletişim, IoT uygulamalarında yaygın olarak kullanılacak olması nedeniyle, bu iletişim teknolojilerinin güvenliğinin sağlanması büyük önem taşımaktadır. (Granjal & Monteiro & Silva, 2015, s. 1294). Ayrıca IP, hiyerarşik ve idari olarak atanmış adreslere bağımlılığı nedeniyle uygun olmadığı için eleştirilmektedir. Bu durum, otomatik olarak kendini yönetebilen bir Unmanaged Internet Protocol (UIP) geliştirilmesi gerekliliğini ortaya çıkarmaktadır (Ford, 2004, s. 93).

Tüm bu teknik ve güvenlik sorunlarının yanında IP, politik sorunlara da konu olmaktadır. Zira internetin erken dönemlerinde alan adları ve IP adresleri tek bir kişinin yönetimindeydi ve o zamanlar bu bir sorun teşkil etmiyordu. Ancak internet kullanımının yaygınlaşmasıyla birlikte IP adreslerinin yönetimi daha sistematik ve profesyonel bir hale geldi. Bu evrim, geleneksel ve daha rastgele yönetim biçimlerinin yerini alırken, IP adresi tahsisi konusunda adalet ve mülkiyet gibi iki temel sorunu ön plana çıkardı. Nitekim bugün ABD, IP adreslerinin %40'ına sahipken; Çin, %5'e sahip (Zhang & Liu & Chhachhar, 2020, s. 2308).

Bunun yanında IP adresleri tükenmekte ve bu durum çözülmeyi bekleyen ciddi sorun alanları açmaktadır. Mayıs 2015'te ICANN, IP adreslerinin tükenmek üzere olduğunu açıkladı. Bu durum, 1995'ten beri geliştirilmekte olan ancak yavaş ilerleyen IPv6'ya geçişi tetiklemiş olsa da; IPv6 internet erişim hızını etkilemediğinden bir avantaj sağlamamaktadır. Üstelik IPv4'ten IPv6'ya geçiş karmaşık ve maliyetli bir süreç olduğundan gelişmemiş ülkeler açısından sorun yaratmaktadır. Ancak daha önemli olan sorun, gelecekte IP adreslerinin nasıl tahsis edileceği konusunda net bir çözüm

olmayışı. ITU, ülkelere ücretsiz IP adresi tahsis etmeyi savunsa da, IP adreslerinin mülkiyeti hala tartışmalı bir konu olmaya devam etmektedir (Zhang vd., 2020, s. 2308).

TCP/IP protokolü, internetin gelişiminde hayati bir rol oynamış olmasına rağmen, mevcut ve gelecek teknoloji taleplerini karşılamakta yetersiz kalmaktadır. Güvenlik zafiyetleri, yeni nesil ağlar için yetersiz veri düzlemi yetenekleri ve IP adres yönetimindeki politik ve adaletsiz dağılım, bu protokollerin revize edilmesi veya yenilerinin geliştirilmesi ihtiyacını açıkça ortaya koymaktadır. Gelecekte, daha güvenli, esnek ve adil bir internet için mevcut protokollerin sınırlılıklarını aşan ve teknolojik yeniliklere uyum sağlayabilecek yeni çözümlerin benimsenmesi kaçınılmaz görünmektedir.

2.1.1.2.DNS

Alan Adı Sistemi (DNS) genellikle ana bilgisayar adlarının IP adresleriyle eşleştirilmesini sağlayan “internet adres defteri" olarak tanımlanır. DNS’nin işlevi, internet adlarını almak ve sayısal IP adreslerine dönüştürmektir. İnternete bağlı cihazlar, birbirleriyle iletişim kurmak için IP numaralarını kullanır. DNS adları, bir durdurma (".") ile ayrılmış bir dizi etiket kullanılarak hiyerarşik olarak düzenlenir. Alan adlarında en üst seviye, "kök"ten (*root*) oluşur. Bu kök, .com veya .org gibi üst düzey alanları (TLD) gösterir. Bu TLD'lerin her biri bağımsız olarak uygulanır. Her TLD'nin altında, yine her biri bağımsız olarak uygulanan ikinci düzey alanlar (SLD's) bulunur (İTÜBİDAB, 2013).

DNS, genel (gTLD) ve ülke kodu (ccTLD) olmak üzere iki tür TLD içerir. gTLD'ler sponsorlu (sTLD) veya sponsorsuz olarak nitelendirilir. Sponsorlu olmayan gTLD'ler, .com, .info, .net ve .org gibi herkes tarafından elde edilebilen alanları içerir. sTLD'ler ise belirli bir grupla sınırlıdır ve yalnızca belirli endüstri kayıtlarına açıktır. ccTLD'ler ise belirli ülkeleri veya bölgeleri (.tr, .fr, .uk vb.) belirtmek için kullanılır (UNCTAD, 2015, s. 14).

DNS tasarımı ve üzerinde uygulanan kontrol hakkında bilinmesi gereken, bu konunun sadece teknik bir mesele olmadığı, aynı zamanda politika, siyaset ve düzenlemelerle iç içe geçmiş bir alan olduğudur. Bu sistem, dijital çağda ifade özgürlüğünden gizliliğe kadar pek çok temel değeri şekillendirir. DNS üzerindeki teknik kontrolün ifade özgürlüğü, erişim, mahremiyet, telif hakkı, ticari marka, sorumluluk, çatışma çözümü, rekabet, yenilik ve piyasa yapısını düzenleyen çeşitli politika ve düzenlemelere yol

açabileceği belirtilmektedir. Yani, bir alan üzerindeki kontrol, geniş bir yelpazede sosyal ve yasal sonuçlara sahip olabilir. Hukuk ve politika perspektifinden, bir DNS'nin merkezi mi yoksa merkezi olmayan bir yapıda mı olduğu, kamu veya özel bir kuruluş tarafından kontrol edilip edilmediği ve yapısının ne kadar uyarlanabilir olduğu gibi konular önem arz etmektedir. Bu faktörler, DNS'nin toplumun sosyal değerlerini nasıl koruduğunu, bilgi, kontrol ve sorumluluğu nasıl dağıttığını etkiler (Bechtold, 2003, s. 1243). Bu bağlamda, DNS'nin yönetim şekli, internetin genel işleyişi ve kullanıcılar üzerindeki etkisi açısından kritik bir öneme sahiptir. Özellikle de internet standartları ve tavsiyeleri bu yönetimde belirleyici rol oynamaktadır.

DNS'nin organizasyonu ve yönetimi, internetin nasıl işlediğine dair temel kararları içerir ve bu, ICANN gibi kurumların rolünü ve önemini ortaya koyar. WGIG Nihai Raporu, DNS konusunda önemli bir tartışma zemini sağlamıştır. Tartışmaların çoğu, kritik internet kaynaklarının yönetimi üzerinde ICANN ve ABD Ticaret Bakanlığı'nın (DOC) sorumluluklarının reformuna ilişkindi (Hubbard & Bygrave, 2009, s. 228). Burada gelişmekte olan ülkelerin DNS yönetimi konusunda daha fazla söz sahibi olma çağrıları, küresel internet yönetişimindeki güç dengelerinin yeniden değerlendirilmesine işaret etmektedir. Çin, Suudi Arabistan, İran, Brezilya ve Pakistan da dahil olmak üzere gelişmekte olan ülkelerden oluşan küresel bir grup, WGIG raporunda ele alınan GIC modelini[32] savunmuştur. Diğer taraftan ABD, DNS güvenliğini veya istikrarını etkileyebilecek her türlü değişikliğe kapalı olduğunu ifade etmiştir. ABD hükümeti, 30 Haziran 2005 tarihinde yaptığı bir açıklamada şu ifadeleri kullanmıştır: "İnternetin dünya ekonomisi için önemi düşünüldüğünde, internetin temelindeki DNS'nin istikrarlı ve güvenli kalması çok önemlidir. Bu nedenle ABD, DNS'nin etkili ve verimli çalışmasını olumsuz yönde etkileme potansiyeline sahip hiçbir eylemde bulunmamayı taahhüt eder ve bu nedenle yetkili kök bölge dosyasında değişiklik veya değişikliklere yetki verme konusundaki tarihi rolünü sürdürecektir." (Hubbard & Bygrave, 2009, s. 228). Bu küresel perspektifler çatışması, kök sunucu

[32] WGIG Nihai Raporu, 'Küresel Kamu Politikası ve Gözetimi' konusunda birkaç farklı yaklaşım önermektedir. Bu yaklaşımlardan üçü, mevcut internet yönetim yapısında önemli değişiklikler yapmayı önermektedir. Bu değişiklikler, ya ICANN'in yerine geçecek yeni bir yapıyı ya da ICANN'in görevlerini, şu anda DOC'un sorumluluğunda olan gözetim işlevlerini, yeni bir uluslararası kuruluşa devretmeyi içermektedir. Ancak, bu üç modelden hiçbiri, internet yönetimi üzerine yapılan Tunus Gündemi'nde kabul edilmemiştir. Yine de, WGIG tarafından önerilen bu modeller, hem raporun yayımlandığı dönemde hem de sonrasında yoğun tartışmalara yol açmıştır. Bu modellerden biri, 'Küresel İnternet Konseyi' (GIC) adında, BM bünyesinde kurulacak bir hükümetlerarası kurum önermektedir. Bu yeni konsey, DOC'un uluslararası internet yönetimiyle ilgili mevcut rollerini üstlenecek ve ICANN'in GAC görevlerini devralacaktır (Hubbard & Bygrave, 2009, s. 226).

kontrolü gibi spesifik teknik meselelerin yanı sıra, internet yönetişiminin geleceği üzerinde derinlemesine düşünmeyi gerektirir.

DNS yönetimi, özellikle kök sunucuların kontrolü konusunda, teknik ve politik düzeylerde önemli sorunlara işaret etmektedir. Zhang vd. (2020), küresel internet yönetişiminin IPv4'ten IPv6'ya dönüşümü, DNS yönetiminin ve diğer önemli konuların ele alınması gerektiğini vurguladıkları çalışmalarında kök sunucunun yalnızca belirli ülkelerin kontrolünde olması durumunu eleştirmişlerdir. Sistemin işleyişi için kritik öneme sahip olan kök sunucuları, şu anda tek yetkili olarak ABD'de bulunmaktadır. Aşağıda da değinileceği üzere on üç kök sunucusundan on tanesi ABD'de bulunmaktadır ve tamamı ICANN tarafından yönetilmektedir. Bu durum, internet yönetişimi ve güvenliği açısından bazı endişelere neden olmakta; bir ülkenin kök bölge üzerindeki hakimiyeti, diğer ülkelerin küresel internet bağlantısını kesme kapasitesine sahip olabileceğini işaret etmektedir. Bu, aynı zamanda, siber savaş bağlamında internet altyapısına zarar verme riskini de artırmaktadır. Kök sunucuların kontrolü ve dağılımı üzerine yapılan bu eleştiriler, internetin gelecekteki yönetişimi için önemli değişiklikleri ve düzenlemeleri gündeme getirmekte, bu da siber güvenlik ve uluslararası işbirliği alanlarında yeni stratejilerin belirlenmesini zorunlu kılmaktadır.

2.1.1.3.Kök Bölge

Kök bölge (*root zone*), hiyerarşik olarak organize edilmiş DNS'nin en üst seviyesidir. Kök bölge, tüm üst düzey etki alanlarının bir listesini tutar ve bunları kök sunucular aracılığıyla uygular. Bugün, on üç kök sunucu mevcuttur. Bunlardan on tanesi ABD'de iken; kalan üçü İsveç, Hollanda ve Japonya'da bulunmaktadır (APNIC, 2024). On üç kök sunucunun IP adresleri, alan adlarının DNS aramalarını gerçekleştiren yazılıma yerleştirilmiştir (ITÜBİDB, 2013). Geliştirilen yüzlerce makine, kök sunucu IP adreslerine gönderilen DNS sorgularına "*anycast*"[33] olarak bilinen bir teknikle yanıt verir. On üç kök DNS sunucusundan yedi tanesi anycast teknolojisi kullanmaktadır (Ketenci ve Akın, 2009). Bu teknik, kök bölge verilerine genel erişilebilirlik sağlar (UNCTAD, 2015, s. 16).

[33] Anycast teknolojisi, ağ teknolojilerinde kullanılan bir yönlendirme metodudur. Bu teknik, veri paketlerinin birden fazla alıcıya aynı anda gönderilmesini sağlar fakat bu paketler yalnızca en yakın veya en uygun alıcıya ulaşır. Anycast, aynı IP adresini paylaşan birden fazla sunucunun olduğu bir yapıda çalışır ve gelen istekleri, ağ üzerindeki en uygun konumdaki sunucuya yönlendirir. Anycast'in en bilinen kullanım alanlarından biri, DNS sunucularıdır. DNS sisteminde Anycast sayesinde, kullanıcılar coğrafi olarak kendilerine en yakın DNS sunucusuna yönlendirilir ve bu durum, çözümleme sürelerinin kısalmasına ve dolayısıyla internet erişiminin hızlanmasına yardımcı olur.

On iki bağımsız kuruluş, yukarıda belirtilen on üç kök sunucusunu yönetir.[34] Kök bölgedeki değişiklikler şu anda NTIA tarafından yönetilen sözleşmeye uygun olarak IANA adına ICANN tarafından yönetilmektedir. NTIA, kök bölgede değişiklik yapma prosedürünün uygun bir şekilde izlenmesini ve gözlemlenmesini sağlamaktadır. 1995'te ABD'de kurulan VeriSign ile bir işbirliği içinde kök bölge yönetimi işlevlerini yerine getirmektedir (UNCTAD, 2015, ss. 16-17).

Tüm DNS servisleri kök sunucularıyla iletişim kurar ve domain adreslerinin hangi IP'de çalıştığını belirler. İnternet adresleri ilk olarak ülkelere göre sınıflandırılır. Örneğin, .tr, .de, .uk bunlardan yalnızca birkaçıdır. Ülke ayrımından sonra ise .com, .edu, ve .gov gibi DNS'de üst düzey (*top-level*) domainler yer almaktadır. Kök dosyadan belirli bir girişin silinmesi halinde dosya erişilemez hale gelir. Bu nedenle kök bölgenin yönetimi, küresel internet üzerinde jeopolitik anlamda avantaj ve yetki sağlamaktadır (Budnitskiy, 2018, s. 78). Bu da kök bölge yönetimini, teknik bir işlev olmanın ötesine, yani politik boyuta taşımaktadır.

Kök bölge yönetiminin küresel yönetişim sorunlarından birine dönüşmesi, özellikle Ulusal Güvenlik Ajansı'nın (NSA) gözetim faaliyetlerinin ortaya çıkmasıyla daha da belirginleşmiştir. Bu durum, ABD'nin internet üzerindeki ağırlığının azaltılması gerektiği yönünde uluslararası çağrıları güçlendirmiştir. 2013 yılında Ulusal Güvenlik Ajansı'nın gözetimine dair ifşalara verilen tepkilerle birlikte ABD'nin rolünün azaltılması gerektiği yönündeki savlar güçlendirilmiş oldu (Timberg, 2014). Zira kök bölgeye ve alan adları sistemine yönelik farklı yaklaşımların ana noktası, ICANN aracılığıyla yönetilen kök bölgedeki değişikliklerin idaresinde ABD'nin üstlendiği tarihsel role ilişkindir. Nitekim gelen tepkiler neticesinde ABD hükümeti, IANA sözleşmesi kapsamındaki gözetim sorumluluklarını küresel çok paydaşlı topluluğa devretmeyi amaçladığını duyurmuş, 2016 yılında ise devir işlemi gerçekleşmiştir (UNCTAD, 2015, s. 17; ICANN, t.y.a).

Politik olarak bu hareket, ABD'nin Web'i kontrol ettiği ve dünyanın geri kalanında gözetim sistemlerinden yararlandığı yönündeki küresel kaygıları belli ölçüde hafifletebilmiştir. Ancak ABD'nin bu girişimini destekleyenlerin yanında eleştirenler de olmuştur. Kararı eleştirenler, ICANN'in ABD gözetimi olmadan ve ABD yasalarının sınırlarının ötesinde çalışmaya uygun olup olmadığı konusunda şüphelerini

[34] Ayrıntılı bilgi için bkz: https://root-servers.org/ (25.04.2021).

dile getirmişlerdir (Timberg, 2014). Bu konuda NetChoice'in yönetici direktörü Steve DelBianco, “ICANN'in tüm dünyaya karşı sorumlu olması düşünülemez. Bu, hiç kimseye karşı sorumlu olmamakla eşdeğerdir" ifadesini kullanarak ABD’nin kararını eleştirmiştir (NetChoice, 2014). Zira bu devir, internet yönetişiminde daha demokratik ve çok paydaşlı bir yaklaşımın benimsenmesi açısından kritik bir dönüm noktası olsa da, internet yönetişimindeki ABD etkisini tamamen ortadan kaldırmamıştır. ICANN'in ABD yasaları altında faaliyet göstermeye devam etmesi ve NTIA'nın kök bölge dosyaları üzerindeki nihai yetkisi, ABD'nin hala önemli bir rol oynadığını göstermektedir.

Bugün küresel IP ve DNS tahsisinde merkezi bir rol oynayan ICANN, dolaylı olarak NTIA’ya bağlı kalmaktadır. IANA'nın yönetim devri planı, yetkili kök bölge dosyalarının NTIA standartlarına uygunluğunu vurgulamaktadır. Öte yandan, ITU gibi BM kuruluşları, yeni nesil IP adreslerinin tahsisinde daha etkin bir rol üstlenmeyi ve IP adreslerini ülkeler arasında ücretsiz olarak dağıtmayı savunmaktadır. Bu durum, ICANN'in mevcut tekelini sarsabilecek bir gelişme olarak görülse de, IP adreslerinin mülkiyeti ve tahsis yöntemleri konusundaki tartışmalar hala devam etmektedir (Zhang vd., 2020, s. 2308).

Çin'in şu anda kök isim sunucusu kurma yetkisine sahip olmaması, ülkenin internet altyapısı üzerinde tam kontrol sahibi olamaması anlamına gelir. Bu durum, internet erişimi ve yönetimi konusunda sadece kiralama ve kullanma haklarına sahip olduğunu gösterir. Bu bağlamda kök isim sunucusu sahibi olmak, bir ülkenin internet üzerindeki egemenliğini artırma ve küresel internet yapısındaki etkisini güçlendirme potansiyeline sahiptir. ABD gibi bir ülkenin siber savaşı ulusal savunma yasasına entegre etmesi, siber tehditlere karşı stratejik bir savunma mekanizması oluşturduğunu ve siber uzayı bir savaş alanı olarak kabul ettiğini göstermektedir. Bu çerçevede, kök sunucusunu kontrol eden bir ülkenin siber savaş başlatması durumunda, kök sunucusuna sahip olmayan ülkelerin küresel internet pazarından dışlanma riski bulunmaktadır (Zhang vd., 2020, s. 2309).

Literatürde kök bölge sayısının artırılması ve DNS sisteminin daha güvenilir ve esnek hale getirilmesi yönünde birçok öneri gündeme gelmiştir (Bush vd., 2000; Wang, 2010; Li vd., 2023). Bu öneriler, kök sunucu ağının coğrafi ve operasyonel çeşitliliğini artırarak küresel internet altyapısının dayanıklılığını ve erişilebilirliğini iyileştirmeyi

amaçlamaktadır. Özellikle, tek bir ülkenin kontrolü altında olmayan, daha dağıtık bir kök sunucu yapısının oluşturulması, internetin küresel yönetişimine katkıda bulunabilir. Ayrıca, yeni kök sunucuların eklenmesi, bölgesel internet kesintilerine karşı direncin artırılmasına ve internet erişiminin kesintisiz olarak sürdürülmesine olanak tanır. Bu bağlamda ICANN ve IANA gibi kurumların kök bölge yönetiminde daha fazla uluslararası işbirliği ve katılımcılığı teşvik etmeleri, internetin küresel bir kaynak olarak kalmasını sağlayacak kritik adımlardır.

2.1.1.4.World Wide Web

World Wide Web (WWW), internet üzerinde bulunan hiper metin belgeleri aracılığıyla bilgi alışverişini sağlayan bir bilgi sistemidir. Tim Berners-Lee tarafından 1989'da CERN'de (Avrupa Nükleer Araştırma Merkezi) geliştirilmeye başlanmıştır. WWW, internetin kendisiyle sıkça karıştırılsa da, internetin sadece bir parçasıdır. İnternet, geniş bir ağ altyapısı üzerinde çalışan çeşitli hizmetlerin ve protokollerin bütünüdür; WWW ise bu hizmetlerden bir tanesidir (CERN, t.y.).

İnternet, standartlaştırılmış TCP/IP'yi kullanarak veri alışverişi yapan küresel bilgisayar ağları sistemidir. Dolayısıyla internet, TPC/IP standartlarıyla tanımlanan bir ağdır. İnternet aynı zamanda WWW'nin temelidir ve WWW sadece internet üzerinde çalışır. WWW ise; kaynaklar olarak adlandırılan öğelerin Tekdüzen Kaynak Tanımlayıcıları (URI) adı verilen küresel tanımlayıcılarla anıldığı bir bilgi alanıdır. Dolayısıyla Web bir bilgi alanıdır. Web teknolojileri için ilk üç tanımlayıcı; URL's, HTTP ve HTML olmuştur.

WWW, kullanıcıların web tarayıcıları aracılığıyla erişebildiği web sayfalarından oluşur. Bu sayfalar, HTML (HyperText Markup Language) adı verilen bir işaretleme dilinde yazılmıştır ve sayfalar arası bağlantıları (hyperlinks) kullanarak birbirine bağlanır. Web sayfaları, metin, görsel, video ve ses gibi çeşitli medya türlerini içerebilir. Bilgi paylaşımını, içeriğin görüntülenmesini ve web etkileşimini kolaylaştıran HTML, ana web standardıdır. Çeşitli web uygulamalarının ortaya çıkmasıyla birlikte web standartları, internet uygulamalarının çoğunun içeriklere erişilebilmesini ve düzgün bir şekilde görüntülenebilmesini sağlamıştır. Diğer bir önemli web standardı, internet içeriği için standartların belirlenmesinde esneklik sağlayan Genişletilmiş İşaretleme Dili'dir (XML) (UNCTAD, 2015, s. 11). WWW, 1994 yılında kurulmuş olan W3C tarafından koordine edilmektedir. W3C, Tim

Berners-Lee tarafından yönetilen ana web standardı geliştirme kurumudur ve standartlar, fikir birliği, doğruluk, kamu sorumluluğu ve kaliteyi artırmayı amaçlayan süreçlerle geliştirilir. HTML, CSS, XML gibi diller web standartlarının temelini oluşturur. HTML5, web gelişiminin temel taşı olarak kabul edilir ve W3C'nin standartları, geliştiricilere zengin etkileşimli deneyimler oluşturma imkânı tanır (Kurbalija, 2016, s. 62). W3C, üyeleri arasında büyük teknoloji şirketleri, akademik kurumlar, devlet kurumları ve diğer organizasyonlar bulunan bir konsorsiyumdur. Bu çeşitlilik, web standartlarının geniş bir yelpazedeki ihtiyaç ve gereksinimleri karşılayacak şekilde geliştirilmesini sağlar. W3C ayrıca, topluluk geri bildirimlerini ve açık bir geliştirme sürecini teşvik ederek, web teknolojilerinin evrimine yön verir.

Kurbalija, W3C'nin internete olan yüksek ilgisi göz önüne alındığında, internet yönetişimi tartışmalarında az dikkat çekmesinin şaşırtıcı olduğunu ifade etmiştir (2016, s. 62). Bu durum, W3C'nin daha çok web standartlarının geliştirilmesinin teknik yönlerine odaklanmasından kaynaklı olabilir. İnternet yönetişimi ise daha geniş bir yelpazeyi kapsar ve teknik, politik, ekonomik ve sosyal boyutları içerir. Bu odaklanma farkı, W3C'nin internet yönetişimi tartışmalarında daha az görünür olmasına yol açabilmektedir. Bunun yanında, W3C, web standartlarını geliştirerek internetin daha erişilebilir, etkileşimli ve entegre bir platform haline gelmesini sağlamakla birlikte, bu standartların uygulanması konusunda zorlayıcı bir güce sahip değildir. Kuruluşun çalışmaları, gönüllü katılım ve endüstri desteğine dayanmaktadır. Bu bağlamda W3C'nin internet yönetişimi konusundaki tartışmalarda daha az öne çıkması, faaliyetlerinin doğası ve internet yönetişimi alanındaki geniş katılımcı yelpazesiyle ilgili olabilir.

WWW'nin geliştirilmesi, bilgiye erişimi kolaylaştırarak eğitim, araştırma ve iş dünyasında devrim yaratmıştır. Kullanıcılar artık dünyanın dört bir yanındaki bilgilere hızlı ve kolay bir şekilde erişebilmekte, sosyal medya üzerinden iletişim kurabilmekte, e-ticaret yapabilmekte ve çok daha fazlasını gerçekleştirebilmektedir. Ancak internetin teknik standartlarında olduğu gibi, web standartlarında da teknik rolü olmayan aktörlerin katılımının teşvik edilmesi önem arz etmektedir. Burada ortaya çıkabilecek herhangi bir politik boşluk; insan hakları, rekabet politikası ve güvenlik gibi konularda sorunlara sebebiyet verecektir. Web standartlarının teknik standartlardan çok, internete erişim ve kullanım biçimini şekillendirdiği ifade edilmiştir. Bu nedenle, web

standartlarının teknik olmayan yönler üzerinde teknik standartlardan daha güçlü bir etkisi olduğu iddia edilmektedir (UNCTAD, 2015, s. 12).

2.1.1.5.Blok Zinciri (Blokchain)

İnternet büyüdükçe, geleneksel piyasa koşullarına meydan okumaya başlamıştır. Dolayısıyla özellikle bazı özel kuruluşlar kendilerini bu ekosistemde baskın oyuncular olarak tanıtmışlardır. Bu yaklaşım, merkeziyetsizliği teşvik ederken; blok zinciri tabanlı platformlar dışındaki siyasi ve ekonomik güçleri hesaba katmaması nedeniyle eksik kabul edilmiştir. Bu durum, merkezi iletişim sistemlerinden daha dağıtılmış ve merkezi olmayan bir iletişim ağına geçişi hızlandırmıştır (Filippi & Lavayssière, 2020, ss. 185-187).

Blok zinciri, ilk olarak Bitcoin kripto para birimi için geliştirilmiş, merkezi olmayan bir işlem ve veri yönetimi teknolojisidir (Yli-Huumo vd., 2016, s. 1). Diğer bir deyişle blok zinciri, dağıtılmış ağlarda bilgi alışverişi yapmak ve dijital varlıkları işlemek için geliştirilen teknolojiyi ifade eder (Ølnes vd., 2017, s. 1). IBM (t.y.) blok zincirini; "bir iş ağındaki işlemlerin kaydedilmesi ve varlıkların takip edilmesi sürecini kolaylaştıran, paylaşılan ve üzerinde değişiklik yapılamayan bir büyük defter" olarak tanımlar. Blok zinciri, bir kripto para birimi ağına katılan herkese dağıtılan dijital bir dosyadır ve ağda gerçekleşen tüm işlemleri takip eder. Blok zincirine katılanlar, ağda hangi işlemlerin gerçekleştiğini görmek için blok zincirine bakabilmektedir. Blok zinciri, kimsenin kurcalamaması için kriptografi[35] kullanılarak mühürlenmektedir (USSC, 2018).

Blok zinciri teknolojisine olan ilgi, fikrin ortaya çıktığı 2008 yılından bu yana artmaktadır. Bu teknolojiye olan ilginin nedeni, işlemlerin kontrolünde herhangi bir üçüncü taraf kuruluş olmaksızın güvenlik, anonimlik ve veri bütünlüğü sağlayan ve bu nedenle blok zinciri oluşturan merkezi özellikleridir (Yli-Huumo & Ko & Choi & Park & Smolander, 2017, s. 1). Bitcoin'in 2009 yılında piyasaya sürülmesi, eşler arası (peer-to-peer) bir ağ üzerinden dağıtılan ilk dijital para birimi olarak, bu teknolojinin pratik bir uygulamasını temsil eder. İşlemler, herhangi bir merkez bankası olmaksızın doğrudan bireyler arası gerçekleştirilir. Bu da Bitcoin'i günümüzde en popüler kripto para birimi yapmaktadır (USSC, 2018). Bitcoin bugün, herhangi bir hukuki çerçeveye

[35] Kriptografi, yüksek düzeyde güvenlik sağlayan matematiksel kanıtlar oluşturulmasına imkân tanıyan matematik dalıdır. Bugün e-ticaret ve bankacılık kriptografiyi kullanmaktadır. Bitcoin söz konusu olduğunda kriptografi, herhangi birinin başka bir kullanıcının cüzdanından para harcamasını imkânsız kılmak için kullanılır. Bunun yanında, bir cüzdanı şifrelemek için de kullanılabilmektedir. Böyle bir durumda cüzdan parola olmadan kullanılamaz. Ayrıntılı bilgi için bkz: (Adomey, t.y.).

bağlı kalmadan işlev görmekte ve yeni finansal yapıları ortaya çıkarmaktadır. Düzenleyici mekanizmalardan bağımsız olarak işlem gören bu sanal para birimi, blok zinciri teknolojisinin merkeziyetsiz yapısı sayesinde ortaya çıkmıştır (Avunduk & Aşan, 2018, s. 370). Satoshi Nakamoto'nun bu sistemi tasarlaması, online ödemelerin herhangi bir finansal kuruma ihtiyaç duymadan doğrudan bir taraftan diğerine transferini mümkün kılmıştır. Bu yönüyle blok zinciri, şirketler ve devletlerin kimlik doğrulamaya ve güvene dayalı sistemlerine bir meydan okuma olarak algılanmaktadır (Ølnes & Ubacht & Janssen, 2017, s. 1).

Atzori (2017), finansal piyasalarda devletin hala gerekli olup olmadığını sorguladığı çalışmasında blok zinciri teknolojisinin devlet otoritesi, vatandaşlık ve demokrasinin geleneksel mekanizmalarına meydan okuduğunu ifade etmiştir. Bu bağlamda blok zinciri teknolojisi, merkeziyetten uzaklaşarak işlemlerin güvenliği ve şeffaflığı konusunda yeni bir paradigmaya öncülük etmektedir. Bu süreç, devletin ve merkezi kurumların geleneksel rolünün sorgulanarak mevcut siyasi sistemlerin ve yönetişim modellerinin dahi hızla değişebileceği bir ortam yaratmıştır. Bu yaklaşım, özellikle bu teknolojinin radikal savunucuları tarafından sıklıkla gündeme getirilmektedir. Tekno-özgürlükçüler (techno-libertarians) ve kripto-anarşistler (crypto-anarchists) olarak adlandırılan bu gruplar, devleti gayri meşru ve gereksiz görmektedir. Bu teknolojinin devlet otoritesi karşısındaki "özgürleştirici" gücünü savunmaktadır (Atzori, 2017, s. 4).

Buterin'e göre (2017) merkeziyetsizlik, mimari, politik ve mantıksal olmak üzere üç önemli boyutta ele alınabilir. Mimari boyut, sistemin fiziksel bilgisayar ağı üzerine kurulu olup olmadığı ve bu ağın ne kadarının arıza durumlarında işlevselliğini koruyabildiği ile ilgilidir. Politik boyut, bu bilgisayarların kaç farklı birey veya organizasyon tarafından yönetildiğini değerlendirirken, mantıksal boyut, sistemin tek bir bütün mü yoksa daha dağıtık bir yapı mı olduğunu sorgular. Merkeziyetsizliğin varlığını test etmenin bir yolu, sistemin yarısını elimine ettiğimizde, geriye kalanın bağımsız olarak işleyip işlemediğini kontrol etmektir.

Nakamato'ya göre ise "ihtiyaç duyulan şey, güven yerine kriptografik kanıtlara dayalı bir elektronik ödeme sistemidir ve bu, herhangi iki istekli tarafın güvenilir bir üçüncü tarafa ihtiyaç duymadan doğrudan birbirleriyle işlem yapmasına olanak tanır." (2008, s. 1). Merkeziyetsiz ve aracısız bu teknoloji, herhangi bir güvenilir otoritenin veya aracının müdahalesini gerektirmemesi nedeniyle geleneksel piyasa koşullarına meydan

okumaya başlamıştır (Filippi & Lavayssière, 2020, ss. 186-187). Bu durum, platformları yönetmeyi veya düzenlemeyi daha da zorlaştırmıştır. "Dağıtılmış fikir birliği" kavramına dayanan blok zincir teknolojisi, merkezi bir aracı veya aracıdan geçmeden çok sayıda katılımcıyı koordine etmeyi mümkün kılar. Yine de, ağın yönetiminden ve idaresinden sorumlu herhangi bir aracı operatör olmadan, bu dağıtılmış altyapıların üzerine yerleştirilebilecek bir yönetişim mekanizması belirlemek olukça zordur (Filippi & Lavayssière, 2020, ss. 201-202).

Yönetişim söz konusu olduğunda blok zinciri teknolojisinin en önemli yeniliği, blok zinciri teknolojisinin şeffaf ve hiyerarşik olmayan bir yönetişim modeli sunmuş olmasıdır. Bu teknoloji, merkezi olmayan organizasyonların oluşturulmasına olanak tanıyarak, akıllı sözleşmeler aracılığıyla eşler arası koordinasyonu mümkün kılar. Ancak, zamanla, blok zinciri ağlarının yönetimi giderek daha merkezileşmiş hale gelmiş ve bu teknolojinin yaygınlaşmasını sağlayan birkaç büyük şirket öne çıkmıştır. Bu durum, internetin yönetişim tarihinden alınan dersle, blok zinciri tabanlı ağların yönetimini, gücün dağıtımını koruyacak şekilde düzenlemenin önemini hatırlatmaktadır (Filippi, 2019).

Yönetişimdeki merkeziyetsizliğin altyapıdaki merkeziyetsizlikten farklı olduğu ve merkezi olmayan bir altyapının otomatik olarak merkezi olmayan yönetişimi gerektirmediği belirtilmektedir (Filippi, 2019). Merkezi bir otoritenin eksikliği, sistemin dış müdahalelere açık hale gelmesine neden olabilir (Bauwens, 2009). Bu bağlamda, blok zinciri teknolojisinin sosyal ve politik sonuçları belirsizdir. Teknolojik ademi merkeziyetçilik, daha demokratik bir topluma yol açabilir ya da aksine, birkaç dominant aktör tarafından kontrol edilen daha otoriter bir yapıya dönüşebilir. Neticede internetin evrimi, başlangıçta özgürlük ve özerklik vaadiyle yola çıkıp, sonunda güçlü ekonomik ve politik çıkarlar tarafından domine edilen merkezileşmiş bir yapıya evrildiği gibi, blok zinciri tabanlı sistemlerin de benzer bir yolu izleyebileceği konusunda uyarıda bulunulmaktadır (Filippi, 2019).

Bu yönüyle blok zinciri teknolojisinin ortaya çıkışı ve hızla gelişimi, internet ve finansal piyasalar başta olmak üzere birçok alanda paradigma değişikliklerine yol açmıştır. Bu teknoloji, merkeziyetçilikten uzak, şeffaf ve güvenilir işlem yapısının mümkün olduğunu kanıtlarken, aynı zamanda mevcut ekonomik ve politik yapılar üzerinde ciddi etkiler yaratmıştır. Bitcoin'in piyasaya sürülmesiyle başlayan bu devrim,

merkezi otoritelerin rolünü sorgulamaya ve alternatif yönetişim modellerini gündeme getirmeye devam etmektedir. Blok zinciri, merkezi olmayan bir internetin ve finansal sistemin temelini atarak, kullanıcıların doğrudan ve güvenilir bir şekilde etkileşimde bulunmasına olanak tanımıştır. Ancak, blok zinciri teknolojisinin vaat ettiği merkeziyetsizlik ve özgürleştirici potansiyel, teknolojinin kendisi ve uygulamaları üzerinde artan merkezi kontrol eğilimleriyle dengelemesi gereken zorluklarla karşı karşıyadır. Teknolojinin uygulaması ve yönetişimi konusunda merkeziyetçilik eğilimlerinin ortaya çıkması, blok zincirinin ilk ideallerinin tam olarak gerçekleşip gerçekleşmediği konusunda soruları beraberinde getirmektedir.

2.1.1.6.Yükselen Sorunlar

Siber uzayın yönetişimi, son 50 yıl boyunca önemli bir evrim geçirmiştir. Bu dönüşüm, teknolojinin politik, ekonomik, sosyal ve kültürel etkilerinin derinleşmesiyle daha da karmaşık bir hal almıştır. Özellikle Blok Zinciri, Bulut Bilişim, IoT, Büyük Veri, 5G, AI ve Metaverse gibi yapay zekâ temelli teknolojiler, yeni hizmetler için standartların kim tarafından tanımlanacağı, piyasayı kimin kontrol edeceği ve temel etik ilkelerin teknolojilere nasıl dahil edileceği gibi konuları içeren teknik ve politik bir tartışma zemini meydana getirmiştir (Kleinwächter, 2020). Tartışmaların önemli bir kısmı, AI teknolojilerinin potansiyel etkilerine ilişkin endişelerden kaynaklanmaktadır. Zira AI, küresel yönetişimin yükselen sorunlarından biri haline gelmiştir.

Artık araştırma ve geliştirme faaliyetleri, sadece internetin sunduğu imkanlarla sınırlı kalmayıp, bu alanlara yoğunlaşmaktadır. Google, Facebook, Amazon ve Microsoft gibi büyük internet şirketleri (Big Tech), önemli miktarda veri işleme kapasitelerine sahip olmaları nedeniyle AI alanında öne çıkan oyuncular haline geldi. Bu şirketler, AI araştırmalarına ve geliştirmelerine büyük yatırımlar yapmaya ve AI'yı kendi ürünlerine ve hizmetlerine entegre etmeye başlamışlardır (Kurbalija, 2017). Bu yeni dijital fenomenler, mevcut internet yönetişimi modellerinin ötesine geçen yönetim ve düzenleme ihtiyaçları doğurmakta, bu da özellikle yapay zekanın etiği gibi konularda yoğun tartışmalara yol açmaktadır. Ancak mevcut yönetişim yapısı, bu yeni sorunlara yanıt vermekte yetersiz kalmaktadır (Souter, 2021).

Diğer yandan bulut bilişim, kişisel bilgisayarlar ve yerel sunuculardan "bulut" adı verilen uzak depolama sistemlerine veri saklama sürecini tanımlar ve bu teknoloji, günlük kullanımdan iş dünyasına kadar geniş bir yelpazede uygulama bulur. Google,

Microsoft, Apple, Amazon Web Services ve Facebook gibi teknoloji devleri, bulut ekonomisinde öncü roller üstlenmektedir. Bu alandaki politika meseleleri, bulut hizmetlerine yönelik saldırıları veya bulut faaliyetlerine uygulanan yasalar ve düzenlemeleri içerir ve ulusal düzeyde ele alınması gereken konulardır. Standartlaştırma çabaları, ITU, ISO, IETF ve Avrupa Telekomünikasyon Standartları Enstitüsü (ETSI) gibi kuruluşlar tarafından yönetilir ve bu kuruluşlar bulut bilişim konusunda çalışma grupları oluşturarak etkin bir rol oynarlar. Bulut bilişimin politik boyutları arasında, veri koruma, şifreleme ve gizlilik gibi güvenlik endişeleri öne çıkar; bu bağlamda, bulutta saklanan verilerin güvenliği ve bulut sunucuları arasında iletişimde verilerin korunması kritik öneme sahiptir. (UNCTAD, 2015, s. 19).

İkinci olarak Metaverse; dijital avatarlar aracılığıyla temsil edilen kullanıcıların içinde yaşayacağı ve etkileşimde bulunacağı, geniş çaplı bir sanal evrenin inşası anlamına gelir. Bu yeni evren, sadece içerik izlemenin ötesine geçerek kullanıcıların sanal gerçeklikte etkileşimli bir deneyim yaşamasını sağlar. Ancak bu ileri düzeyde etkileşim ve dijitalleşme, veri güvenliği ve gizlilik konularında önemli zorlukları da beraberinde getirir. Metaverse, diğer bilişim teknolojisi hizmet platformları gibi, kullanıcı verilerinin korunması ve gizlilik ihlallerinin önlenmesi konusunda ciddi sorunlarla karşı karşıyadır. Bu, kullanıcıların kişisel bilgilerinin, etkileşimlerinin ve finansal işlemlerinin sürekli olarak tehdit altında olabileceği anlamına gelir. Bu kavram, özellikle Facebook'un konuya ilgi duymaya başlamasıyla daha da ön plana çıkmıştır. Facebook, elinde bulundurduğu büyük veri havuzu ve milyonlarca kullanıcının metaverilerine sahip olması nedeniyle Metaverse'te önemli bir rol oynama kapasitesine sahiptir. Bu nedenle Facebook'un Metaverse'e olan ilgisi, bireysel sınırlar açısından bazı endişeleri daha da artırmaktadır. Zira Facebook, halihazırda kullanıcıların mahremiyetini korumak konusunda ciddi eleştirilere maruz kalmakta iken; Metavese'in öngörülemez güvenlik ve gizlilik tehditleri, Facebook'a dair endişeleri büyük oranda artırmaktadır.

Üçüncü olarak IoT; internetin fiziksel dünyaya her yerde bulunan sensörler aracılığıyla bağlandığı bir sistemi tanımlamak için kullanılır. IoT kavramı, ilk defa 1999 yılında MIT'de görevli Auto-ID Labs'ın İcra Direktörü Kevin Ashton tarafından kullanılmıştır (Madakam & Ramaswamy & Tripathi, 2015, s. 166). IoT'un yönetişimi, nispeten erken bir aşamadadır. IETF ve IEEE, IoT ile ilgili standartlar geliştirmiştir. ITU ise Nesnelerin İnterneti Küresel Standartlar Girişimi'ne ev sahipliği yapmış ve IoT ile ilgili

konuları ele alan bir Çalışma Grubu kurmuştur. Bölgesel düzeyde ise AB'nin bu konuda çalışmaları mevcuttur. IGF'de ise bu konu Dinamik Koalisyon tarafından ele alınmaktadır (UNCTAD, 2015, s. 21).

Avrupa Komisyonu, en başından beri IoT'un yönetişimi üzerinde durmuştur. Esasen Komisyon'un bu çabası, ICANN'e tam olarak bağımlı olmayan yeni bir rejim kurma isteğinin bir yansıması idi. Giderek daha fazla cihazın entegre edildiği bu sistem, teknik açıdan ayrıntılı olarak tartışılırken, herhangi bir yasal çerçeveye sahip değildir. IoT için bir yönetişim çerçevesi oluşturmaya çalışan ilk ulusüstü organizasyon, Avrupa Komisyonu olmuştur (Weber, 2010, s. 26). Ancak bu teknoloji üzerindeki düzenleme çabaları da yanıtsız kalmaktadır (Souter, 2021). Öyle ki, buna yönelik atılan birtakım adımlar dahi yetersiz kaldığı gerekçesiyle eleştirilere tabi tutulmaktadır. Örneğin; Başkan Trump'ın 11 Mayıs 2017'de yayınladığı siber güvenlik yürütme emri, devlet hizmetlerinin buluta taşınması, NIST Çerçevesi en iyi uygulamalarının benimsenmesi ve kritik altyapının korunmasına yönelik planların geliştirilmesi gibi stratejileri içermesine rağmen, IoT güvenliği, veri ihlalleri ve güvenlik açıklarının sorumlu şekilde ifşa edilmesi gibi önemli sorunları ele almadığı için eleştirilmiştir. Bu eksikliklerin, ABD'nin siber güvenliğine ve küresel siber istikrarına zarar verebilecek ciddi sonuçlara yol açabileceği ifade edilmiştir (Kurbalija, 2017). Dolayısıyla bu alandaki çabaların baltalanması, yönetişim mekanizmasının oluşturulması önünde engel teşkil etmektedir.

Netice itibariyle bulut bilişim, Metaverse ve IoT gibi yükselen teknolojiler, siber uzayın yönetişimiyle ilgili var olan sorunların derinleşmesine sebebiyet vermektedir. Bu teknolojilerle ilişkili veri koruma, şifreleme, gizlilik ve güvenlik gibi kaygılar, siber uzayın yönetişimi tartışmalarının gündemine yerleşmiştir. Avrupa Komisyonu'nun IoT yönetişimine odaklanması ve yeni bir yönetişim rejimi oluşturma çabaları, bu ihtiyacın farkında olunduğunun bir göstergesidir. Ancak, mevcut yönetişim yapısının bu yeni sorunlara yeterli yanıtlar verememesi ve atılan adımların yetersiz kalması, siber uzayın yönetişimi konusunda ciddi endişeler yaratmaktadır. Üstelik bu yeni teknolojilerin ortaya çıkardığı sorunların yanı sıra; etik, güvenlik ve gizlilik üzerindeki etkileri ayrıca bir yönetişim krizi yaratmaktadır. Bu noktada uluslararası işbirliğinin güçlendirilmesi, standartların belirlenmesi ve etik ilkelerin teknolojilere entegre edilmesi yönünde ortak bir çaba, bu sorunların etkin bir şekilde yönetilmesi için elzemdir. Bu nedenle oluşturulacak yönetişim yapısının sürekli gelişen teknolojilere ve bu teknolojilerin

beraberinde getirdiği yeni sorunlara hızlı ve etkili yanıt verebilecek, esnek ve dinamik bir yapıda olması gerektiği görülmektedir.

2.1.2. Politik Sorun Alanları

Yukarıda detaylı bir biçimde incelediğimiz internetin teknik standartları, internetin işleyişini desteklemeleri nedeniyle diğer kamu politikası konularını da etkilemektedir. Örneğin; internet kullanımı nasıl gerçekleştirilmektedir? Dijital sistemler güvenli bir şekilde korunmakta mıdır? İnternet kullanımında insan hakları güvence altına alınmakta mıdır? Bütün bu sorular, dijital sistemlerin kullanımında mülkiyet hakları, veri koruma, ifade özgürlüğü ve gizlilik gibi kamu politikasını içeren konuları gündeme getirmektedir. Bu sorular, internetin sadece teknik bir altyapıdan ibaret olmadığını, aynı zamanda geniş kapsamlı sosyal, ekonomik ve politik etkileşimlerin merkezi olduğunu göstermektedir. Özellikle internet erişiminin ve kullanımının bireysel özgürlükler ve toplumsal gelişim üzerindeki doğrudan etkileri, bu konuları kamu politikasının merkezine taşımıştır.

Bu politik sorun alanları, internetin yönetişimi ve kullanımıyla ilgili geniş kapsamlı tartışmaları beraberinde getirmekte, bireylerin, devletlerin ve uluslararası kuruluşların bu konulara yönelik politikalarını şekillendirmekte önemli bir rol oynamaktadır. Dolayısıyla, internet teknik standartlarının ötesine geçerek sosyal, politik ve ekonomik yaşamın her alanını derinden etkileyen bir araç haline gelmiştir. Bu nedenle, küresel internet yönetişimi konusunda kapsayıcı, adil ve etkili politikaların geliştirilmesi, günümüzün en acil ihtiyaçlarından biri olarak öne çıkmaktadır. Bu konuların incelenmesi, internetin kamu politikası üzerindeki etkilerini daha iyi anlamamıza yardımcı olacaktır. Aşağıda; güvenlik sorunları, insan hakları sorunları ve diğer sosyo-politik sorunlar detaylı bir şekilde ele alınacaktır. Bu analiz, internetin sosyal, politik ve ekonomik boyutları arasındaki karmaşık ilişkileri ortaya koymak açısından önem arz etmektedir.

2.1.2.1. Güvenlik Sorunları

Güvenlik, ilk olarak dijital yönetişim sorunlarının sınıflandırmasında altyapı ve standardizasyon sepetinin bir parçası olarak kabul edilmiştir. Ancak 2014'te yapılan

revizyon neticesinde güvenlik, ayrı bir sepet olarak tanıtılmıştır.[36] Güvenlik sepeti şu konuları içerir: siber güvenlik, siber suç, siber çatışmalar, online çocuk güvenliği, şifreleme, spam, kritik bilgi altyapısının bir parçası olarak internet ve dijital imzalar (Kurbalija, 2015, s. 103).

Siber güvenlik ve siber suçlar, bu alanın iki temel sütununu oluşturmaktadır. Siber güvenlik ve siber suçlar, internet yönetişimi tartışmalarında kritik bir öneme sahip olan iki temel sütun olarak karşımıza çıkmaktadır. Bu bağlamda, siber güvenlik, bireylerin, kurumların ve devletlerin dijital ortamda karşılaştıkları tehditlere karşı korunmasını hedeflerken, siber suçlar ise bu dijital ortamda işlenen yasa dışı faaliyetleri ifade etmektedir. Aşağıda güvenliğin bu iki sütununun yarattığı yönetişim sorunlarına değinilecektir.

i. Siber Güvenlik

İnternet, başta akademisyenlerden oluşan kapalı bir çevre tarafından güvenlik kaygısı olmaksızın kullanılıyordu. Ancak internet kullanıcılarının hızla genişlemesi nedeniyle teknoloji hem kritik hem de tehditkâr hale geldi. Dahası, bilimsel ve teknolojik gelişmeler, "güvenlik" kavramının boyutunda değişiklikler yarattı. Bunun üzerine siber güvenlik, bütün aktörler için önemli hale geldi (Vedder vd., 2019, s. 263). 1995 yılında ABD Merkezi İstihbarat Teşkilatı ve Savunma Bakanlığı, "Bilgi sistemleri ve ağların güvenliği, bu on yılın ve muhtemelen gelecek yüzyılın en büyük güvenlik sorunudur" ifadesini belirten ortak bir basın açıklaması yayınladı. Bu açıklama, o dönemde internetin güvenlik açısından giderek artan bir tehdit olarak algılandığını göstermiştir (Deibert, 2002, s. 115). Bu algıdaki artışın temelinde, toplumların ağ bağlantılı bilgi altyapılarına olan bağımlılıklarının artması ve bu nedenle elektronik felaketlere karşı daha savunmasız hale gelmeleri yatmaktadır. Bu potansiyel felaketler, elektrik şebekelerinin çökmesi, finansal sistemlerin bozulması veya kritik altyapıların devre dışı bırakılması gibi çeşitli şekillerde ortaya çıkabilmektedir. Bu bağlamda, 1995'teki açıklama, bilgi sistemleri ve ağ güvenliği konusundaki önemli bir dönüm noktasını temsil etmiştir.

Yirmi birinci yüzyıla gelindiğinde ise ekonomik, politik ve sosyal faaliyetlerin büyük çoğunluğu, cihazlar ve ağlar aracılığıyla gerçekleştiği görülmektedir. Bu durum, sosyal

[36] Bunda Edward Snowden'ın 2013 yılında başladığı ifşaat faaliyetleri etkili olmuştur. Zira Snowden'ın ifşaatları, siber güvenliğin önemini arttırmış ve devletlerin bu konudaki eğilimini güçlendirmiştir (Kurbalija, 2015, s. 103).

hayattan küresel piyasalara, siyasi kurumlardan kültürel faaliyetlere kadar pek çok alanın işleyişini etkilemektedir. Dolayısıyla bunların korunması, bütün aktörler için önem arz etmektedir. Bu noktada ortaya çıkan ve önemi anlaşılan siber güvenlik, internet yönetişiminin önemli sorun alanlarından birini oluşturmuştur (Eggenschwiler, 2019, s. 81).

Siber güvenlik, kullanıcıların, ağların ve verilerin kötü niyetli saldırılardan korunmasını içerir. Küresel çapta neredeyse bütün aktörler, giderek artan siber tehditlere karşı koymak için çeşitli stratejiler geliştirmektedir. Bu bağlamda, uluslararası güvenlik ve ekonomik istikrarı doğrudan etkileyen siber güvenlik, büyük bir öncelik haline gelmiştir. Devletin siber güvenlik politikalarına yaklaşımı, 2007 yılından itibaren önemli bir dönüşüm geçirmiştir. Bu dönem, siber saldırıların ve bilgi güvenliği ihlallerinin, teknik bir zorluktan çok, ulusal güvenliğin bir parçası olarak değerlendirilmeye başlandığı bir dönüm noktasını işaret eder. Bu değişiklikle birlikte siber güvenlik, siyasi gündemde daha üst sıralara tırmanmış ve çok daha geniş bir politika yelpazesine entegre olmuştur (Globe, 2020, s. 10).

Kurbalija'ya göre siber güvenlik yönetişimi, siber yönetişim politikası konularını içeren yedi sepetten birini oluşturur ve siber çatışmalar, siber suç, siber terörizm ve kritik kaynakların koruması ve düzenlenmesi gibi konuları içermektedir (2009, ss. 61-64). Benzer şekilde DeNardis ve Raymond, siber güvenlik yönetişiminin, internet yönetişiminin temel altyapılarını güvence altına alma zorluğundan doğan alanlardan biri olduğunu ifade etmişlerdir. Siber güvenlik yönetişimi alanına giren konular genel anlamda şu şekildedir: ağ altyapısının güvenliğini sağlamak; şifreleme standartlarını tasarlamak; yazılım güvenlik açıklarını düzeltmek; adresleme ve DNS güvenliğini sağlamak; güvenlik sorunlarına yanıt vermek ve kimlik doğrulama işlemlerini onaylamak (Raymond & DeNardis, 2015, s. 588).

Hansen ve Nissbaum'a göre siber güvenlik, geleneksel güvenlik sektörlerinden farklı olarak kendine özgü tehditler ve referans nesneler dizisi ile karakterize edilir. Bu tehditler, geleneksel güvenlik sektörlerinde görülen tehditlerden farklıdır ve siber alanın kendine özgü özelliklerinden kaynaklanmaktadır. Örneğin, siber saldırılar, fiziksel dünyayı etkilemeyen ancak ekonomik ve toplumsal zararlara yol açabilen bilgi ve sistemlere yöneliktir (2009, s. 1165). Esasen siber güvenlik, hem teknik terimler (bilgisayar/sistem/veri güvenliği, bilgi güvenliği) hem de uluslararası ilişkiler, kriz

yönetimi ve kamu güvenliği gibi alanlarda artan bir şekilde atıfta bulunulan bir kavramdır (Veale & Brown, 2020, s. 4). Ancak siber güvenlik, sadece yazılım, donanım ve veri kaynaklarının korunmasını değil, aynı zamanda mobil teknolojilerin hızlı gelişimi ve mobil uygulamaların yaygınlaşmasıyla birlikte akıllı telefonlar gibi cihazların güvenliğini de içerir (Zhang vd., 2018). Ayrıca, siber güvenlik alanında yapay zekâ kullanımı da dikkat çekmektedir. Siber suçlarla mücadelede yapay zekâ tabanlı yöntemler, modern teknolojilerin siber güvenliği sağlamada önemli bir rol oynayabileceğini göstermektedir (Mijwil et al., 2023, s. 65).

Bu yönüyle siber güvenlik; siber suç ve siber çatışmalar dahil olmak üzere çeşitli alanları kapsayan bir şemsiye kavramdır (UNCTAD, 2015, ss. 21-22). Dolayısıyla siber güvenlik yönetişimi de sosyal, politik ve ekonomik sonuçları olan çok boyutlu bir yapıdır. Teknik, sosyo-politik ve ekonomik etkilerin tamamı hesaba katıldığında, siber güvenlik için tek bir yönetişim yapısının olmadığı sonucuna varılabilir. Tek bir yönetişim modeli, siber güvenliğin tüm farklı yönlerini etkili bir şekilde ele almaktan yoksundur. Siber güvenliğin farklı yönlerini kimin yönettiği alana göre değişiklik göstermektedir. Örneğin bazı alanları teknik uzmanlar yönetirken, diğer alanları devlet kurumları yönetmektedir. Benzer şekilde bazı alanları düzenleyici kurumlar yönetirken, bazı alanların yönetimi kullanıcıların elindedir (Dutton & Peltu, 2007, s. 26). Nitekim siber güvenlik yönetişimi, çok sayıda aktörü içermekte ve bu durum farklı işbirliği sorunlarını gündeme getirmektedir. Buna rağmen paydaşlar, etkili güvenlik mekanizmaları geliştirmeye çalışmaktadır.

Ulusal düzeyde çok sayıda ülke, siber suçla mücadeleye odaklanarak kritik bilgi altyapısını siber saldırılara karşı korumaya çalışmaktadır. Bölgesel düzeyde ise çok sayıda kuruluş, siber güvenliğin öneminin farkına varmış ve bununla ilgili stratejiler, öneriler ve sözleşmeler üzerinde çalışmıştır. Bunun yanında, siber güvenliği sürdürmek ve geliştirmek için bölgesel düzeyde düzenleme ve politikaların uygulanmasına yönelik çabalar da mevcuttur. Bölgesel düzeyde Avrupa Konseyi, 2004 tarihli Siber Suçlar Sözleşmesi aracılığıyla siber güvenliği ele almıştır. 2003 yılında, OAS, Amerikalılar Arası Siber Güvenlik Stratejisini oluşturmuştur. Afrika'da siber güvenlik politikası, Afrika Birliği Siber Güvenlik ve Kişisel Verilerin Korunması Sözleşmesi'nin taslağının hazırlanmasına odaklanmıştır (IFLA, t.y.a, s. 6). NATO ise, 2014 yılında bir Siber Savunma Politikası kabul etmiştir (CCDCOE, t.y.a).

Uluslararası düzeyde BM'nin 2004'ten beri görevlendirdiği GGE'ler, siber alandan gelen mevcut ve potansiyel tehditleri önlemeye yönelik işbirlikçi yaklaşımlar benimsemektedir. BM Uyuşturucu ve Suç Ofisi (UNODC) siber suçlarla mücadelede de oldukça aktiftir. WSIS 2005 gündeminin bir sonucu olarak, ITU, Küresel Siber Güvenlik Gündemi (GCA) ve Küresel Siber Güvenlik Endeksi (GCI) gibi kuruluşlar da siber güvenlik konusunda çeşitli faaliyetler başlatmıştır (IFLA, t.y.a, s. 6). Bunun yanında ITU, GCA kapsamında, Çocukların Online Korunması ve ITU-IMPACT Ortaklığı gibi girişimleri teşvik etmiştir (UNCTAD, 2015, s. 22). ITU, GCI 2020 raporunda, COVID-19 salgını ile birlikte ekonominin, toplumun ve devletin dijital sistemlere daha çok entegre olduğunu ve bu durumun siber güvenliğin "öncelikli" olarak konumlandırılmasını beraberinde getirdiğini ifade etmiştir (ITU, 2020a, s. 1).

Siber uzayın güvenliğinde önemli roller üstlenen bir dizi özel kuruluş da bulunmaktadır. Bu kuruluşlar arasında büyük ticari çokuluslu şirketler, sivil toplum kuruluşları, özel güvenlik firmaları ve bağımsız gruplar yer alır. Örnek olarak, Microsoft, Google ve Symantec gibi büyük teknoloji şirketleri; bu şirketler siber güvenlik alanında çözümler ve hizmetler sunarak önemli bir rol oynarlar. Ayrıca, bilgisayar acil müdahale ekipleri (CERT'ler) gibi sivil toplum kuruluşları, siber saldırılara hızlı ve etkin bir şekilde yanıt vermek için hayati öneme sahiptir. Spamhaus ve Kimlik Avı Önleme Çalışma Grubu gibi gruplar, siber dolandırıcılık ve kimlik hırsızlığı gibi siber suçlarla mücadelede kritik işlevler görürler. Hibrit kuruluşlar, örneğin Sanal Küresel Görev Gücü ve Çocuk Fuhuşuna Son, Çocuk Pornografisi ve Cinsel Amaçlı Çocuk Ticareti (ECPAT) gibi, online çocuk istismarına karşı mücadelede öne çıkarlar. Ayrıca, Siber Melekler gibi bağımsız, 'serbest' gruplar ve geçici kolektifler, siber uzayda devriye gezip araştırma yaparak önemli katkılarda bulunurlar (Chang & Grabosky, 2017, s. 534).

Bütün bu girişimlere rağmen siber alanın sınır ötesi doğası, hızı ve hacmi siber güvenlik sorunlarıyla mücadelede zorluklar meydana getirmektedir. Bu bağlamda siber güvenlik ihlali yapanların tespiti, soruşturulması ve yargılanması da zorlu bir süreç olarak karşımıza çıkmaktadır. Siber güvenliğe yönelik uluslararası bir çerçevenin oluşturulmasına yönelik talep olsa da bu konuda bir fikir birliğine varılmamıştır. Ayrıca, siber güvenlik konularında çok taraflı ve çok paydaşlı işbirliği ve koordinasyon için çağrılar yapılsa da genellikle yapılan girişimler ulusal mahiyette olmaktadır.

ii. Siber Güvenlikleştirme

İnternet, 1989 yılında siyasallaşmadan başladı (Pew Research Center, 2014). Bu dönemde internet, üniversiteler ve araştırma enstitüleri arasındaki bilgi paylaşımı için kullanılan bir araçtı. İnternet, kamusal tartışmanın bir parçası değildi ve siyasi kararlardan etkilenmiyordu. İnternetin siyasallaşması ise 1990'lı yıllarda daha da hızlandı. Bu dönemde, internet kullanımının yaygınlaşması ve internet teknolojilerinin gelişmesi, internetin siyasi bir araç olarak kullanılmasına olanak sağladı. Bu dönemde, internet, devletler ve şirketler tarafından giderek daha fazla benimsendi. Aynı zamanda, internetin potansiyel tehditleri de giderek daha fazla tartışılmaya başlandı. Örneğin, internetin siber saldırılar, veri ihlalleri ve terörizm için bir araç olarak kullanılabileceği endişeleri dile getirilmeye başlandı.

İnternetin bir tehdit unsuru olarak algılanmaya başlaması, onu bir güvenlik nesnesi haline dönüştürdü. Dolayısıyla bu durum, internetin güvenlikleştirilmesine yol açtı. İnternet, varoluşsal bir tehdit olarak sunuldu ve normal siyasi prosedürlerin sınırları dışında gerekçelendirilen güvenlik önlemleri gerektirdiği iddia edildi. Bu önlemler arasında, siber güvenlik yasaları ve düzenlemeleri, siber güvenlik altyapısının geliştirilmesi ve siber güvenlik farkındalığının artırılması yer aldı. Özellikle, Çin hükümetinin "güvenlik duvarı" oluşturma çabaları, ABD hükümetinin gelişmiş şifreleme teknolojilerinin yayılmasını sınırlama gibi girişimleri interneti güvenlikleştirmek adına atılan adımlar olarak nitelendirilmiştir (Deibert, 2002, s. 116).

2000'li yılların sonlarına gelindiğinde ise internet, son derece siyasallaşmış bir yönetişim nesnesi haline geldi (Hösl, 2019, s. 1). İnternetin siyasi kampanyalarda kullanımı, ilk kez 1996 yılındaki ABD başkanlık seçimlerinde Bill Clinton'ın adayı Bob Dale tarafından olmuştur (Harbath & Fernekes, 2022). Bu bağlamda güvenlikleştirme teorisi, siber uzayın yönetişimini anlamak için giderek daha önemli bir araç haline gelmektedir. Güvenlikleştirme teorisi, bir sorunun bir güvenlik sorunu olarak tanımlanmasını ve bu sorunu çözmek için belirli politikaların benimsenmesini inceleyen bir teoridir. Güvenlikleştirme teorisine göre, bir meselenin güvenlikleştirilmesi, bir söylem süreci yoluyla gerçekleşir. Bu süreçte, bir mesele, varoluşsal bir tehdit olarak sunularak, normal siyasi prosedürlerin sınırları dışında gerekçelendirilen güvenlik önlemleri gerektirir. İnternetin güvenlikleştirilmesi de bu bağlamda ele alınabilir.

Tablo 1. Siber Güvenliğin Tarihsel Evrimi ve Güvenlikleştirme

	Tehdit Türleri	Siber Güvenlikte Yenilikler ve Gelişmeler	Güvenlikleştirme Açısından Önemi
1960'lar	İlk bilgisayar korsanlığı faaliyetleri	Bilgisayar korsanlığının farkındalığı arttı	Siber güvenliğin temellerinin atılması
1970'ler	İlk bilgisayar virüsleri ve solucanları	Antivirüs yazılımlarının geliştirilmesi	Tehditlerin çeşitliliğinin ve savunma mekanizmalarının öneminin anlaşılması
1980'ler	ARPANET'e saldırılar	Ağ güvenliğine yönelik ilk protokoller ve savunma stratejileri	Siber alanın savaş alanı olarak potansiyeli
1990'lar	İnternetin yaygınlaşmasıyla artan siber saldırılar	Güvenlik duvarları, şifreleme teknikleri gibi savunma mekanizmalarının geliştirilmesi	Siber güvenlik farkındalığının ve önlemlerin geniş kitlelere yayılması
2000'ler	Büyük ölçekli veri ihlalleri	Gelişmiş tehdit tespit sistemleri, veri koruma kanunları	Bireylerin ve kurumların veri koruma bilincinin artması
2010'lar	Siber savaş, siber casusluk	Ulusal siber güvenlik stratejileri, uluslararası işbirlikleri	Siber güvenliğin ulusal ve uluslararası güvenlik politikalarında merkezi bir yer edinmesi
2020'ler	Yapay zekâ destekli tehditler ve savunmalar	Yapay zekâ ve makine öğrenimi tabanlı güvenlik çözümleri	Yapay zekanın siber güvenlikteki rolünün artması ve yeni nesil tehditlere karşı savunma

Kaynak: Tablo, yazar tarafından oluşturulmuştur.

Yukarıdaki tablo, 1960'lardan günümüze kadar siber güvenlik alanındaki önemli dönüm noktalarını ve bu dönemlerde ortaya çıkan tehdit türlerini, yanıt olarak geliştirilen yenilikler ve güvenlikleştirme teorisi açısından incelemektedir. Tablo, siber güvenlik uygulamalarının ve teorilerinin nasıl evrildiğini, her on yılın kendine has zorluklarına nasıl yanıt verildiğini ve bu süreçte siber güvenlik farkındalığının, teknolojilerin ve politikaların nasıl ilerlediğini göstermektedir. 1960'lardaki basit bilgisayar korsanlığı faaliyetlerinden 2020'lerin yapay zekâ destekli tehditlerine kadar uzanan geniş bir yelpazede, siber güvenlik alanında karşılaşılan tehditlerin karmaşıklığının ve çeşitliliğinin arttığı görülmektedir. Aynı zamanda, siber güvenlik stratejilerinin ve teknolojilerinin de bu tehditlere karşı daha sofistike hale geldiği açıktır. Bu evrimsel süreç, siber güvenliğin sadece teknik bir mesele olmaktan çıkıp, ulusal ve uluslararası güvenlik politikalarının merkezine yerleştiğini de göstermektedir.

Siber alanın ve internetin güvenlikleştirilmesi, ulusal güvenlik, ekonomik kalkınma ve küresel liderlik açısından giderek daha fazla önem kazanmaktadır. Bu bağlamda, çatışmaların ve siber uzaydaki tartışmalı konuların çözümü, kuralların oluşturulması ve düzenlemelerin geliştirilmesini gerektirir. Ramich ve Piskunov (2022), siber uzayın güvenlikleştirilmesi sürecini siber uzayın "tam teşekküllü bir politik alan haline geldiği" ve dijital egemenliğin baskın geldiği bir ortama işaret ederek tasvir etmektedir. Bu bağlamda güvenlikleştirme süreci, devletlerin yalnızca kendi dijital sınırlarını koruma çabalarını tetiklemektedir.

Halbuki siber alan, negatif bir güvenlik algısının hâkim olamayacağı kadar uluslararasılaşmış bir alandır. Bu nedenle, uluslararası işbirliği ve norm oluşturma çabaları ile dengelenmesi gereken bir alandır. Bu durum, internetin küresel mahiyetine uygun, esnek ve dinamik bir yönetişim modelinin gerekliliğini bir kez daha ortaya koymaktadır. Zira siber güvenlik, teknolojinin hızla ilerlediği ve internetin hayatımızın her alanına nüfuz ettiği bir dönemde, uluslararası güvenliğin en önemli unsurlarından biri haline gelmişken; bu alanın güvenlikleştirilmesi sorunu, çok daha büyük yönetişim krizlerine sebebiyet vermektedir. Başlangıcından itibaren internet, basit bir bilgi alışverişi aracından, küresel politik kampanyaların ve sosyo-ekonomik etkileşimlerin merkez üssü haline gelmiştir. Bu dönüşüm, siber güvenlik yönetişimi üzerinde derin etkiler bırakmıştır ve siber güvenlik yönetişiminin sadece teknik bir mesele olmadığını, aynı zamanda politik, sosyal ve ekonomik boyutları da barındırdığını göstermiştir. Örneğin, Çin'in "güvenlik duvarı" oluşturma çabaları ve ABD'nin gelişmiş şifreleme teknolojilerinin yayılmasını kısıtlama girişimleri, ulusal güvenlik ile bireysel özgürlükler arasındaki hassas dengeyi sağlama konusundaki zorlukları ortaya koymaktadır. Bu kapsamda, güvenlikleştirme girişimleri ve internetin politikleşmesi, alanın dar bir çerçevede yorumlanmasına ve diğer sorun alanlarının göz ardı edilmesine yol açmaktadır. Bu nedenle siber güvenlik politikalarının geliştirilmesi ve uygulanması sürecinde esneklik, çok yönlülük ve uluslararası işbirliğine dayalı bir yaklaşımın gerekliliği açıktır.

iii. Siber Suçlar

Günümüzde uluslararası barış ve güvenliğe yönelik en büyük tehditler, yalnızca ordular tarafından önlenebilecek veya hafifletilebilecek fiziksel tehditler değildir. Teknolojideki ilerlemeler, internetin icadı ve yaygın kullanımıyla birlikte, tüm ulus devletlere karşı devletlerin sahip olduğu kara, deniz veya hava birliklerinin

yenemeyeceği bir tehdit ortaya çıktı: Siber suç ve tehditler. Siber suçlar, ağ bağlantılı teknolojik bir cihazda meydana gelen yasa dışı faaliyetlerdir. Bu suçlar arasında siber saldırılar, gasp, taciz, kara para aklama ve bilgisayar korsanlığı gibi suçlar yer alır. Son derece sofistike ve her geçen gün gelişen siber uzayda suçların artması kaçınılmazdır. BİT giderek aktörler tarafından bir tehdit olarak algılanmaktadır. Siber suçların yaygınlaşması ve bunlara yönelik geliştirilebilecek caydırıcı mekanizmaların yokluğu, bu algıyı derinleştirmektedir (Duberry, 2019, s. 4). Dağıtılmış Hizmet Reddi (DDoS) saldırıları veya diğer kötü amaçlı yazılım saldırıları (solucanlar, virüsler, fidye yazılımları, casus yazılımlar gibi) ciddi zarar ve maliyetlere sebebiyet vermektedir (Eggenschwiler, 2019, s. 82).

ABD Siber Güvenlik ve Altyapı Güvenliği Ajansı (CISA), Şubat 2021 ile Şubat 2022 arasında siber suç vakalarında yıllık %62 oranında artış bildirmiştir (Morgan, 2020). Siber saldırılar, dolandırıcılık, kimlik avı, siber fidyecilik gibi faaliyetler günden güne artış göstermektedir. Özellikle Covid-19'un yarattığı dijital entegrasyon, siber suçlular için ciddi bir zemin hazırlamıştır. Online çalışmaya geçişle birlikte siber suçluların zayıf hedefleri bulma ve bunlardan yararlanma fırsatı artış göstermiştir. Verilere baktığımızda, 2020'de gerçekleşen kötü amaçlı yazılım saldırıları, 2019'a kıyasla %358 artış göstermiştir. 2021 yılına kadar küresel olarak siber saldırılar %125 artış gösterirken, 2022'de yükseliş trendinin devam etmiştir (AAG, 2022). Cybersecurity Ventures, küresel siber suç maliyetlerinin 2025 yılına kadar yıllık 10,5 trilyon ABD dolarına ulaşmasını bekliyor (Morgan, 2020).

Bu suçlar, giderek daha fazla ulusötesi hale gelmektedir (DCAF, 2019, s. 18). Bu nedenle uluslararası işbirliğini ve etkin yasal çerçevelerin oluşturulmasını zorunlu kılmaktadır. Ancak internetin sınırsızlığı nedeniyle giderek artan bu suçların ortadan kaldırılması veya sınırlanması, özel müdahaleler gerektirmektedir. Zira bugün herhangi bir internet kullanıcısı, kendi ülkesinin sınırları dışında dahi siber operasyonlar yürütebilmekte ve bu durum diğer devletler tarafından tehlike arz etmektedir. Dolayısıyla bu durum, siber suç ve tehditleri ulusal sorunlar olmaktan çıkarıp onları uluslararası veya küresel sorunlar haline getirmektedir. Siber suçların bazı durumlarda küresel olması nedeniyle, bu suçların ortaya çıktığı alan olan siber alan veya dijital ortamın yönetişiminin veya kontrolünün nasıl sağlanacağı da küresel bir soruna dönüşmüştür.

Siber alanın sınır ötesi doğası, online suçların tespiti ve kanun yaptırımı konusunda zorluklar ortaya çıkarmaktadır. Siber suçlara ilişkin güvenilir istatistik ve verilerin eksikliği, siber suç faaliyetlerini tetiklemektedir. Bu alandaki politika boşluğu, ortak veya geniş çapta kabul gören bir siber suç tanımının bulunmamasından kaynaklanmaktadır. Bunun yanında, siber suçlara karşı oluşturulacak politikanın teknolojik gelişmelere ayak uydurması beklenmekte iken; siber alanın dinamik doğası buna izin vermemektedir. Pratikte de karşılıklı yardım anlaşmaları, bölgesel ve küresel düzenlemeler gibi araçların yargılama yetkisi oldukça sınırlıdır. Bu bağlamda siber suçlarla mücadelede işbirliğinin teşvik edilmesi için ulusal siber suç mevzuatlarının uyumlaştırılması elzemdir. Ancak, siber suçlarla ilgili uluslararası bir mekanizma henüz oluşturulamamıştır (UNCTAD, 2015, s. 25).

Siber suçla mücadele edilmek adına çeşitli adımlar atılsa da, siber suçla mücadele, çeşitli ve ayrıntılı mekanizmalar gerektirmektedir. Mart 2024 itibariyle 156 ülke (devletlerin %80'i) siber suç mevzuatını yürürlüğe koyarken; 10 ülke (%5) ise taslak bir mevzuat hazırlamıştır. 16 ülke (%13) ise, henüz yasal bir mevzuata ve taslağa sahip değildir. Ülkelerin %1'lik kısmı için ise elde edilen veriler bulunmamaktadır[37] (UNCTAD, t.y.). 2001 tarihli Avrupa Konseyi Siber Suçlar Sözleşmesi, siber suçların önlenmesi için oluşturulmuş en eski yasal çerçevedir. Sözleşme, birçok bölgesel ve ulusal mevzuata esin kaynağı olmuştur. AGİT ise siber suçla mücadelede bir dizi güven artırıcı önlemler (CBM'ler) geliştirmiştir. ŞİÖ Uluslararası Bilgi Güvenliğinin Sağlanmasında İşbirliği Anlaşması (2009), Bilgi Teknolojisi Suçlarıyla Mücadele Üzerine Arap Devletleri Birliği Sözleşmesi (2010) ve Siber Uzayda Güven ve Güvenliğe İlişkin Afrika Birliği Sözleşmesi (2014) bunlardan bazılarıdır (UNCTAD, 2015, s. 24).

Yasaların onaylanması ve yürürlüğe girmesi, uygulanması veya iyileştirilmesi, ulusal siber güvenlik stratejilerinin geliştirilmesi veya revize edilmesi önemlidir. 1990 yılında kurulan Olay Müdahale ve Güvenlik Ekipleri Forumu (FIRST), ulusal ve bölgesel Bilgisayar Acil Durum Müdahale Ekiplerinin (CERT's)[38] faaliyetlerini koordine eden

[37] Ülke dağılım haritasını görmek için bkz: UNCTAD. (t.y.). Cybercrime Legislation Worldwide. https://unctad.org/page/cybercrime-legislation-worldwide (02.03.2022).

[38] CERT'ler, siber güvenlik olaylarını tespit etme, izleme ve potansiyel güvenlik ihlallerini belirleme görevini üstlenirler. Bu ekipler, tespit edilen güvenlik olaylarına hızlı ve etkili bir şekilde müdahale ederler. Olayların nedenlerini ve etkilerini analiz etmek, güvenlik açıklarını belirlemek gibi önemli araştırma ve analiz çalışmalarını yürütürler. Ayrıca, etkilenen sistemlerin güvenliğini yeniden sağlamak ve gelecekte benzer olayların önlenmesine yardımcı olacak düzeltme ve kurtarma önlemlerini uygularlar.

uluslararası bir teknik ağdır (Cybil, t.y.). FIRST, ulusal düzeyde siber güvenlik sorunlarını ele almak için ana organlar olan CERT'lerin bir ağı olarak işlev gören, siber güvenlik ve siber suç konularını ele alan bir forumdur (UNCTAD, 2015, s. 24). CERT'ler genellikle devletler tarafından veya onların desteğiyle kurulur. Örneğin, ABD'de ilk CERT, 1988 yılında Carnegie Mellon Üniversitesi'nde, Morris solucanının neden olduğu büyük bir internet güvenlik krizinin ardından ABD Savunma İleri Araştırma Projeleri Ajansı (DARPA) tarafından finanse edilerek kurulmuştur. Bu, dünyadaki ilk CERT olarak kabul edilir ve model, daha sonra diğer ülkeler tarafından da benimsenerek kendi ulusal CERT'lerini oluşturmalarına ilham kaynağı olmuştur (SomCert, t.y.).

Siber suçlarla mücadele, fiziksel suçlarla mücadeleden farklı bir yaklaşım gerektirir. Polis ve geleneksel yargı mekanizmaları fiziksel suçları önlemede ve soruşturmada önemli roller oynarken, siber suçlarla mücadele çok daha geniş bir işbirliği gerektirir. Bu durum, sadece ulusal çapta bir yaklaşımın yetersiz kalabileceğini göstermektedir. Bu nedenle devletlerin, bireylerin ve kurumların siber güvenlik sorumluluğunu paylaşmaları gerektiğini vurgulanmaktadır. Bu yaklaşım, siber güvenliği sadece devletin sorumluluğu olarak görmek yerine, bireylerin ve özel sektörün de aktif roller alması gerektiğini savunur (Chang & Grabosky, 2017, s. 539). Ayrıca siber suçla mücadelede uluslararası işbirliği iki nedenden dolayı hayati önem taşır. Birincisi; suçluların genellikle yargı alanının dışında bulunmaları ve internetin sınır ötesi doğasını istismar etmelerinden kaynaklanmaktadır. Bu durumda suçlunun vatandaşı olduğu devlet tarafından cezalandırılması caydırıcılığın devreye girmesi bakımından önem arz etmektedir. İkinci neden ise; siber suçlara etkili yanıtlar vermenin hızlı bir eylem mekanizması gerektirmesidir. Burada da ağlar arasında işbirliği aracılığıyla oluşturulacak mekanizmalar daha hızlı harekete geçilmesini sağlayabilir (UNCTAD, 2015, ss. 23-24).

Görüldüğü üzere siber suçlara yönelik alınan önlemler genel itibariyle ulusal ve bölgeseldir. Halbuki siber suçların büyük çoğunluğu küreseldir ve dolayısıyla mücadele mekanizmalarının da küresel bir mahiyet taşıması gerekliliğini ortaya çıkarmaktadır. Bu suçların küresel bir sorun haline gelmesi, BM gibi uluslararası örgütlerin konuya

---

Bilgi paylaşımı ve farkındalık yaratma faaliyetleriyle, güvenlik tehditleri, olaylar ve en iyi uygulamalar hakkında bilgi paylaşımında bulunarak genel siber güvenlik farkındalığını artırırlar (Sullivan, t.y.).

daha fazla odaklanması gerekmektedir. Örneğin, Avrupa Konseyi'nin Siber Suçlar Sözleşmesi gibi uluslararası anlaşmalar, siber suçlarla mücadelede bir çerçeve sunmaktadır. Ancak, siber suçlarla mücadelede uluslararası işbirliği, sadece anlaşmalara imza atmakla sınırlı kalmamalı, aynı zamanda bu anlaşmaların uygulanması ve etkin bir şekilde izlenmesi de gerekmektedir.

2.1.2.2. İnsan Hakları Sorunları

İnsan hakları standartları ve yasaları, tüm insanlar için geçerli olan evrensel değerlerdir. Ancak, bu standartlara uyulması ve bağlı kalınması, her zaman ulusal düzeyde sağlanabilmektedir. Bunun nedeni, insan hakları ihlallerinin genellikle ulusal düzeyde meydana gelmesidir (Mihr, 2014, s. 32). İnternetin yaygınlaşması, insan hakları üzerinde de önemli etkilere sahiptir. WSIS Bilgi Toplumu Deklarasyonu'nda demokrasi, sürdürülebilir kalkınma ve insan hakları ile temel özgürlüklere saygının, her düzeyde iyi yönetişimin birbirine bağlı ve karşılıklı olarak güçlendirici olduğu belirtilmektedir (WSIS, Geneva 2003). NETmundial (2014) da internette bazı insan hakları ilkelerine vurgu yapmaktadır. Ancak bunlar yalnızca tavsiye niteliğindedir ve hiçbir ülke veya aktör için yasal olarak bağlayıcı değildir. Bu haklar, ifade özgürlüğü, toplanma ve örgütlenme özgürlüğü ve bilgi edinme özgürlüğünü içermektedir. Bu haklar özellikle devlet gözetiminin yaygın olarak kullanıldığı otokratik rejimlerde tehdit altındadır.

Siber uzayda insan haklarına odaklanan görüş, internetin otoriter rejimler tarafından kullanımını ve bunun devlet gözetimi üzerindeki etkisine odaklanmaktadır (Deibert, 2008). Bunun yanında teknoloji şirketlerinin rolü ve gözetim teknolojilerinin kişisel veriler ve küresel ticaret üzerindeki etkisini de ele almaktadır (Chase, 2019; Jorgensen, 2019). Bu konuların birleştiği temek başlıklar ise veri koruma, gizlilik ve online özgürlük, ifade özgürlüğü ve unutulma hakkı gibi insan hakları sorunlarıdır.

i. Veri Koruma ve Gizlilik

Yasal olarak gizlilik/mahremiyet hakkı, modern insan hakları hukukunun temel bileşenleri arasında yer almaktadır (Rehman, 2010, s. 106). Bu hakkın genel amacı, toplumun ve devletin bir kişinin işlerine ne kadar müdahale edebileceğinin sınırlarını belirlemektir (Davis, 1997, s. 23). Mahremiyet, bireylerin aile yaşamı, arkadaşlıkları, sağlık durumları ve kişisel gelişimleri gibi özel alanlarını kapsayan bir kavram olarak tanımlanmaktadır. Ancak bu mahremiyet alanı, 2000 yılında imzalanan AB Temel

Haklar Şartı'nın 7. ve 8. maddeleri dışında, küresel olarak neredeyse hiç tanımlanmamıştır (Mihr, 2016, s. 316). Avrupa'da, 2000 yılında kabul edilen AB Temel Haklar Şartı'nın 7. maddesi, bireylerin özel ve aile yaşamlarına saygı gösterme hakkını güvence altına alırken, 1995 tarihli AB Veri Koruma Direktifi de kişisel verilerin korunması hakkına odaklanmıştır (IFLA, t.y.b.).

Siber uzayda da en çok vurgulanan insan hakkının gizlilik hakkı olduğu vurgulanmaktadır. Online gizlilik hakkı, NETmundial (2014) tarafından açıkça belirtilmiştir. Belgede; "Mahremiyet hakkı korunmalıdır. Bu, kişisel verilerin keyfi veya yasa dışı gözetimine, toplanmasına, işlenmesine ve kullanımına tabi tutulmamayı içerir. Bu tür müdahalelere karşı kanunun korunması hakkı sağlanmalıdır" ibaresi yer almaktadır. Dolayısıyla belge, devletler veya devlet dışı aktörler tarafından keyfi veya sürekli online gözetime tabi tutulmama hakkını saklı tutmuştur. Diğer yandan, Avrupa İnsan Hakları Mahkemesi Araştırma Dairesi'nin 2011 yılında yayınladığı belge, veri koruma ve veri depolama sorunlarını ele alan önemli bir belgedir. Belgede, ifade özgürlüğü, fikri mülkiyet ve siber suç konuları, daha fazla tanımlanması ve mahkeme kararları yoluyla yorumlanması gereken ana eksiklikler olarak görülmektedir (CoE, 2011, s. 10). 1995 yılında AB tarafından kabul edilen Veri Koruma Direktifi bu noktada önem arz etmektedir. Zira direktif, siber uzayın doğasını dikkate almadan hazırlanmasına rağmen hükümleri dijital alana uygulanabilir düzeydedir[39] (Bygrave & Michaelsen, 2009, s. 120).

Gizlilik ve diğer temel haklar, siber alanın doğası gereği aşındırılabilmektedir (DCAF, 2019, s. 19). İnternet kullanıcıları, sosyal medya platformlarını kullanırken, online alışveriş yaparken, resmi bilgi servislerini kullanırken veya e-posta ve SMS gibi özel mesajlaşma yollarıyla iletişim kurarken sürekli olarak dijital izler bırakırlar. Bu dijital izler, kimlik hırsızlığından reklamcılığa, siyasi manipülasyona kadar bir dizi amaç için kullanılabilir. Verinin büyüklüğü göz önüne alındığında, bu veriler üzerinde etkin bir kontrol mekanizması neredeyse imkansızdır. Bu durum, verilerin kötüye kullanılma riskini artırır ve bireylerin kendi özel verileri üzerindeki sahipliğini zayıflatır. Bu veriler, özel sektör ve kamu sektörü tarafından geniş çapta kullanılıp işlenmektedir ve hiçbir devlet, en demokratik olanlar dahi, bu veriler üzerinde tam bir kontrol

[39] Ancak Direktifin 4. Maddesi, AB ülkelerinin yasal veri korumasının AB dışında da uygulanmasını öngörmektedir. Dolayısıyla bu durum, sorunlu olarak görülmektedir. Zira başka ülkelerde AB'den gelen web sitesi ziyaretçilerinin AB üye devletlerinin gizlilik normlarına uymasını beklemek gerçekçi görünmemektedir (Bygrave & Michaelsen, 2009, s. 120).

sağlayamamaktadır. Verilerin korunamaması, bireylerin şirketlere ve ulusal otoritelere olan güvenini sarsmakta ve bu durum devletlerin ve diğer yetkililerin meşruiyetini zedelemektedir (Mihr, 2016, s. 334). Bu bağlamda, siber alandaki bu geniş çaplı veri toplama ve işleme faaliyetlerinin getirdiği tehlikeler, bireysel gizlilik haklarını ve diğer temel özgürlükleri koruma altına almanın önemini daha da artırmaktadır.

Gizlilik haklarının ve diğer temel özgürlüklerin aşındırılması, hukukun üstünlüğü ilkesinin de baltalanma tehlikesini artırmaktadır. Hukukun üstünlüğü ilkesi, uluslararası mahkemeler tarafından daha ayrıntılı şekilde yorumlanmıştır. AİHM, temel haklara ilişkin tüm kısıtlamaların açık, kesin, erişilebilir ve öngörülebilir hukuk kurallarına dayanması ve açıkça meşru amaçlara hizmet etmesi gerektiğini belirtmiştir. Bu kısıtlamalar, ilgili meşru amaç açısından gerekli ve orantılı olmalı ve etkili bir çözüm yolu sunmalıdır (DCAF, 2019, s. 19). Zira özellikle küresel ekonominin internet aracılığıyla artan bağlantılılığı, yetki alanı çatışmalarını daha yaygın hale getirmiştir. Bu bağlamda veri koruma yasalarının evrensel uygulanabilirliği, internet üzerindeki davranışları düzenlemeye yönelik yargısal iddiaların karmaşıklığında yol gösterici olmakta ve uluslararası düzenlemelere olan ihtiyacı vurgulamaktadır (Kuner, 2010, s. 176). IoT gibi yeni teknolojilerin ortaya çıkışı da, mal ve hizmet alışverişini kolaylaştırırken aynı zamanda güvenlik ve gizlilik endişelerini de beraberinde getirmektedir. Bu yeni alanın saldırılara karşı korunması ve kullanıcı mahremiyetinin güvence altına alınması için uluslararası düzeyde uygun yasal çerçeveler oluşturulması gerekmektedir (Weber, 2010, s. 23).

Dünya genelindeki yasama organları, kişisel bilgilerin toplanmasını, yönetimini ve paylaşımını düzenlemek amacıyla mahremiyet ve veri koruma yasalarını güncellemeye çalışmaktadır. Bu güncellemeler sıklıkla, kişisel verilerin sınır ötesi transferlerinde alıcı ülkenin mahremiyet korumalarının "yeterli" olarak değerlendirilmesini zorunlu kılmaktadır. Özellikle AB, bu yaklaşımın öncüsü olmuş ve Brezilya gibi diğer önemli ekonomiler de benzer modelleri takip etmiştir. Ayrıca Çin ve Rusya gibi ülkeler, kişisel veri transferleri üzerinde daha katı kontroller uygulayarak bu eğilimi daha da ileriye taşımışlardır. Böylesine çeşitli ulusal düzenlemeler, her ne kadar kişisel verilerin korunması amacını gütmekte olsa da (bazı eleştirilere göre bu politikaların altında yatan nedenler ticari korumacılık ya da yasalara erişim sağlama çabaları olabilir), farklı standartlardaki uyumsuzluk, "yetersiz" veri koruma standartlarına sahip ülkelerden veri alışverişini kısıtlayarak internetin bütünlüğünü tehlikeye atmaktadır. Bu durumun

somut bir örneği, 2015 yılında Avrupa Adalet Divanı'nın, Avrupa'dan Amerika'ya kişisel veri transferleri için koruma sağlayan ve uzun süre yürürlükte olan AB-ABD Güvenli Liman Anlaşması'nı iptal etmesiyle yaşanmıştır. Bu karar, uluslararası veri transferleri üzerinde önemli etkilere sahip olmuş ve uluslararası veri koruma standartlarının uyumlaştırılması konusunda yeniden düşünmeye sevk etmiştir (Ellis & Mohan, 2019, s. 206).

Uluslararası kişisel bilgi akışının internet üzerindeki etkisi, demokratik ülkeler arasında bile kişisel bilgilerin adil bir şekilde işlenmesine dair genel prensiplere rağmen, gizlilik haklarının sınırlar arasında büyük farklılıklar gösterdiğini ortaya koymaktadır. Yukarıdaki örnekte de görüldüğü gibi özellikle Avrupa ve ABD arasındaki gizlilik standartlarındaki farklar dikkate değerdir. Gizlilik kurallarının uluslararası düzeyde uyumlaştırılmasının, ülkelerin iç siyasi dengelerine olumsuz etkileri olabileceği ve bu tür girişimlerin siyasi istikrarsızlığa yol açabileceği konusunda endişeler bulunmaktadır. Bunun yerine, liberal piyasa tabanlı yaklaşımlar ile sosyal korumacı ve hak temelli sistemler gibi farklı yönetim tercihlerine uyum sağlayabilecek, bilgi gizliliğinin bir arada yönetilmesine olanak tanıyan bir çerçeve önerisi ön plana çıkmaktadır (Reidenberg, 2000, s. 1315). DeNardis (2014), 21. yüzyılda internet yönetişimi ile ilgili çatışmaların yeni siyasi ve ekonomik güç alanlarını nasıl ortaya çıkardığına dikkat çekmiştir. İnternet yönetişimi teknolojilerinin, ifade özgürlüğü ve gizlilik gibi önemli kamu çıkarı alanlarında giderek artan bir rol oynadığına işaret eden DeNardis, bu teknolojilerin kontrolünün egemen ulus devletlerden özel ve küresel şirketlere doğru kaydığını belirtiyor. Bu bağlamda, DeNardis, internet yönetişimiyle ilgili bu tartışmaları anlamak ve yönetmek için internet yönetişiminin karmaşık yapısının derinlemesine incelenmesi gerektiğini vurgulamıştır.

Diğer yandan, gizliliğe yönelik endişelerin başında gözetlenme korkusu gelmektedir. Zira devletler artık filtreleme programlarını finanse etmenin çok ötesinde faaliyetler yürütmektedir. Bazı devletlerin gözetleme sistemleriyle kitleleri izleme eylemleri de artış göstermektedir (Kleinwächter, 2020). Bugün çoğu ülkenin çeşitli gözetim mekanizmaları geliştirdiği bilinmektedir. Genellikle bu mekanizmaları şiddet veya terörle mücadele kapsamında kullandıklarını iddia etseler de, gözetleme ağlarını genişlettikleri öne sürülmektedir (Bygrave & Michaelsen, 2009, s. 124). Bazıları ise gözetleme sistemlerini kullanmak yerine, servis sağlayıcıları aracılığıyla veri depolamakta ve gerektiğinde bu verilere devletin erişmesini sağlamaktadır. Depolama

sistemlerinin gizlilik içinde yürütülmesi genellikle zordur. Wikileaks olayında görüldüğü üzere devletler bu depolama işlemlerini gizlilik çerçevesinde yürütme becerisini henüz kazanabilmiş değildir. Bu tür olaylar, kamuoyunda büyük çaplı tartışmalar yaratmakla beraber siber uzaydaki aktörlerin davranışları üzerinde "caydırıcı bir etki"ye de sebep olmuştur. Çünkü aktörler, siber uzayda attıkları her adımın bir gün "ifşa" edilebileceğinin bilincine varmıştır.

Özellikle bulut bilişimin yaygınlaşmasıyla, güvenlik, veri koruma ve gizlilikle ilgili endişeler artmıştır. Verilerin bulut ortamında korunması ülkelerin çoğunluğu tarafından sağlanmaya çalışılsa da, farklı ülkelerde bu verilerin ele alınmasında yargı alanları önemli ölçüde farklılık göstermektedir. Bulut bilişime özgü yasa ve düzenlemelerin geliştirilmesi henüz gündemde olmasa da; gizlilik, veri koruma, bilgi güvenliği ve siber suç gibi bulut bilişimle ilgili alanlarda yasal reformların yapılması önemlidir. Politika düzeyinde veri koruma, gizlilik, teknik altyapı, e-ticaret ve güvenlik gibi internet kamu politikası konuları göz önünde bulundurulmalıdır. Bu sorun alanlarına yönelik oluşturulacak uluslararası mekanizma, küresel ve ulusal düzenlemelerin uyumlu çalışmasını gerektirecektir (UNCTAD, 2015, s. 19).

Bu gelişmeler, siber uzayda veri korumasının çok paydaşlı bir yaklaşım gerektirdiğine işaret etmektedir. Bu yaklaşım, arama motorları, sosyal ağlar, uluslararası kuruluşlar, ulus devletler ve sivil toplum kuruluşlarını kapsamaktadır. Bu aktörler, gayri resmi ve resmi forumlar aracılığıyla bir araya gelir ve istişare amaçlı ortaklıklar kurar. Bu forumlar, bilgi toplumu hakkında ortak bir anlayış geliştirmeye yardımcı olur. Ancak bu aktörler, farklı roller oynamakta ve farklı amaçlara sahip olmaktadır. Devlet temsilcileri karar alabilir, uygulayabilir ve icra edebilir. Özel şirketler ve sivil toplum kuruluşları ise danışman ve uzman olarak görev yapabilir. Bu ortaklıklar gönüllülük esasına dayanmaktadır ve katılım, sürecin algılanan faydalarına göre yönlendirilmektedir. Bu ortaklıklar, politika süreçlerinde değişime meydan okumak ve lobi yapmak için giderek daha fazla kullanılmaktadır (Mihr, 2016, s. 332).

Bu karmaşık sorunları çözümlemek adına uluslararası topluluğun bir araya gelmesi ve verilerin küreselleşmesi ile ulusal egemenlik ve mahremiyet gibi kritik değerleri dengede tutacak yeni yöntemler geliştirmesi gerekmektedir. Bugün internet, içeriklerin izlenmesi ve kullanıcıların kimlik bilgilerinin elde edilmesine imkân tanımaktadır. Bu durum, internet servis sağlayıcılarına yönelik eleştirilere sebebiyet vermektedir.

Rundle, "özgürlüğü sevenler, ortaya çıkan bu uluslararası sisteme demokratik değerler inşa etmek için çalışmalıdır" demiştir (2005, s. 19). Zira bireylerin bilgi edinme hakkı, bu bilgilerin başkalarının onurunu veya mahremiyetini ihlal etmeyecek şekilde kullanıldığı sürece geçerlidir. Özellikle sağlık veya aile ile ilgili özel bilgilerin genel erişime açık olması, ilgili kişinin haklarını riske atabilir. Ancak, veri koruması her zaman sansürü veya keyfi gözetlemeyi haklı çıkarmamalıdır. Bu denge, bilgi edinme özgürlüğünün sınırlarını ve sınırlarını kimin belirleyeceğine bağlı olarak oluşur. Ne kadar çok paydaş katılırsa, bu dengeleme süreci ve sonuçların genel kabul görme olasılığı o kadar artar (Mihr, 2016, s. 322). Bu nedenle uluslararası veri akışlarını düzenleyecek yeni yasal ve politik rejimlerin kurulması, verinin coğrafi konuma dayalı yasal yargı yetkisine olan bağlılığın azaltılması, farklı ülkeler arasında veri paylaşımını ve işbirliğini kolaylaştıracak uluslararası anlaşmaların yapılması ve ifade özgürlüğü ile mahremiyet gibi temel hakların korunması gerekmektedir.

ii. Online Özgürlük

Online özgürlük, sınırların ötesindeki etkisiyle küresel bir internet yönetişimi sorunudur. Teknolojinin hızlı ilerlemesi ve internetin küresel doğası, bilgiye erişim ve ifade özgürlüğü gibi temel hakların korunması konusunu ön plana çıkarmaktadır. Devletlerin, özel sektörün ve sivil toplumun etkileşimi, bu özgürlüklerin nasıl denetleneceği ve korunacağı konusunda karmaşık sorunlara yol açmaktadır. WGIG, online ifade özgürlüğüne ilişkin sorunları, birçok faaliyetin yanı sıra kamu politikasının tüm alanlarını etkileyen önemli konular olarak kabul etmiştir (ITU, 2005, s. 27). Online özgürlük, bütün paydaşların rol oynadığı geniş bir alanı kapsamaktadır. Zira bütün paydaşlar, siber uzaydaki davranış biçimleriyle online özgürlük üzerinde etkili olabilmektedir.

Devletlerin rolü burada nispeten daha fazladır. Devletler, vatandaşların iletişimini denetlemek amacıyla interneti giderek daha fazla kullanmakta; bu süreçte belirli online platformlara ve hizmetlere erişimi kısıtlamakta ya da tamamen engellemektedirler. Asya, Orta Doğu ve Kuzey Afrika bölgelerindeki ülkeler internet kısıtlamalarına daha eğilimlidir. Çin ve İran, en kapsamlı filtreleme sistemine sahip ülkeler arasında yer almaktadır. Freedom House, "China: Freedom on the Net 2020 Country Report" isimli raporda Çin'deki internet kullanıcıları için koşulların günden güne daha da kötüleştiğini ifade etmiş; ülkenin üst üste altıncı yıldır internet özgürlüğü konusunda dünya sıralamasında en aşağıda olduğunu teyit etmiştir (Freedom House, 2020). Yine

Freedom House'ın "Ağın Özgürlüğü 2021" adlı raporu "Orta Doğu ve Kuzey Afrika'da internet özgürlüklerinin "saldırı altında" olduğu ifade edilmiştir. Orta Doğu ve Kuzey Afrika ülkelerinin büyük çoğunluğu siber alanda "kısmen özgür" veya "özgür değil" olarak derecelendirilmiştir (Freedom House, 2021). En güncel verilere göre yine Çin, 2022 yılında internet kapatmalarından etkilenen kişi sayısına göre ilk sırada yer almıştır. Diğer yandan Nisan 2023 itibariyle Kuzey Kore nüfusu neredeyse tamamen çevrimdışı kalmıştır, çünkü vatandaşların internet erişimi devlet tarafından büyük ölçüde kısıtlanmış ve kullanımlar yalnızca özel izne tabi tutulmuştur (Statista, 2023).

Online özgürlük, yalnızca Asya, Orta Doğu veya Kuzey Afrika'da kısıtlanmamaktadır. Liberal ve demokratik olarak adlandırılan Batılı ülkeler de online filtrelemeyi kullanmaktadır. Ancak burada filtreleme sistemleri çoğu zaman devletler tarafından dayatılmaktan ziyade, gönüllü uygulamalar aracılığıyla yapılmaktadır. Yasadışı içeriklere halkın erişimini engellemeyi hedefleyen gönüllü girişimlerin sayısı oldukça fazladır. Bu girişimler, kararnamelerle empoze edilmekten ziyade, özel kuruluşların resmi inisiyatifleriyle gerçekleştirilmektedir. Ancak bu faaliyetler çoğunlukla kolluk kuvvetleri gibi devlet kurumları ile yakın işbirliği içinde yürütülmektedir (Bygrave & Michaelsen, 2009, s. 122). Gönüllü proje başlatan ülkelerin başında İngiltere, Kanada, İtalya ve İskandinav ülkeleri gelmektedir. Avusturalya da 2009 yılında şiddet içerikli ve müstehcen içerikleri hedefleyen oldukça sert bir plana gitmiş olsa da karşılaştığı muhalefet nedeniyle planını ertelemek durumunda kalmış, 2019 yılında tekrar gündeme getirmiştir (Crozier, 2019).

Diğer yandan devletler, OECD ve Avrupa Konseyi gibi hükümetlerarası kuruluşlarla birlikte internet faaliyetleriyle doğrudan veya dolaylı olarak ilgilenmeye başlamışlardır. Siber suç ve spam, devletlerin hedefindeki başlıca faaliyet gruplarıdır. Devletler, bazı durumlarda siyasi, dini ve sosyal nedenlerle de Web'deki bilgilere kamu erişimini kısıtlayabilmekte veya buna yönelik düzenlemeler yapabilmektedir. Bunu, web sitelerinden veri akışına teknik engeller koyarak veya ISP'ler[40] üzerinde filtreleme işlemleri yaparak uygulamaktadır (Bygrave & Michaelsen, 2009, s. 122).

[40] ISP (İnternet Servis Sağlayıcı), internete erişim sağlayan ve genellikle çeşitli internet hizmetleri sunan şirket veya kuruluşlardır. Bu hizmetler arasında geniş bant internet erişimi, e-posta hizmetleri, web hosting, alan adı kaydı ve bazen de VoIP (Voice over Internet Protocol) gibi ses hizmetleri bulunur. ISP'ler, bireysel kullanıcılar, işletmeler ve hükümet dahil olmak üzere çeşitli müşteri gruplarına hizmet verirler. ISP'ler, müşterilerinin internete bağlanmasını sağlayarak onlara dünya çapında bilgi ve kaynaklara erişim imkânı sunarlar. Bu bağlantı, çeşitli teknolojiler kullanılarak sağlanabilmektedir.

Etkin izleme kabiliyetlerine rağmen devletler, internette paylaşılan tüm içerikleri izleyerek zararlı içeriği tespit edip kaldıramazlar. Bunun birkaç nedeni var. Birincisi, internet çok büyük bir yer ve her gün çok fazla içerik paylaşılıyor. Devletler bu kadar çok içeriği takip edemezler. İkincisi, zararlı içeriği tanımlamak kolay değildir. Neyin zararlı olduğu, kültürden kültüre ve zamana göre değişebilir. Üçüncüsü, devletlerin zararlı içeriği kaldırması, ifade özgürlüğü gibi temel haklara müdahale anlamına gelebilir. Zira içerik moderasyonu karmaşık ve zor bir süreçtir. İçerik moderatörleri, bir içeriğin zararlı olup olmadığını belirlemek için içeriğin amacını, mevcut kültürel normları ve kamuoyu tartışmasını göz önünde bulundurmalıdır. Bu bazen zor ve hatta tartışmalı kararlar gerektirebilen bir süreçtir. Örneğin, bir içeriğin nefret söylemi olup olmadığı, içerik moderatörlerinin kendi değerlerine ve inançlarına göre yorumlanması gereken bir konu olarak nitelendirilmektedir (Ricknell, 2020, ss. 110-111).

Peki sorumluluk yalnızca hakaret içeren ifadeyi kullanan kişide mi yoksa ISP üzerinde mi olmalıdır? ISP'lerin sorumluluğuna ilişkin belirsizlik, ISP'lerin hakaret içeren ifadeyi hızlı bir şekilde kaldırmasına neden olabilir. Bu, ifade özgürlüğü haklarını tehlikeye atabilir. Mevcut yasalar, hakaret içeren ifadenin tespit edilmesinden sonra ISP'lerin bu içeriği kaldırmasını gerektiriyor. Ancak, "bilgi"nin ne anlama geldiği ve hangi zaman çerçevesinin geçerli olduğu belirsizdir. Bu, ISP'lerin sorumluluklarını belirlemeyi zorlaştırır. ISP'ler, hakaret içeren ifadeyi kaldırmak için ahlaki koruyucular olarak hareket edebilir. Ancak, ISP'lerin sorumluluğuna ilişkin belirsizlik, ISP'lerin bu sorumluluğu üstlenmek istememesini sağlayabilir. Bu, potansiyel olarak zararlı içeriğin internette kalmasına neden olabilir (Mansell, 2004, ss. 4-5).

ISP'ler, farklı abonelik türleri ile internete erişimi mümkün kılan bir aracı sistemdir. Her coğrafyaya göre farklı bir şekilde hizmet verirler. ISP'ler; karşılaştırmalı hukuka göre içerik, servis ve erişim olmak üzere üç kategoride sağlayıcı görevi görürler (Yıldız, 2002, s. 169). Ancak erişim kategorisinde başkalarına ait verileri depolama yetkisi yoktur. Bunun yanında, ISP'lerin herhangi bir kaynaktan gelen bilgileri denetleme veya kontrol etme imkânı oldukça sınırlıdır. Bu nedenle yasadışı içerikleri ayırt edememesi nedeniyle herhangi bir sorumluluğu söz konusu değildir (Yıldız, 2002, s. 172). Dahası, ISP'ler içeriği izleme veya yasadışılığını tespit etme işlevine de sahip değildir. İçeriğin aktarılması veya depolanmasında yalnızca bir kanal veya önbellek

Örneğin dial-up (telefon hattı üzerinden), DSL (dijital abone hattı), kablo modem, fiber optik, uydu veya hücresel veri hizmetleri gibi. Ayrıntılı bilgi için bkz: (Investopedia, t.y.).

görevi görürler. Nitekim sahip oldukları bu muafiyetler, özellikle ulusal hukuk sistemleri bağlamında halen pek çok tartışmaya konu olmaktadır. Öyle ki bazı durumlarda ISP'ler için sağlanan muafiyetler, ISP kullanıcılarının özgürlüklerini kısıtlayabilmektedir. Örneğin, ISP'lerin kullananların kimliklerini ifşa etmeye zorlaması artan faaliyetler arasındadır (Bygrave & Michaelsen, 2009, s. 123).

Devletlerin faaliyetlerinin yanında bölgesel, uluslararası ve ulusüstü kuruluşların da rolü önemlidir. Örneğin, AB tarafından geliştirilen dijital yönetişim politikalarının çoğu, zararlı veya yasadışı içerikle mücadeleye yöneliktir. AB'nin bu politikası, genellikle filtreleme araçlarının geliştirilmesini finanse etmek ve içeriğin ISP'ler tarafından engellenmesini gönüllü olarak teşvik etmek amacıyla oluşturulan bir Eylem Planı'na dönüşmektedir (Bygrave & Michaelsen, 2009, s. 123). Ancak bu tür Eylem Planlarının ifade özgürlüğünü kısıtlayacağı yönünde endişeler olabilmektedir. Bu endişeler, e-ticaretin teşviki ve ifade özgürlüğünün korunması gibi sebeplerle azaltılmaya çalışılsa da halen devam etmektedir. Avrupa Konseyi'nin 2008 tarihli bir tavsiyesinde de bu Eylem Planlarının ifade özgürlüğü ilkesine zarar vermemesi gerektiği belirtilmiştir (CoE, 2008).

Online özgülük konusunda sivil toplum da oldukça etkilidir. İnsan hakları, ifade özgürlüğü, açık kaynak geliştirme ve bilgi paylaşımı gibi konularla yakından ilgilenir (Kowack, 1997, s. 55). Diğer yandan özel sektörün rolü de burada önem arz etmektedir. Özel kuruluşlar, menşei ülkelerin ulusal yasalarına tabi olmaları nedeniyle evrensel insan hakları normlarını göz ardı edebilmektedirler. Bu nedenle online özgürlük konusunda insan haklarını ihlal edebilmekte hatta bazı durumlarda gözetim mekanizmalarını dahi kullanabilmektedirler. Bu kuruluşların eylemleri, diğer devletlerin egemenliğine aykırı olabilecek uygulamalarla sonuçlanabilmekte ve kullanıcıların gizlilik haklarını ihlal edebilmektedir (Council of Europe Commissioner for Human Rights, 2014, s. 9).

Online özgürlüğe yönelik bu kısıtlamalar, ifade özgürlüğü, gizlilik hakları ve bilgiye erişim gibi temel insan haklarını tehlikeye atmaktadır. Devletlerin ve özel kuruluşların internet üzerindeki denetimleri, kullanıcıların online ortamda özgürce bilgi paylaşımı yapmalarını ve bilgiye erişimlerini engelleyebilir. Özellikle, zararlı olarak kabul edilen içeriğin tanımı ve bu içeriğin kaldırılması süreçleri, ifade özgürlüğüne müdahale edebilir ve öznel kararlara yol açabilir. Bu bağlamda, ulusal yasalar ve uluslararası

normlar arasında denge kurulmalı, ifade özgürlüğü ve gizlilik haklarını koruyacak politikalar geliştirilmelidir.

iii. İfade Özgürlüğü

İfade özgürlüğü hakkı, siber alan dahil olmak üzere uluslararası politika gündeminin önemli bir parçası haline gelmiştir. WSIS Bilgi Toplumu Deklarasyonu'nda da ifade özgürlüğünün İHEB sınırları çerçevesinde korunacağı teyit edilmiştir. "Herkes, her yerde katılma fırsatına sahip olmalı ve kimse Bilgi Toplumu'nun sunduğu faydalardan mahrum bırakılmamalıdır. Bu Deklarasyonun hiçbir hükmü, BM Antlaşması'nı ve İnsan Hakları Evrensel Beyannamesi'ni, bu araçların ilerletilmesi için kabul edilen diğer uluslararası araçları veya ulusal yasaları zedeleyecek, çelişecek, kısıtlayacak veya ortadan kaldıracak şekilde yorumlanmayacaktır." (WSIS, Geneva 2003).

İfade özgürlüğü, bilgi ve fikirleri serbestçe arama, alma ve yayma özgürlüğünü içermektedir. Bu ilke, siber çatışma alanlarında ve diğer siber alanlarda, örneğin siber güvenlik, ticaret ve suçla mücadele gibi konularda önemli bir rol oynamaktadır. İnternetin yaygınlaşması, insanların kendilerini ifade etme olanaklarını büyük ölçüde artırdı. İletişimi merkeziyetsizleştiren, katılımcılara yeni ifade biçimleri ve kültürel ifadeler sunan internet, demokrasinin radikal bir şekilde gelişmesine ön ayak olan bir ağ olarak görüldü. Nitekim zaman içinde sosyal medya platformları aracılığıyla internet, vatandaşların özgürlük ve demokrasi mücadelelerinde önemli bir araç haline geldi. Bu durum, özellikle 2011'deki Arap Baharı sırasında olduğu gibi belirgin bir şekilde ortaya çıkmıştır (Ricknell, 2020, s. 110). Ancak bu durum, ifade özgürlüğüne yönelik çeşitli zorlukları da beraberinde getirdi. İnternet, fiziksel sınırları olmayan küresel bir ağ olduğundan, internette gerçekleşen eylemlerin ve olayların, her bir kullanıcının bulunduğu ülkeye göre farklı yasalara tabi olabileceği anlamına gelir. Bu durum, özellikle mahremiyet ve ifade özgürlüğü gibi konularda hukuki veya yasal sorunlara yol açabilir (Şeker, 2020). Bu nedenle siber alanda ifade özgürlüğünü korumak, yalnızca siber uzaya yönelik stratejinin bir parçası değildir. Aynı zamanda uluslararası hukuk çerçevesinde ortaya çıkan dış politika gündeminin de bir parçasıdır (Koh, 2012, s. 10).

AİHS 10. maddenin 1. fıkrası şöyledir: Herkesin ifade özgürlüğü hakkı vardır. Bu hak, kamu otoritesinin müdahalesi olmaksızın ve sınırlar dışında görüş sahibi olma, bilgi ve fikir alma ve verme özgürlüğünü içerecektir. Benzer şekilde, BM'nin 1948 tarihli İnsan

Hakları Evrensel Beyannamesi'nin 19. maddesi şöyle der: Herkesin fikir ve ifade özgürlüğü hakkı vardır; bu hak, müdahale olmaksızın görüş sahibi olma ve herhangi bir araçla ve sınırlar olmaksızın bilgi ve fikir arama, alma ve verme özgürlüğünü içerir. Madde, herkesin düşünce ve ifade özgürlüğü hakkına sahip olduğunu, bu hakkın müdahale edilmeden kendi görüşlerini oluşturma, bilgi ve fikir arama, alma ve iletme özgürlüğünü kapsadığını, herhangi bir sınırlama (bölge) olmaksızın her türlü medya aracılığıyla gerçekleştirebileceğini ifade eder. Bilgi teknolojisiyle ilişkili konuşma ve fikir belirtme hakkı, bireylerin bu sınırları aştığı gerekçesiyle suçlu olarak görülmesine yol açabilmektedir. Aslında ifade özgürlüğü hakkı, 1945 BM İnsan Hakları Beyannamesi'nin 29. maddesinde de düzenlenmiştir. Bu madde, ifade özgürlüğü, örgütlenme ve toplanma özgürlüğü, sözlü ve yazılı konuşma özgürlüğü gibi hakların kanunla sınırlandırılabileceğini belirtir (Lukitasari, 2013, s. 78).

Avrupa İnsan Hakları Mahkemesi kararlarına göre, ifade özgürlüğü demokratik bir toplumun temellerinden biridir ve her bireyin kendini gerçekleştirmesi için temel koşullardan biridir. Bu nedenle, özellikle yeni demokrasilerde yeni medya yoluyla kullanılan ifade özgürlüğü, demokrasinin "oksijeni" olarak adlandırılmıştır. Eğer ifade özgürlüğü demokrasinin oksijeni ise, internet de insanların yaşadığı, nefes aldığı ve ifade özgürlüklerini kullandıkları atmosferdir (Benedek & Kettemann, 2013, s. 24).

BM, OAS, Afrika İnsan ve Halkların Hakları Komisyonu ve AGİT bazı raportörler, "İfade Özgürlüğü ve İnternet Ortak Bildirgesi" adlı bildirgede; "tüm nüfus veya halk kesimleri için internete veya internetin bazı kısımlarına erişimin kesilmesi (internetin kapatılması) kamu düzeni veya ulusal güvenlik gerekçeleri dahil olmak üzere hiçbir zaman haklı gösterilemez" şeklinde bir ifade kullanarak ifade özgürlüğünün önemine vurgu yapmışlardır. Bununla birlikte, ifade özgürlüğünün tanınmasının yanında, soykırım veya nefret söylemi gibi uluslararası hukuk açısından suç teşkil eden içeriklere yönelik sınırlamalar da mevcuttur (OSCE, 2011). Son olarak, üyeliği neredeyse tamamen bölgesel olan Online Özgürlük Koalisyonu (FOC), dünya çapında internet özgürlüğünü ve ifade özgürlüğünü geliştirmeye yönelik çalışmalar düzenlemektedir. FOC, internet kullanıcılarını korumak, insan haklarını savunmak ve interneti özgür ve açık tutmak için Dijital Savunucu Ortaklığı (DDP) başlattı (DDP, t.y.).

Tüm bu girişimlerden de anlaşılacağı üzere internet, ifade özgürlüğü için önemli bir araç sağlamış ve bu aracın yönetişimine atfedilen önem günden güne artmıştır. İnsanlar, internet üzerinden düşünce ve fikirlerini özgürce ifade edebilmektedir. Ancak, ifade özgürlüğü de bazı sınırlara tabidir. Örneğin, bir kişinin internette yaptığı paylaşımlar, başkalarının haklarını ihlal ediyorsa veya suç teşkil ediyorsa, hukuki yaptırımlara tabi olabilir. Bu sınırlamalar, internette ahlaksızlığın önlenmesi için gereklidir. Örneğin, bir kişinin internette çocuk pornografisi yayması, ifade özgürlüğü kapsamında değildir. Bu tür paylaşımlar, çocukların korunması için yasaklanmıştır.

İnternette ifade özgürlüğü, diğer insan haklarını destekleyen ve kendi başına da önemli bir insan hakkıdır. İfade özgürlüğü online olarak, UDHR, ICCPR ve AİHS gibi insan hakları yasalarıyla korunmaktadır. Mahkemeler, tavsiye komisyonları, sivil toplum kuruluşları ve insan hakları örgütleri ifade özgürlüğünü korumada rol oynamaktadır. Ancak online ifade özgürlüğünün kısıtlanması konusunda, genel olarak Avrupa İnsan Hakları Sözleşmesi (AİHS) kapsamındaki müdahale kurallarına uygun olma gerekliliği vardır. AİHS, bireylerin temel hak ve özgürlüklerini koruma amacını taşır ve ifade özgürlüğünü de bu haklar arasında önemli bir yerde tutar (Benedek & Kettemann, 2013, s. 171).

Online ifade özgürlüğünün korunması açısından temel bir prensip şu olmalıdır: Fiziksel alanda izin verilene, online olarak da izin verilmelidir (Benedek & Kettemann, 2013, s. 171). Yani, geleneksel medya veya diğer ifade biçimlerinde tanınan haklar ve özgürlükler, dijital ortamda da aynı ölçüde korunmalıdır. Bu prensip, bireylerin düşünce, ifade ve bilgi edinme özgürlüklerini sadece fiziksel dünyada değil, aynı zamanda internet üzerinde de güvence altına almayı amaçlar. Online platformlarda da demokratik değerlere uygun bir şekilde ifade özgürlüğünün savunulması, toplumsal çeşitliliğin ve tartışmanın teşvik edilmesi için önemlidir. Ancak, bu hakların sınırları, yasa dışı faaliyetlerin önlenmesi ve toplumun genel güvenliğinin korunması gibi temel prensiplerle dengelenmelidir. Online ifade özgürlüğünün korunması, bu dengeyi bulmak ve uygun düzenlemeleri yapmak suretiyle sağlanabilir.

Önemli bir diğer faktör, küresel online içerik toplayıcıları arasında (sosyal medya devleri), içerik düzenleme uygulamalarında tekdüzelik ve şeffaflık eksikliğidir. Bu şirketler, yıllar boyunca içerik düzenleme ve kaldırma politikalarını açıkça belirlemek adına adımlar atmış olmalarına rağmen, uygulamada bu kılavuzların tutarsız ve şeffaf

bir şekilde uygulanmadığı gözlemlenmektedir. Bu şirketlerin içerik düzenleme ve kaldırma politikaları genellikle mahkemeler için ayrılmış bölgelere girmektedir. Dahası, internet üzerinden paylaşılan içeriğin büyük miktarı, online materyali tamamen kontrol etmeyi neredeyse imkânsız kılmaktadır (Ülgen, 2016, s. 18).

Netice itibariyle ifade özgürlüğü, temel bir insan hakkı olarak kabul edilir, ancak bu özgürlüğün uygulanmasında diğer insan haklarına da saygı gösterilmesi önemlidir. Özellikle siber alanda ifade özgürlüğüne getirilen kısıtlamaların başkalarına zarar vermemek, toplumsal düzeni korumak ve diğer temel hakları güvence altına almak amacıyla gerekli olabileceği kabul edilmektedir. Bu nedenle ifade özgürlüğü, diğer hak ve özgürlüklerle denge içinde olmalıdır. Kısıtlamaların temel nedenleri arasında başkalarının haklarına ve özgürlüklerine saygı göstermek, ahlaki değerleri korumak, din, güvenlik ve kamu düzenini sağlamak yer almaktadır. Bu kısıtlamalar, toplumun genel çıkarlarını korumayı amaçlar ve hakların demokratik bir düzen içinde adil bir şekilde dengelemesini sağlamayı hedefler (Lukitasari, 2013, s. 81).

iv. Unutulma Hakkı

"Unutulma hakkı" (*right to be forgotten* – RTBF) veya "arama sonuçlarından çıkarılma hakkı" (*right to be delisted* – RTBD) internet yönetişimi açısından geleneksel içerik düzenlemelerinden farklı ve daha temel düzeyde zorluklar oluşturmaktadır. Unutulma hakkı, bir bireyin üçüncü kişilerin artık kendisini takip edemeyeceği şekilde belirli verilerin silinmesini talep etme hakkını yansıtır (Weber, 2011, ss. 120-121). Bu hak, dijital çağın getirdiği yeni bir insan hakkı olarak öne çıkmaktadır (Miyashita, 2016, s. 3; Razmetaeva, 2020, s. 59). Özellikle Avrupa'da geçerli olan veri gizliliği ve kişisel veri işleme yasalarına dayanan bir düzenlemedir. Bu düzenleme, bireylere kendi hakkındaki bilgilerin yayılmasını kontrol etme yetkisi verir (Bavitz, 2018, s. 3).

Unutulma hakkı, bireylerin dijital ortamda kendi kimliklerini ve itibarlarını korumak için önemli bir mekanizma sunar. Kişisel verilerin geniş çapta paylaşıldığı internet ve sosyal medya platformlarında, insanların geçmişleriyle ilgili bilgiler üzerinde bir kontrol sahibi olmalarını sağlar. Bu hak, özellikle geçmişte yaşanan olumsuz olayların veya yapılan hataların, bir bireyin dijital kimliği üzerinde derin izler bırakmayı önlemeye yöneliktir. Diğer bir deyişle, unutulma hakkı, kişilerin geçmişteki faaliyetlerinin sonsuza kadar internet ortamında kalmaması için bir çözüm sunar. Bu, dijital çağda bireylerin geçmişteki hatalarından ötürü sürekli bir damgalanma ile karşı

karşıya kalmalarını engeller. Geleneksel olarak zamanla unutulan bilgiler, dijital ortamın kalıcı doğası nedeniyle, kişilerin hayatlarını uzun yıllar boyunca etkileyebilir. Bu durum, kişisel verilerin kontrolü, verilerin paylaşımının etik ve yasal sınırları gibi konuları önemli hale getirir (Razmetaeva, 2020, s. 59). Unutulma hakkı, bu bağlamda, bireylerin geçmişteki bilgiler üzerinde bir dereceye kadar kontrol sahibi olmalarını sağlayarak, özel hayatın gizliliği ve kişisel onurun korunmasına katkıda bulunur.

Unutulma hakkının uygulanması ve sınırları konusunda çeşitli tartışmalar mevcuttur. Bu hak, özellikle ifade özgürlüğü gibi temel haklarla çatışabileceği endişeleriyle karşı karşıyadır. Öyle ki, unutulma hakkının uygulanması sürecinde en önemli zorluklardan biri, bu hakkın ifade özgürlüğü ile dengelemesidir (Szeghalmi, 2018, s. 256; Razmetaeva, 2020, s. 62, Miyashita, 2016, s. 13). Bireylerin kişisel verilerini silme veya düzeltme talepleri, kamuoyuyla paylaşılan bilgilerin düzenlenmesi konusunda hassasiyet yaratmaktadır. Bu durum, unutulma hakkının, kamu yararı ile bireyin hakkı arasında bir denge kurularak uygulanmasını gerektirmektedir (Razmetaeva, 2020, s. 59). Özellikle ulusal yasaların bu konuda sınandığı gözlenmektedir. Örneğin, ABD'de unutulma hakkı, genellikle ABD Anayasası'na uyumsuz olarak değerlendirilmiş ve özellikle ifade özgürlüğü ile çakıştığı belirtilmiştir (IFLA, t.y.b.).

2010 yılında Fransa'da internet ortamında "unutulma hakkı" yaratmayı hedefleyen ilk yasal proje ortaya çıkmıştır. Bu hak, online ve mobil şirketleri belirli bir süre sonra veya ilgili kişinin talebi üzerine e-posta ve metin mesajlarını silmeye zorlamayı amaçlıyordu. 2010 Kasım ayında AB Komisyonu, 95/46 sayılı Veri Koruma Direktifi'nin revizyonu kapsamında unutulma hakkını uygulama fikrini ele almıştır (Weber, 2011, s. 120). AB Genel Veri Koruma Yönetmeliği'nin 17. maddesinde "unutulma hakkı" yer almaktadır. Bu hak, bireylere kişisel verilerinin belirli durumlarda silinmesini talep etme yetkisi verir ve veri sorumlularına bu tür talepleri yerine getirme yükümlülüğü getirir. (GDPR, Art. 17). Diğer yandan, AB Adalet Divanı (CJEU), Güvenli Liman çerçevesi ile unutulma hakkı ve kitlesel gözetim konusundaki kararlarda önemli bir rol oynamıştır.

Ulusal mahkemelerin de bu yönde talepleri olmuştur. Ulusal mahkemeler, teknoloji şirketlerinden, kendi ülkelerinde yasal olarak yasaklanmış içeriğin sadece kendi sınırları içinde değil, tüm dünyada kaldırılmasını talep etmişlerdir. Örneğin, Avusturya'daki mahkemeler, Facebook'tan yasal olarak yasaklanmış bir içeriğin

yalnızca Avusturya'da değil, tüm dünyada kaldırmasını talep ederken; Kanada ve Fransa'daki mahkemeler, Google'dan yasal olarak yasaklanmış içeriğin dünya çapındaki arama sonuçlarını kapsamasını talep etmiştir. Ancak bu durum, şöyle bir sorunsalı gündeme getirmiştir: Herhangi bir ülkenin kendi yetki alanları dışındaki ülkelerin neye erişmesi gerektiğine karar vermesi uygun mudur? Bu durumda Google gibi teknoloji şirketleri, internetteki bilgilerin ana dağıtıcıları olarak önemli bir rol oynamaktadır (Kurbalija, 2017). Zira arama motorları, internetteki bilgilerin en büyük dağıtıcılarından biridir. Bu nedenle, unutulma hakkının uygulanmasında önemli bir rol oynamaktadırlar. Bireylerin arama sonuçlarında yer alan bilgileri kaldırma taleplerini yerine getirmekle yükümlü olup olmadıkları, bu alandaki en önemli hukuki tartışmalardan birini oluşturmaktadır (Miyashita, 2016, s. 3).

Mario Costeja González'un "Google Spain" davası, unutulma hakkı için önemli bir dönemeçtir. González, internetteki kişisel bilgilerinin güncel olmayan ve onun itibarına zarar verebilecek bir biçimde arama sonuçlarında görünmesi nedeniyle Google'a karşı mahkemeye başvurdu. Bu durum, CJEU tarafından ele alındı ve sonucunda unutulma hakkının kabul edilmesine yönelik önemli bir karar alındı. CJEU, davada González'in lehine karar verdi. Mahkeme, kişisel verilerin işlenmesindeki sorumluluğun sadece veri kontrolöründe (Google) değil, aynı zamanda veri işleyeninde (Google'ın Avrupa'daki birimi) olduğunu belirledi. Ayrıca, bireylerin geçmişleriyle ilgili kişisel bilgilerin belirli durumlarda silinmesini talep etme hakkına sahip olduklarını kabul etti (CURIA, 2014). Bu karar, Avrupa'da ve dünya genelinde kişisel veri koruması konusunda çeşitli düzenlemelerin yapılmasına ve unutulma hakkının dijital dünyada tanınmasına öncülük etti.

Unutulma hakkı, internetin küresel doğası nedeniyle, geleneksel içerik düzenlemelerinden farklı bir şekilde yetki sorunları ortaya çıkarır. Bu sorunlar, hangi ülkenin hangi faaliyeti düzenleyeceğine bağlıdır. İlk olarak, bir kişinin unutulma hakkı talebi, o kişinin verilerinin o ülkede işlenmesiyle ilgili olabilir. Bu durumda, veri işleyen kişinin o ülkedeki yasalara uyması gerekir. İkinci olarak, bir kişinin unutulma hakkı talebi, o kişinin arama sonuçlarının o ülkede teslim edilmesiyle ilgili olabilir. Bu durumda, arama motorunun o ülkedeki yasalara uyması gerekir. Son olarak ise, bir kişinin unutulma hakkı talebi, dünyanın herhangi bir yerinden yapılan aramalarda o kişinin arama sonuçlarının o ülkede teslim edilmesiyle ilgili olabilir. Bu durumda, arama motorunun dünyanın her yerindeki yasalara uyması gerekir (Bavitz, 2018, s. 3).

2.1.3. Diğer Sosyo-Politik Sorunlar

i. Erişim

Dünya çapında internete erişim hakkı, WSIS tarafından yayınlanan en önemli iki belgede de yer almıştır (2003;2005). İnternet erişimi sorunu, aynı zamanda, BM Düşünce ve İfade Özgürlüğünün Geliştirilmesi ve Korunması Özel Raportörü tarafından hazırlanan 2011 tarihli BM İnsan Hakları Konseyi raporunda da ele alınmıştır. Rapor, internet erişiminin pratik ve hukuki yönlerini inceleyerek internet altyapısına erişimle doğrudan ilgili hususları ele almıştır. Rapor, internet erişiminin ifade özgürlüğü hakkının temel bir bileşeni olduğunun altını çizerek, internetin bireylerin bilgi edinme, elde etme ve yayma haklarını etkin bir şekilde kullanmaları için bir araç olduğunu ifade etmiştir. Dolayısıyla erişimin kısıtlanmasının, yalnızca uluslararası insan hakları standartlarına uygun olarak ve belirli şartlar dâhilinde mümkün olduğu belirtilmiştir. Bu doğrultuda, devletlerin internet erişimini artırıcı politikalar ve eylem planları oluşturmasının önemi de vurgulanmıştır.

Mayıs 2015'te BM Fikir ve İfade Özgürlüğü Özel Raportörü (UNHRC), AGİT, OAS ve Afrika İnsan ve Halkların Hakları Komisyonu'nun (ACHPR) temsilcileri, internet kesintilerini ve "acil anahtarları" (kill switches)[41] kınadıklarını bildirmişlerdir. 2016'da UNHRC, uluslararası insan hakları hukukunu ihlal ederek online bilgiye erişimi veya bilgilerin yayılmasını kasıtlı olarak engellemeye yönelik faaliyetlerde bulunan bütün devletleri "tartışmasız bir şekilde" kınadığını ilan ederken; devletler bugün halen bu tür kısıtlamaları meşru muhalefeti susturmak veya halkın tepkisini bastırmak için siyasi bir araç olarak kullanmaktadır.

BİT, suç grupları tarafından yasadışı operasyonlarda kullanılırken; devletler tarafından içeriği sansürlemek amacıyla kullanılabilmektedir. Devletler BİT'i bilgileri kontrol etmek, seçimleri manipüle etmek, bilgiye erişimi kısıtlamak ve gözetleme amacıyla kullanabilmektedir. Bunun yanında, sahte haberler yaymak ve demokratik süreçlerin sonucunu etkilemek için de kullanırlar (Duberry, 2019, s. 4). İnternete erişim hakkı, fiziksel alandaki ifade özgürlüğünün bir sonucu olarak algılanmaktadır. Bu nedenle, bu

[41] "Acil anahtarlar" veya "kill switches", bir cihazı, sistemi veya yazılımı uzaktan veya otomatik olarak devre dışı bırakmak için kullanılan mekanizmalar veya komutlar anlamına gelir. Bu tür kesintiler, hükümetler veya diğer yetkililer tarafından, genellikle güvenlik endişeleri, kamu düzeninin korunması veya siyasi istikrarsızlık durumlarında bilginin yayılmasını kontrol altında tutmak amacıyla uygulanmaktadır. Ancak, bu eylemler aynı zamanda bireylerin bilgi edinme, ifade özgürlüğü ve barışçıl toplanma haklarını ciddi şekilde sınırlayabilmektedir.

ilkenin pratik uygulaması şimdiden önemli bir zorlukla karşılaşmıştır. Pratikte hiçbir devlet, ifade özgürlüğünün herhangi bir sınırlama olmaksızın kullanılmasına izin vermediğinden, yasal kısıtlamalarını online alanda da uygulamaya çalışmaktadır. Bu nedenle sosyal, politik ve güvenlik gibi nedenlerle sansür veya filtreleme yoluna başvurur. Bu durum, bazı içeriklere erişimin engellenmesi veya sınırlandırılması ile sonuçlanır.

Bugün, erişim hakkı ile ilgili tartışmalara iki zıt bakış açısı hakimdir. Birincisi, internete erişimin kısıtlanmasını hiçbir durumda gerekli görmeyen bakış açısı. Çoğu insan hakları kuruluşu, bu görüşü desteklemekte ve bunu fiziksel alandaki sorunların siber alandaki tezahürü olarak görmektedir. Örneğin, çocuk pornografisine erişimin engellenmesi, sanal olmayan gerçek sorunu çözmeyeceğinden, erişimin engellenmesine karşı çıkmaktadırlar (Kulesza, 2012, s. 142). İkincisi ise, daha çok devlet kurumlarının bakış açısını yansıtan ve internete erişim engelini savunan görüştür. Bu görüşe göre toplumu korumak devletin görevi olduğundan, devlet fiziksel alandaki gibi hareket etmelidir. Dolayısıyla ulusal politika ve hukuka aykırı olduğu düşünülen sitelere erişimin engellenmesini makul bulurlar (Kulesza, 2012, s. 143).

2019'da gerçekleştirilen G7 ve G20 zirveleri de bu konuya güncel bir ışık tutmuştur. Ancak bu konu özellikle teknoloji şirketlerinin yetkilerinin belirlenmesi konusunda tartışmaya konu olmuştur. Örneğin, zararlı veya yasadışı kabul edilen içeriklerin filtrelenmesinin Twitter veya Facebook gibi şirketlerin inisiyatifine bırakılması zamanla bu şirketlerin bağımsız hareket etmelerine veya taraflı bir tutum sergilemelerine yol açabilecektir. Esasen "zararlı" olarak nitelendirilen bir içeriğin aynı zamanda "yasadışı" olup olmadığı genellikle bağlama bağlıdır ve buna yalnızca bağımsız mahkemeler karar verebilmektedir. Ancak bağımsız mahkemeleri devre dışı bırakacak mekanizmaların oluşturulması, "özel sektör sansürünü" gündeme getirebilecektir. Bağımsız yargının özel sektörden başlayarak devre dışı bırakılması beraberinde devket sansürünü de getirecektir (Kleinwächter, 2020).

ii. Kalkınma ve Dijital Bölünme

İnternet, bilgiye erişimi artırarak toplumlardaki farklı seslere daha fazla alan açmıştır. Ancak, buna rağmen, internet kullanımında ve erişimindeki eşitsizlikler, demokratik katılımın tam anlamıyla eşit olmasını engelleyebilmektedir (Ricknell, 2020, s. 110). Öncelikle, internet erişimine sahip olmayan veya sınırlı erişime sahip kesimler, dijital

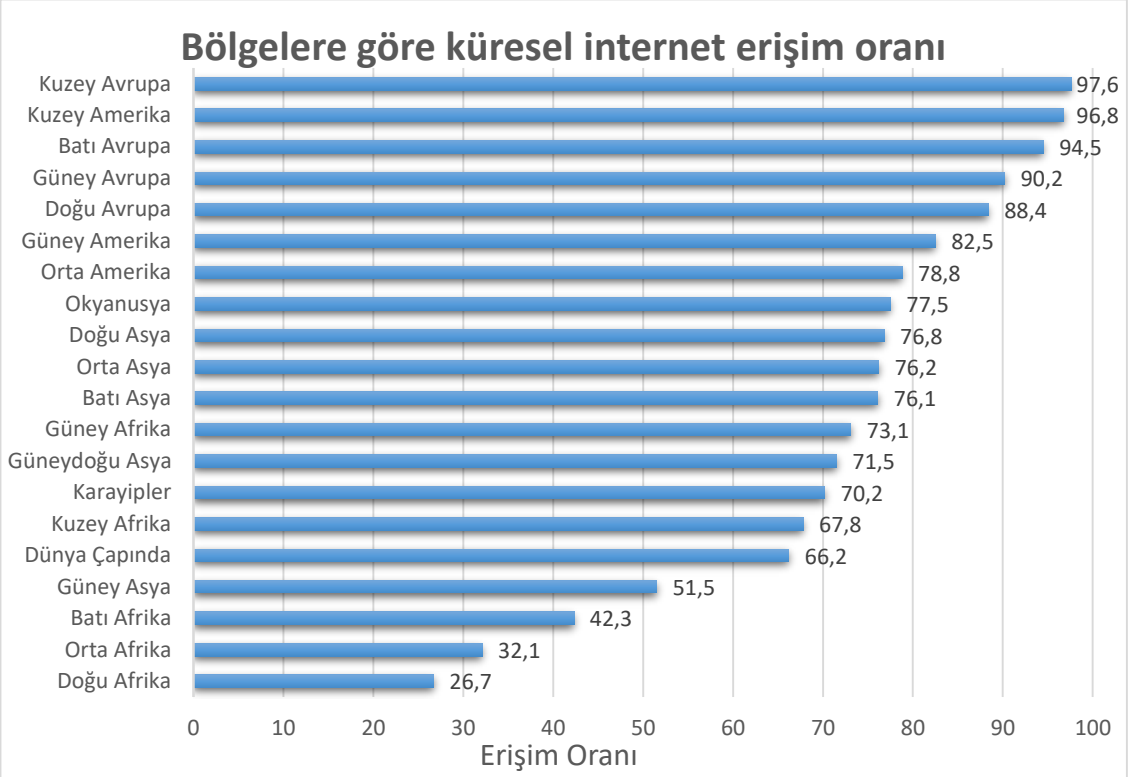
katılımın sunduğu avantajlardan tam olarak yararlanamamaktadır. Eğitim düzeyi, ekonomik durum ve coğrafi konum gibi faktörler, bireylerin internet kullanımına eşit şekilde erişim sağlayamamasına neden olmaktadır ve bu durum, toplumun belirli kesimlerinin dijital demokratik süreçlere tam anlamıyla katılamamasına yol açabilmektedir. Bu sorun, BM dahil olmak üzere tüm internet yönetişimi platformlarında gündeme getirilmekte ve mevcut durumun vehameti sıklıkla dile getirilmektedir.[42]

Küresel düzeydeki erişim sorunu, kalkınma ve dijital bölünmeye[43] de sebebiyet vermektedir. WSIS Bilgi Toplumu Deklarasyonu'nda ve Viyana Deklarasyonu'nda da öngörüldüğü şekilde, tüm insan hakları ve temel özgürlüklerin evrenselliği, bölünmezliği, birbirine bağlılığı ve karşılıklı ilişkisi, kalkınma hakkı da dahil olmak üzere, bir kez daha teyit edilmiştir. Aynı zamanda, demokrasi, sürdürülebilir kalkınma ve insan hakları ile temel özgürlüklere saygı, her düzeyde iyi yönetişimin birbirine bağlı ve karşılıklı olarak güçlendirici olduğu hususunda bir kez daha vurgu yapılmaktadır. Bu kavramsal çerçeve, internet yönetişimi ve kalkınma sorunlarını ele alırken, özellikle erişim, dijital bölünme ve kapasite geliştirme gibi konuları ön plana çıkarır. Ancak erişim, en çok gündem olan internet yönetişimi sorunudur (Kurbalija, 2015, s. 106). Aşağıdaki tablodan da görüleceği üzere erişim sorunu, küresel bir eşitlik ve adalet sorununu doğurmakta, özellikle kırsal alanlardaki mobil geniş bant ağlarının eksikliği ve birçok hanenin internet erişiminden mahrum kalmasıyla gündemde kalmaya devam etmektedir.

[42] 17 Ekim 2023'te BM Genel Kurulu'nun Altıncı Komitesinde gerçekleşen tartışmalar sırasında, teknolojinin insan hakları çerçevesinde herkese adil bir şekilde erişim sağlama kapasitesi ele alındı. Bu görüşmelerde, özellikle gelişmekte olan ülkelerde, teknolojinin geniş kapsamlı kabulü için zaruri olan internet ve dijital altyapı eksikliklerinin önemli bir engel teşkil ettiği vurgulandı. Toplantıda BM İnsan Hakları Yüksek Komiseri Volker Türk, internet erişiminin çocuklar için bir hak olarak güçlendirilmesi gerektiğini belirtmiştir. Türk, internetin modern dünyada temel bir yapı taşı olduğunu ve çocukların eğitim, haber, sağlık bilgisi gibi temel haklara erişiminde giderek daha fazla önem kazandığını vurgulamıştır. Dünya genelinde 2,2 milyar çocuğun internet erişiminden mahrum olduğuna ve bu durumun dijital ayrımı derinleştirdiğine dikkat çeken Türk, internet erişiminin bir hak olarak tanınmasının, bu ayrımın azaltılması ve çocukların dijital ortamda haklarının korunması açısından önemli bir adım olabileceğini ifade etmiştir. Türk ayrıca, çocukların dijital ortamlarda güvenli ve sağlıklı bir şekilde büyüyebilmeleri için alınması gereken önlemlerin altını çizmiştir (OHCHR, 2023).

[43] Dijital bölünme, toplumun farklı kesimleri arasında, bilgi ve iletişim teknolojilerine erişimde ve kullanımda mevcut olan uçurumu ifade eder. Bu bölünme, genellikle internet erişimi, bilgisayarlar ve diğer dijital araçlara erişim gibi teknolojik kaynakların dağılımındaki eşitsizliklerle karakterize edilir. Dijital bölünme, sadece teknolojiye erişimle ilgili bir mesele olmanın ötesinde, bu teknolojileri kullanma becerisi ve dijital okuryazarlık düzeyi gibi faktörleri de kapsar.

Grafik 1. Bölgelere Göre Ocak 2024 İtibariyle Küresel İnternet Erişim Oranı



Kaynak: (Statista, 2024).

Bu anlamda bugün, eşitlikçi ve kapsayıcı bir uluslararası yönetişim sorunu mevcuttur. Özellikle gelişmekte olan ülkelerin uluslararası diyaloglara katılımı, çeşitli nedenlerle sorunlu bir süreçtir. Kuzey'de bulunan gelişmiş ülkeler, toplantılara katılma, inisiyatifleri şekillendirme, anlaşmaları müzakere etme ve nihayetinde sonuçları belirleme gibi süreçlere kaynak, insan gücü ve finansal destek sağlama konusunda daha fazla imkana sahiptir. Buna karşılık, Güney'deki birçok gelişmekte olan ülke bu olanaklardan yoksundur. Bu durum, uluslararası kararların genellikle gelişmekte olan ülkelerin değil, gelişmiş ülkelerin menfaatlerini yansıtmasına neden olmaktadır. Teknik standartlar da benzer şekilde etkilenmekte; sınırlı kaynaklara sahip ülkelerin ihtiyaç ve kapasiteleri yerine, daha zengin ülkelerin teknolojik yeteneklerine dayanarak şekillenmektedir. Bu eşitsiz durum, karar verme forumlarının artmasıyla daha da kötüleşmiştir (Souter, 2021). Peki, internet yönetişimi gibi alanlarda daha fazla kapsayıcılık sağlanabilir mi? Ve eğer sağlanabilirse, bu nasıl gerçekleştirilebilir?

Siber alanda yaşanan jeopolitik değişimler, Çin ve ABD'nin, en büyük 70 dijital platformun piyasa değerinin yüzde 90'ını elinde bulundurmasıyla somut bir örneğini bulmuştur. Bu durum, Afrika ve Latin Amerika gibi bölgelerin ise sadece yüzde 1'lik bir paya sahip olmalarıyla keskin bir kontrast oluşturmuştur. Dijital nüfus dünyanın

birçok yerinde gözle görülür bir şekilde artarken, internet erişimi ve kullanılabilirliği bölgelere göre önemli farklılıklar gösterebilmektedir. İnternet erişiminin küresel ortalamanın oldukça altında kaldığı ülkeler ve bölgeler hala mevcuttur. 2022 itibariyle, Afrika diğer bölgeler arasında en düşük sabit geniş bant aboneliğine sahipken, Asya ve Pasifik en yüksek sayıyı temsil etmektedir. Öte yandan, gelişmiş altyapılara sahip ülkelerde internet bağlantı kalitesinin üstün olması, bu ülkelerin dijital rekabetçilikte öne çıkmasını sağlamaktadır. Örneğin, Singapur'un 2022'de dünya genelinde en hızlı ortalama sabit geniş bant internete sahip olması, bu ülkeyi dijital altyapı ve erişim açısından lider konuma taşımıştır. Bu durum, Güney Sudan ve Somali gibi internete bağlı olmayan insanların oranının son derece yüksek olduğu ülkelerle karşılaştırıldığında daha da belirginleşmektedir (Statista, 2023). Dijital rekabetçilik açısından Danimarka, 2022 yılı itibariyle dünyanın dijital açıdan en rekabetçi ülkesi olmuştur.[44] İsveç, Finlandiya ve Norveç'in de ilk on beşte yer aldığı listede birçok İskandinav ülkesi üst sıralarda yer almıştır. ABD, 2021'de en rekabetçi ülke olarak listelenerek ikinci sırada yer almıştır (Statista, 2022).

Siber alandaki dijital bölünme, sorunların başlangıç noktasını temsil etmektedir. 2015 ve 2020 arasında 4G ağ kapsama alanı küresel olarak iki kat arttı (ITU, 2020b, s. 4). Ancak, küresel nüfusun yaklaşık yüzde 85'i 4G mobil ağından yararlanmaktadır. Bu oran, 2019 itibariyle küresel nüfusun yalnızca yarısından biraz fazlasının online olabildiği anlamına gelmektedir. Dolayısıyla bu sayılar, günümüz itibariyle erişim konusunda tatmin edici seviyelere işaret etmemektedir. Özellikle internet giderek bir zorunluluk haline geldikçe; adil erişimin sağlanması daha da önem kazanmaktadır. Ancak böylesine bir düzenin oluşturulması oldukça karmaşık bir hedef olarak görülmektedir (Sambuli, 2021). Zira uluslararası kuruluşların hedefleri ve sonuç raporlarının da birbirleriyle örtüşmediği görülmektedir. Örneğin BM, 2014 yılında "insanlık tarihinin en hızlı büyüyen teknolojisi" olan mobil geniş bant ağının 2017 yılına kadar küresel nüfusun yarısından fazlasının erişimine açılacağı hedefini koymuştu. Ancak daha sonra bu hedefini 2019'un sonuna kadar uzatmak durumunda kalmıştı (Dreyfuss, 2018). 2019'a gelindiğinde ise küresel olarak kentsel alanlardaki

[44] Dijital rekabetçilik sıralamaları, ülkelerin dijital teknolojileri benimseme, dijital ekonomiye entegrasyon ve dijital inovasyon kapasiteleri gibi kriterlere göre karşılaştırıldığı endekslerdir. Bu sıralamalar, bir ülkenin dijital teknolojileri benimseme ve bu teknolojileri işletmelerde ve devlet kurumlarında uygulama becerisini analiz etmeyi amaçlamaktadır. Örneğin 2023 sıralaması için bkz: IMD. (t.y.). World Digital Competitiveness Ranking. https://www.imd.org/centers/wcc/world-competitiveness-center/rankings/world-digital-competitiveness-ranking/ (05.03.2024).

hanelerin yaklaşık yüzde 72'sinin 2019'da evde internet erişimi vardı, bu kırsal alanlardakinin neredeyse iki katını (yaklaşık %38) oluşturur (ITU, 2020b, s. 6).

Dijital bölünme, COVID-19 pandemisinin ekonomik ve sosyal yaşam üzerinde yarattığı olumsuz etkilerle birlikte daha da şiddetlenmiş ve derinleşmiştir. Özellikle dünyanın her yerinde değişen eğitim sistemi, eğitime erişme hakkı üzerinde olumsuz etkilere sebebiyet vermiştir. Zira bütün düzeydeki öğrenciler, online eğitim sistemi nedeniyle internete ihtiyaç duymuştur. Ancak çoğunluğu internete erişim sağlayamadığı için pandemi koşullarından önemli oranda etkilenmiştir. 190 ülkede okulların kapanması, yaklaşık 1,6 milyar öğrenciyi etkiledi. Dünya çapında bu öğrencilerin en az %31'i (463 milyon) internete ve gerekli diğer cihazlara erişim sağlayamamış ve uzaktan eğitime katılım sağlayamamıştır (ITU/UNESCO Broadband Commission for Sustainable Development, 2021).

Bu büyük dengesizlik, teknolojinin yönetilmesinden çok daha fazlasını, insan hakları gibi temel değerlerin korunması ve geliştirilmesi meselesini de gündeme getirmektedir. Dijital jeopolitikteki bu değişim, internet yönetişiminin evrenselliği ve üniter karakteri üzerinde derin etkiler yaratmaktadır (Souter, 2021). Bu bağlamda, internetin sürdürülebilir ve adil bir yönetişim modeline sahip olup olamayacağı ciddi bir soru işaretidir. Küresel internet yönetişiminin, sadece belirli güç merkezleri tarafından domine edilmesi, internetin evrensel ve eşit erişim ilkelerine ters düşmektedir.

2008 yılında "Sonraki Milyara Ulaşmak" (*Reaching Next Billion*) temasıyla düzenlenen IGF, internet erişiminin küresel eşitsizlik sorununa dikkat çekmesi açısından önemli bir toplantı olmuştur. Altyapısal eksiklikler, coğrafi izolasyon, sosyal ayrımcılık, cinsiyet ve yaş gibi faktörlerin neden olduğu erişim engelleri, Forum'un en önemli sorunlarından biriydi. Bu bağlamda, kablosuz teknolojilere yönelik spektrum düzenlemeleri ve telekomünikasyon sektöründeki standartların yeniden şekillendirilmesi, erişimi genişletme çabalarında kritik öneme sahip olmuştur. Özellikle "son mil" problemi[45] ve kırsal kesimlerdeki bağlantı sorunları, dikkat edilmesi gereken başlıca konular arasında yer almaktaydı (Pizzaleo, 2011). O dönemde, dünya nüfusunun yaklaşık %30'u internete erişebiliyordu ve bu erişim büyük ölçüde gelişmiş

[45]"Son mil" problemi, telekomünikasyon ve internet hizmetlerinde, hizmet sağlayıcının merkezi ağ altyapısından son kullanıcının konumuna (ev, iş yeri vb.) kadar olan son kısmın sağlanmasında yaşanan zorlukları ifade eder. Bu terim genellikle kırsal veya uzak bölgelerdeki kullanıcıları kapsayan ve maliyet, coğrafi zorluklar veya altyapısal eksiklikler nedeniyle hizmetin etkili bir şekilde sunulamadığı durumları tanımlamak için kullanılmaktadır.

ülkelerle sınırlıydı. "Sonraki Milyara Ulaşmak" teması, internet erişiminin küresel bir öncelik olarak kabul edilmesine ve bu alandaki yatırımların artmasına önemli katkıda bulundu. Tema ayrıca, dijital uçurumu kapatmaya yönelik uluslararası çabaların ivme kazanmasına ve çeşitli paydaşlar arasında işbirliğinin gelişmesine yardımcı oldu. Ancak hala önemli zorluklar da mevcuttur. Yaklaşık 3 milyar insan hala internete erişemiyor ve bu insanlar büyük ölçüde gelişmekte olan ülkelerde yaşıyor. Ayrıca, internet erişimi olanlar arasında bile dijital beceriler, içerik ve altyapıya erişim gibi konularda eşitsizlikler devam etmektedir.

Bu durum karşısında, internet yönetişimi gibi kritik alanlarda daha fazla kapsayıcılık ve eşitlik sağlama ihtiyacı gündeme gelmektedir. Ancak dünya genelinde hala erişimden mahrum milyarlarca insanın bulunması ve internet yönetişimi mekanizmalarının büyük ölçüde belirli güç merkezleri tarafından domine edilmesi, bu alandaki eşitsizliklerin ve zorlukların üstesinden gelinmesi gerektiğini bir kez daha göstermektedir. Bu, özellikle teknik standartlar ve politika yapım süreçlerinde gelişmekte olan ülkelerin seslerinin daha fazla duyulmasını gerektirmektedir. Bu doğrultuda gelişmekte olan ülkelerin teknik kapasitelerinin geliştirilmesine yönelik yatırımlar, bu ülkelerin uluslararası diyaloglarda daha etkin roller almasını ve kendi çıkarlarını etkili bir şekilde savunmalarını sağlayabilir. Böylesi bir yaklaşım, küresel internet yönetişiminde daha adil ve eşit bir zemin oluşturarak, WSIS ve Viyana Deklarasyonları'nda vurgulanan kalkınma hakkının korunması ve geliştirilmesi hedefine katkıda bulunabilir.

2.2. Soyut Tartışma: Siber Uzay Yönetilebilir Mi?

Siber uzayda daha fazla düzenlemeye ihtiyaç duyulduğuna dair artan bir konsensüs her halükârda söz konusu iken; tartışma konusu, düzenlemenin gerekliliği değil, nasıl ve ne şekilde yapılacağıdır (IGF Report, 2019). Zira internet yönetişiminin geleceği, devam eden politik bir sorundur. Bugün bu konu, devletler arasındaki uluslararası çatışmanın odak noktalarından biri haline gelmiştir. WGIG'in internet yönetişimi tanımında yer alan "internetin gelişimini ve kullanımını şekillendiren ortak ilkelerin, normların, kuralların, karar alma prosedürlerinin ve programlarının devletler, özel sektör ve sivil toplum tarafından kendi rollerinde geliştirilmesi ve uygulanması" ibaresi aktörlerin rol ve sorumluluklarıyla ilgili fikir verse de, internet yönetişimini neyin oluşturduğuna dair soruları yanıtsız bırakmıştır.

Dolayısıyla bugün internet yönetişimini neyin oluşturduğuna dair soruya verilen cevaplar da çeşitlilik arz etmektedir. Dijital yakınsama (*digital convergence*)[46] olarak adlandırılan teknolojik eğilim, interneti tüm bilgi ve medya türleri için ortak bir platform haline getirdi (Mueller, 2010, s. 9). Saat, telefon, televizyon, bilgisayar gibi çeşitli teknolojik cihazların yaygınlaşmasıyla birlikte başlayan entegrasyon süreci; e-ticaret ve sosyal medya platformlarının yaygın kullanımıyla beraber daha derin bir birleşmeye doğru gitmiştir. Teknik anlamda internet yönetişiminin buradaki etkinliği, daha önceleri ayrı yasal ve düzenleyici rejimler tarafından yönetilen bu teknolojileri TCP/IP adı altında bir araya getirmesi olmuştur.

Bugün tüm dünyayı kapsayan bir ağ olan internet, birçok bilgisayar grubunu ve cihazı birbirine bağlar. Ağ, genel ve özel bileşenlerden oluşmaktadır. Bu nedenle internetin tek bir sahibi olmadığı bilinmektedir. Bu yönüyle internetin sınır aşan, hiçbir devletin veya kuruluşun menşeinde olmayan bir ağ olduğu söylenebilir. Bunun yanında internetin dayandığı temel teknoloji olan kök sunucuları, ağın merkezileştirilmesini gerektirmez. Bu nedenle buradaki temel varsayım, siber yönetişimin herkesi ilgilendirdiği üzerinedir.

Herkesi ilgilendiren bu teknoloji, olağanüstü büyümesi ve yönetişim düzenlemelerinin karmaşıklığı nedeniyle uluslararası ilişkiler alanında önemli bir istikrarsızlık faktörü olarak ortaya çıkmıştır. Lewis tarafından belirtildiği üzere bu durum, devletleri mevcut durumdan sapma ve yeni düzenlemeler arayışına yönlendirmektedir. Bu süreçte internetin genişleyen etki alanı ve yönetişim mekanizmalarının sürekli evrim geçirmesi, uluslararası politika sahnesinde yeni dinamiklerin ve müzakerelerin şekillenmesine zemin hazırlamaktadır (2013, s. 3).

Fiziksel alanda etkin bir yönetişimin önündeki zorluk; güvenlik, düzen, adalet, özgürlük ve refah gibi temel toplumsal değerleri sağlamaya devam edebilmek idi (Aydınlı & Rosenau, 2005, s. 91). Siber alanın yönetişimi ise; veri güvenliği, siber suçlarla mücadele, uluslararası işbirliği eksikliği, teknolojik gelişmelere ayak uydurma, mahremiyet haklarının korunması ve siber egemenlik gibi bir dizi karmaşık zorlukla

[46] Dijital yakınsama, farklı teknolojik alanların birbirlerine doğru ilerleyip zamanla iç içe geçmesini ve sonuç olarak yeni, daha kapsamlı ve çok işlevli teknolojilerin ortaya çıkmasını ifade eder. Başlangıçta birbirinden tamamen bağımsız ve farklı işlevlere sahip cihazlar ve platformlar –saatler, telefonlar, televizyonlar, bilgisayarlar ve sosyal medya platformları gibi– zamanla dijital elektronik ve yazılımın ortak unsurlarını paylaşarak birbirlerine yaklaşmış ve hatta birleşmişlerdir. Bu birleşme, hem donanım hem de yazılım düzeyinde gerçekleşmektedir.

karşı karşıyadır. Fiziksel alanın yönetişiminde karşılaşılan sorunlardan farklı olarak bu zorluklar, büyük ölçüde siber uzayın anonimliği, sınırları aşan yapısı ve hızla değişen doğasından kaynaklanmaktadır.

İnternetin büyük bir hızla gelişmesi, siber uzay için farklı bir yönetişime olan ihtiyacın tartışılmasını zorunlu hale getirmiştir. Tarihsel bir perspektiften bakıldığında nispeten hala yeni olan internet, hemen hemen her elektronik cihazdan erişilebilen bir ağ haline gelmiştir. Bunun yanında internet, getirdiği kolaylıkların yanı sıra birçok çelişkiyi de beraberinde getirmektedir. Katkıları bir yana, yönetişimi başlı başına bir sorundur. İnternetin doğası, aktör çeşitliliği, internetin yalnızca teknik bir mesele olarak ele alınması, internetin yönetişiminde ortaya çıkan işbirliği ve çıkar sorunları siber yönetişim tartışmalarını şiddetlendirmiştir. Zira bahsi geçen, sınırları olmayan bir ağdır.

Peki bunca sınırsızlığın arasında pozitif bir "sınırlılık" mümkün müdür? Gerek siber uzayın doğasından kaynaklanan zorluklar, gerekse de geleneksel yönetişim sorunlarına rağmen siber uzayın yönetişiminin olasılığı var mıdır? Özellikle son yıllarda, bu soruların yanıtlanması için önemli tartışmalar yaşanmaktadır (Mueller & Schmidt & Kuerbis, 2013; Xiaoju, 2015; Liaropoulos, 2017). Bilhassa internete dair düzenlemelerin mahiyeti sorgulanmakta ve yeni düzenlemeler tartışma konusu olmaktadır. Bunun yanında, küresel olarak kabul görmüş resmi bir yapının eksikliği sıklıkla vurgulanmaktadır (Deibert & Crete-Nishihata, 2012; Yongping, 2023). Öngörülen düzenleme biçimlerinde vurgulanan ilkeler genellikle meşruiyet, şeffaflık, hesap verilebilirlik ve katılım gibi iyi yönetişimin temel ilkelerini kapsamaktadır. Bu nedenle iyi yönetişimin olasılıklarını belirlemek de önem kazanmaktadır. Bu bağlamda aşağıda yapılacak incelemede öncelikle siber uzayda yönetişimi zorlaştıran unsurlar hakkında genel bir çerçeve çizilecek, daha sonra siber iyi yönetişimin olasılıkları üzerine değerlendirmeler yapılacaktır.

2.2.1. Siber Uzayda Yönetişimi Zorlaştıran Unsurlar

Küresel internet yönetişimi birçok nedenden dolayı önemli ve karmaşık bir sorundur. Bu sorunun temelinde yatan bazı faktörler vardır. Her şeyden önce, küresel internet yönetişimi, ulusal sınırların ötesine geçen karmaşık ve önemli bir meseledir, çünkü farklı ülkelerin egemenlik hakları ve ulusal yasaları arasındaki çatışmalar, siber güvenlik tehditleri ve veri mahremiyeti gibi konularla iç içe geçmiştir. İnternetin sınırları aşan doğası, her ülkenin kendi içeriğini kontrol etme veya sansürleme

çabalarının başka yerlerde ifade özgürlüğü haklarını ihlal etme potansiyeline sahip olduğunu göstermektedir. Ayrıca, teknolojik eşitsizlikler, dünya genelindeki bazı bölgelerin internetin sunduğu fırsatlardan yararlanamamasına yol açmakta, internet yönetişimindeki paydaşlar arasındaki bölünmeler ise etkili bir denetim mekanizması kurmayı zorlaştırmaktadır.

Siber uzayın sınır ötesi doğası, dijitalleşmenin yaygınlaşması ve her şeyin dijital iz bırakması, özel hayatın gizliliği ve temel özgürlükler üzerinde ciddi etkilere sahip olmaktadır. Bu, demokratik yönetişim ve insan haklarından yararlanma üzerindeki zorlukları artırırken, aynı zamanda devletlerin ve özel sektörün vatandaşların ve tüketicilerin her hareketini izlemesine olanak tanıyarak, demokrasinin temel düzenini tehdit etmektedir.

Bu karmaşık ortamda, küresel internet yönetişimi ile ilgili sorunlar, uluslararası işbirliğini ve çok paydaşlı çözüm arayışlarını zorunlu kılmakta, etkili bir modelin geliştirilmesi için geniş bir paydaş yelpazesinin katılımını ve uzlaşısını gerektirmektedir. Ancak teknolojik gelişmeler hızla artmasına rağmen, paydaşların bu teknolojilerin yönetişimine dair zorlukların üstesinden gelmeleri epey zaman almaktadır. Bugün hiçbir paydaş, küresel dijital yönetişimin zorluklarından muaf değildir. Bir yönetişim mekanizmasının oluşturulmasının önündeki zorlukların listesini yapmak veya sınırlamak mümkün değildir. Zira küresel ağın kapsamı genişledikçe zorluklar da artmaktadır. Dolayısıyla zorlukların kapsamı ve şiddeti zamana ve mekâna göre değişeceğinden, burada sunulan liste spesifik ve ayrıntılı değil, oldukça geniş ve yüzeysel bir çerçeveyi kapsayan bir liste olmuştur.

2.2.1.1.Siber Uzayın Doğası

Uluslararası ilişkilerde uluslararası sistemin anarşik bir düzen içerisinde yer aldığı kabul edilmektedir. Böyle bir ortamda devletler egemen eşit iken güçleri eşit değildir. Dolayısıyla küresel anlamda meşru bir siyasi düzen ve merkezi bir otorite söz konusu değildir. Ancak bu şartlara rağmen BM, uluslararası hukuk kuralları aracılığıyla devletleri dizginlenmeye çalışmaktadır. Bu anlamda BM, bağlayıcı uluslararası yükümlülükler oluşturabilen ve devletlerin bu yükümlülükleri yerine getirmelerini talep edebilen birkaç meşru kurumdan biridir (BM Şartı, Madde 25).

Oysa siber uzay, uluslararası sistemi "yapısal" olarak da değiştiren birtakım dönüşümlere yol açmıştır (Ermağan, 2022b, s. 55). Siber uzayın karmaşık dinamikleri

incelendiğinde, burada da benzer bir anarşi gözlemlenmekle birlikte, durum fiziksel uluslararası ilişkilerden daha farklıdır. Fiziksel uluslararası ilişkilerde anarşi, uluslararası hukuk, uluslararası örgütler, diplomasi ve büyük güçler gibi çeşitli kurumlar tarafından azaltılır ve yönetilebilir hale getirilir. Ancak siber uzayda, bu tür kurumlar ya çok zayıftır, ya yoktur, ya da devlet-dışı aktörler tarafından temsil edilirler (Akyeşilmen, 2018b, s. 1). Bu, siber uzayda daha derin bir anarşi düzeyine, yani "hiper anarşi"ye işaret eder. Siber uzayın bu özelliği, devletler ve devlet-dışı aktörler arasında yeni ve karmaşık güvenlik sorunlarına, siber saldırılara ve savunma stratejilerine yol açar. Buna yönelik Henry Kissinger, 2014 yılında yayımlanan *World Order* adlı kitabında, teknolojinin nihayetinde geleneksel egemenlik ve dünya düzeni algılarımızın sonunu getirebileceğini öne sürmüştür.

Uluslararası ilişkiler teorisi, devletlerin dünya siyasetinde önemli oyuncular olduğu ve devletlerarası anlaşmaların çatışmayı azaltabileceği fikri üzerine kuruludur. Bu teori, 19. ve 20. yüzyıllardaki deneyimlere dayanır ve ulusal sınırlara büyük önem atfeder. Ancak siber uzayın ortaya çıkışı, bu geleneksel bakış açısını derinden etkilemiştir. Zira siber uzay, devletlerin çatışma ve siyasete katılım şeklini değiştiren yeni çatışma ve işbirliği yolları sunmaktadır. Siber saldırılar, uluslararası suç ve casusluğa yeni boyutlar eklerken, siber savaşlar askeri sistemleri bozabilir, devlet sunucularını durdurabilir ve önemli altyapılara zarar verebilir. Her ne kadar siber suçlarla mücadelede işbirliği gibi yeni girişimler olsa da, bu çabalar henüz başlangıç aşamasındadır. Bu nedenle siber uzayın uluslararası ilişkilere etkisi; güç, politika, çatışma ve savaş açısından önemli dönüşümler yaratmaktadır (Choucri & Goldsmith, 2012, s. 70).

Tablo 2. Siber Uzayın Özellikleri ve Yarattığı Sonuçlar

Siber Uzayın Özellikleri	**Etkileri ve Sonuçları**
Sosyal Boyut	-Günümüz teknolojik yaşam tarzını şekillendirir. -Ulusal ve uluslararası konularda farkındalığı artırır. -Ulusal ve askeri güvenlik operasyonlarını karmaşıklaştırır.
Sanal Gerçeklik	-İnsanların birbirleriyle etkileşim kurmalarını ve bağımsız sanal gerçeklikler oluşturmalarını sağlar.
Etkileşimli Yapı	-Kişisel ve kurumsal bilgilerin risk altında olmasına neden olur.

	-Sanal tuzakların ortaya çıkmasına yol açar.
Kırılganlık	-Bilgi kontrolünün zor olması ulusal çıkarların siber saldırılara karşı savunmasız kalmasına yol açar.
Düzenlenmemiş Yapı	-Düzenlenmemiş bir para sistemi gibi işler, manipülasyona açık olabilir.
Anonimlik	-Siber saldırganların kimliklerinin belirlenmesinin zor olması, siber güvenlik için büyük bir sorundur.
Küresel Erişim	-Uluslararası toplum, çok uluslu şirketler ve çeşitli suç faaliyetleri için önemli bir faktördür.
Bağımlılık	-Toplumlar iletişim ve kontrol bağlamında giderek daha fazla siber alana bağımlı hale gelmiştir.
Güvensizlik	-Siber donanım ve yazılımın küreselleşmiş üretimi, güvenlik açıklarını artırabilir.
Ölçeklenebilirlik	-Siber uzayın genişleyebilir doğası, küresel iletişim ve kontrol olanaklarını artırır.
Elitizm	-Operasyonlar genellikle bu alanda uzman bilgiye sahip küçük bir grup tarafından yönetilir.
Kontrol Edilemezlik	-Dağıtılmış yapısı, tek bir kişi veya grubun tam kontrolünü engeller.
Dinamik Yapı	-Sürekli gelişen teknolojiyle birlikte hızla değişir ve yeni güvenlik riskleri oluşturabilir.
Her Yerde Bulunma	-Kapalı sistemlerden ticari kuruluşlara kadar geniş bir yelpazede bulunur.
Ayrımlı Yapı	-Kullanıcıların eylemlerini güvenli bir şekilde doğru aktörlere atfetmelerini zorlaştırır.

Kaynak: Tablo, yazar tarafından (Songip vd., 2013) kaynağından elde edilen bilgilerle oluşturulmuştur.

Siber uzayın karmaşıklığı, onun fiziksel olmayan doğasına ve küresel ölçeğine bağlıdır. Siber uzayda bilgi ve veri, fiziksel sınırları tanımadan hızla hareket edebilir (Akyeşilmen, 2018b, s. 1). Siber uzayın bu özellikleri, onun bir "kamu malı" veya "küresel ortak mal" olarak tanımlanmasına yol açsa da bu tanımlamalar siber uzayın mahiyetine tam olarak uymamaktadır (Canazza, 2018; Raymond, 2012; Surman, 2016). Zira kamu malı, herkesin yararlanabileceği ve hiçbirinin dışlanmadığı bir maldır.

İnternetin bilgi protokolleri kamu malı niteliğinde olabilirken, fiziksel altyapısı kıt bir kaynaktır ve egemen devletlerin sınırları içinde bulunmaktadır. Siber uzay, açık denizler gibi bir müşterek alan değildir çünkü bir kısmı egemen kontrol altındadır. Nye siber uzayı "en iyi ihtimalle, iyi geliştirilmemiş kuralları olan bir 'kusurlu müşterek' veya ortak bir mülkiyetin kat mülkiyeti" olarak tanımlamaktadır (2010, s. 15). Kusurlu müşterek, herkesin yararlanabileceği bir maldır, ancak bazı kurallara tabidir. Ortak mülkiyetin kat mülkiyeti ise, birden fazla kişinin ortak sahip olduğu bir mülktür. Bu durum, siber uzayın asimetrik yapısını anımsatmaktadır. Siber uzaydaki anonimlik, düşük maliyet, yasal belirsizlikler ve çeşitli amaçlar için kullanılabilirliği gibi özellikler, onu hem ulus devletleri hem de devlet dışı aktörleri için cazip kılmaktadır (Sigholm, 2013, s. 1).

Bu anlamda geleneksel yönetişim anlayışının ötesine geçen siber uzay, ulusal güvenlik konularında da yeni bir boyut kazanmıştır. Bu, özellikle 11 Eylül sonrası dönemde, küresel güvenlik yapılanmasında önemli bir değişim yaratmıştır. Siber uzayın doğası, bilgi ve veri akışının hızlanması ve yaygınlaşmasıyla birlikte ulusal güvenlikle ilgili yeni zorluklar ortaya koymuştur. Gelişen bilgi sistemleri, siber uzayın artan kullanımı ile birlikte, devletlerin ulusal güvenlik stratejilerinde önemli bir yere sahip olmuştur. Küreselleşmenin etkisi altında, siber uzayın potansiyelleri, güvenlikten politikaya, ekonomiden sosyale kadar geniş bir yelpazede etkiler yaratmaktadır. Bu durum, devletlerin siber uzaya olan bağımlılığını artırırken, aynı zamanda ulusal savunma ve güvenlik ihtiyaçları üzerindeki etkisini de göz önünde bulundurmalarını gerektirir. Ancak, bu küresel etkileşim ağına bağlılık nedeniyle, siber uzayın bu karmaşık doğasına yeterince önem verilmemiş olabilir (Songip, vd., 2013, s. 1). Bu nedenle siber güvenlik, devlet kurumları ve devlet dışı aktörlerin ortak çabalarıyla sağlanmak zorundadır. Siber suçların uluslararası doğası, etkili bir mücadele için devletler arası işbirliğini zorunlu kılar. Büyük ticari kuruluşlar, sivil toplum kuruluşları ve bağımsız gruplar da siber güvenliğin sağlanmasında önemli roller üstlenirler. Bu çeşitlilik, siber uzayın yönetişimi ve güvenliğinin, fiziksel dünyadaki sosyal kontrol sistemlerinden farklı olarak, daha çoğulcu bir çaba gerektirdiğini gösterir (Chang & Grabosky, 2017, s. 534).

Siber uzayın doğası, uluslararası ilişkilerin geleneksel, devlet odaklı paradigmasına meydan okumakta, yeni çatışma modelleri ortaya koymakta ve aynı zamanda küresel gerilimleri tırmandırma ya da çatışmaları önleme konusunda yeni yollar sunmaktadır.

Bu yeni çatışma türleri arasında uluslararası sınırları aşan suçlar, istihbarat faaliyetleri ve kritik altyapılara yönelik saldırılar bulunmakta iken; bu durum, siber suçlara karşı mücadelede uluslararası anlaşmalar ve diğer işbirliği çabalarının önemini göstermektedir. Bu bağlamda, siber uzayın yönetişimi ve güvenliği, mevcut uluslararası düzeni tamamlayacak yeni kurallar, normlar ve işbirliği mekanizmaları geliştirilerek ele alınmalıdır. Dolayısıyla, siber uzaydaki hiper anarşinin üstesinden gelmek ve siber güvenliği sağlamak için uluslararası toplumun bütünleşik bir yaklaşım benimsemesi gerekmektedir. Bu yaklaşım, devletlerin yanı sıra özel sektör, sivil toplum ve teknoloji topluluklarını da içeren çok paydaşlı işbirliklerini teşvik etmeli ve siber uzayın barışçıl kullanımını desteklemelidir.

2.2.1.2.Aktör Çeşitliliği

Siber uzay, çok sayıda aktörü içerir ve bu aktörlerin her birinin teknik altyapı ve politik süreçler üzerinde farklı düzeylerde kontrolü ve etkisi vardır. Bu da yönetişim mekanizmasının inşasında ciddi bir karmaşıklığa yol açar. Bu karmaşıklık, onu yönetme sorumluluğunun kimde olduğu konusunda sürekli bir tartışma alanı açmıştır. Çok sayıda aktörün varlığı, teknik altyapı ve politik süreçler üzerindeki kontrol ve etkinin dağıtılmasını gerektirirken, bu durum yönetişim mekanizmasının oluşturulmasını da zorlaştırmaktadır. Zira internetin yönetişimi, teknik ve politik kararların bir araya gelmesiyle şekillenen bir alan haline gelmiştir. Dolayısıyla, internetin kim tarafından yönetildiği sorusuna verilecek yanıt, yönetişimin çok katmanlı ve disiplinler arası bir çaba olduğu gerçeğini göz önünde bulundurmayı gerektirir. Bu alan, teknik uzmanların ötesine geçerek politika yapıcıları, özel sektör temsilcilerini, sivil toplum kuruluşlarını ve son kullanıcıları da içermektedir. Bu geniş aktör yelpazesi, internet yönetişiminin yalnızca teknik kuralları değil, interneti yöneten kuralların şekillendirilmesinde söz sahibi olma ve rol oynama hakkını ifade ettiğini göstermektedir.

İnternet, ilk olarak devlet istihbarat servisleri arasında bilgi paylaşımı amacıyla sınırlı araştırmacı ağları tarafından kurulmuştur. Sonrasında online faaliyetler için "iç düzenleyici sistemler" aracılığıyla geliştirilmeye başlanmıştır (Bonnici, 2008, s. 9). Online faaliyetlere yönelik geliştirilen bu kuralları bir “öz düzenleme” biçimi olarak tanımlayan bir grup mevcuttur (de Vey Mestdagh & Rijgersberg, 2010; Koops vd., 2006). Çoğu yazar tarafından kabul edilen bu görüşe karşın Lessig, başlangıçta internetin donanım ve yazılım gibi teknik araçları temsil eden, insanlar tarafından

geliştirildikçe sürekli değişime uğrayan bir kod tarafından yönetildiğini ileri sürmüştür (2006, ss. 78-79). Temelde, birbirine yakın görünen bu iki görüş arasındaki yaklaşım farkı, Lessig'in "insan" faktörünü de sürece dahil etmesinden kaynaklanmaktadır. Buna rağmen Lessig'in yaklaşımının teknolojinin kendisine daha fazla ağırlık verdiğini söylemek mümkündür. Görüldüğü üzere internet yönetişimine yönelik ilk yaklaşımlar birbirine benzer veya zıt fark etmeksizin herhangi bir devlet düzenlemesi ile ilişkili değildir. Bunun yanında, siber uzayın tamamen devletlerin kontrolü dışında bir alan olması gerektiğini savunanlar da mevcuttur (Barlow, 1996).

İnternet yönetişiminin ilk kuşağında bireysel şahısların güçlü etkisi söz konusu olmuştur. Yukarıda saydığımız kuruluşların üyeleri arasında bireysel anlamda öne çıkan isimler mevcuttur. Öne çıkan isimler arasında Jon Postel, Vinton Cerf ve Tim Berners-Lee bulunmaktadır. Bu isimler, internetin ilk teorik temellerini ortaya koymaları ve orijinal protokolleri geliştirmeleri gerekçesiyle internetin gelişimi üzerinde öncü olarak kabul edilmişlerdir. Bu isimlerin öne çıkması, bazı yazarların internet yönetişiminin belli bir dönemini "şahsi" olarak nitelendirmesine sebebiyet vermiştir. Örneğin Bygrave ve Michelsen, internet yönetişimini 1970'lerden 1990'ların sonlarına kadar yukarıda bahsi geçen şahısların öne çıkması gerekçesiyle "şahsi" (*personal*) nitelendirmişlerdir (2009, s. 93). Bu dönemden itibaren kuruluşlar, bu kişilerden internet yönetişimini giderek devralmaya başlamıştır.

İlk nesil internet yöneticilerinin başlıca sorumluluk alanları, internet mimarisi ve altyapısının yönetişimidir. Bunlar yöneticiliği IP ve HTTP gibi protokollerin ve uygulamaların tasarımı üzerinde kullanırlar. Bunu yaparken bu protokol ve uygulamaların tasarım ilkelerinin korunmasına özen göstermişlerdir. Aynı zamanda, "*decisional principles*" olarak adlandırılan karar verme ilkeleri üzerinde de bazı düzenlemeler yapmışlardır (Bygrave & Michaelsen, 2009, s. 94). Bu konuda IETF'nin desteklediği tek bir kişinin görüşünün uygulanmasından ziyade tüm katılımcıların rızasının alınmasını öngören kaba fikir birliği (*rough consensus*) ve mühendislik ürünlerinin çalıştırılmasını ve öne çıkmasını öngören çalışan kod (*running code*) ilkeleri öne çıkmıştır (Resnick, 2014).

Günümüzde ise hiçbir taraf, interneti tamamen kendi kurallarına göre şekillendirme kapasitesine sahip değildir. İnternet yönetişimi; devlet, özel sektör, akademi ve sivil toplum temsilcileri de dahil olmak üzere tüm paydaşları interneti yöneten kuralları

tartışmak için bir araya getirmeyi gerektirir. Ancak dünyadaki internet trafiğinin yönetimi, herhangi bir devletin menşeinde olmayan bazı kuruluşlar tarafından üstlenilmiştir. Bygrave ve Michaelsen de internet yönetişiminin birtakım özel, kamusal, eski ve yeni organlar tarafından oluşturulduğunu belirtmişlerdir. Onlara göre bu organların etkileşiminden kaynaklanan yönetişim yapısı geçici ve özgünlükten uzak görünmektedir. Üstelik bu organların etkinlik ve finansman bakımından sorumluluk almada başarısız olduklarını iddia etmişlerdir (2009, s. 92).

Bu aktörler, oluşturdukları tehditler bağlamında değerlendirilecek olursa; siber alanda işlenen suçlara yönelik hesap verilebilirlik mekanizmasının olup olmadığına bakılmalıdır. Bu durumda yalnızca yukarıda ana aktörler arasında saydığımız geleneksel devlet-dışı aktörlere değinmek eksik bir yaklaşım olacaktır. Zira bir devletin azmettirmesiyle hareket eden vekil aktörlerin (*proxies*) varlığı da azımsanmayacak derecede fazladır. Bu aktörler, farklı bir yönetişim zorluğuna sebebiyet vermektedir. Devletlerin herhangi bir suç teşkil edecek eylemlerinde uluslararası hukuk devreye girerken; devlet dışı aktörler, uluslararası hukuk kapsamında herhangi bir yükümlülük taşımazlar. Dolayısıyla bu durum, devlet dışı aktörleri herhangi bir suçu işlemekten caydırabilecek bir mekanizmanın yokluğuna işaret etmektedir.

Devletler, siber uzayda kuvvet kullanmak amacıyla çeşitli vekil aktörden yararlanırlar. Maurer siber vekilleri; "bir varis tarafından ister aktif ister pasif olarak kasten devreye sokulan, saldırgan bir siber eylemi gerçekleştiren veya buna doğrudan katkıda bulunan aracılar" olarak tanımlar (2018, s. xi). Vekil ilişkileri genellikle yetkilendirme, düzenleme ve yaptırım gibi unsurlar üzerinden gerçekleşmektedir. Özellikle bu üç unsur, bir ulus-devletin vekâlet ilişkisinde sahip olduğu güç seviyesini göstermektedir.

Bununla birlikte, devlet dışı aktörler hakkında düzenleme ve uygulama mekanizmalarına ilişkin bilgi boşluğu mevcuttur. Tallinn Manual'in Uluslararası Uzmanlar Grubu (IGE), siber faaliyetlerin normatif bir boşlukta bulunmadığını; mevcut uluslararası hukukun siber operasyonlar için de geçerli olduğu yönünde görüş bildirmiştir (Jensen, 2017). Bu görüşe göre internet yönetişimi, yalnızca ulus-devletler tarafından düzenlenen egemenlik kavramına dayanamaz. Resmi uluslararası yönetim mekanizmaları, siber uzay sınırlarının küresel olarak anlaşılması ve anlaşmazlıkların çözülmesi için gerekli olan kolektif eylem açısından elzemdir.

IGE, Tallinn Manual'da uluslararası hukukun siber alana uygulanabileceğini belirtmiştir. Ancak bunun aksini iddia eden yaklaşımlar da mevcuttur. Zira uluslararası hukuk, yalnızca devletleri süje olarak kabul eder ve onlar üzerinden bir hukuk düzeni inşa eder. Oysa siber alanda devlet dışı aktörler çoğu durumda devletlerden bile daha etkin bir konumda olabilmektedir. Dolayısıyla bu durum, küresel internet yönetişime devlet-dışı aktörlerin de dahil edildiği alternatif yaklaşımlar gerektirmektedir. Çok sayıda paydaş, uluslararası alanda siber stratejileri etkilemekte hatta çoğu durumda yön vermektedir. Bu nedenle tek bir aktör üzerinden kurulacak bir düzenleyici mekanizmanın varlığı söz konusu değildir. Bilakis, küresel siber yönetişim mekanizması, bütün aktörleri bünyesinde barındıran siber topluluğun çok yönlü ve çok taraflı bir yaklaşımı temsil etmelidir.

Henüz aktörlerin rol ve sorumluluklarına rehberlik edecek herhangi bir parametre üzerinde uzlaşmaya varılamamıştır. Bu rol ve sorumluluklar zamana bağlı olarak farklılık arz etse de yönetişim sorununu derinleştirmektedir. Zira bu paydaşlar; politikalar, normlar ve kurallar gibi faktörlerin geliştirilmesi ve uygulanmasında rollerini kendi çıkarları doğrultusunda kullanabileceklerdir. Bu nedenle internet yönetişiminde aktörlerin her birine ayrı bir konuda otorite sağlanması, yararlı bir formül olarak görülmemektedir. Dolayısıyla çok paydaşlı süreçlerdeki esneklik ve paydaşlara atfedilen rol ve yetkilerin genişliği, internet üzerindeki etki alanıyla uyumlu olarak kabul görmemiştir.

2.2.1.3.Teknik Bakış Açısı

İnternetin erken dönemlerinde, ağırlıklı olarak teknik bir altyapı olarak görülmesi ve kullanılması, bu alanda çalışanların çoğunlukla mühendis ve teknisyenlerden oluşmasına yol açmıştır. Bu durum, internetin politik, sosyal ve ekonomik yönlerinin, özellikle de yönetişim ve güvenlik politikalarının geliştirilmesinde yeterince dikkate alınmamasına sebep olmuştur. Ancak, internetin küresel etkileşim ve iletişimde merkezi bir role sahip olmasıyla birlikte, siber güvenlik konuları da dahil olmak üzere, internet yönetişimi ve politikası üzerine yapılan tartışmaların kapsamı genişlemiştir.

Yukarıda bahsi geçen internetin ilk dönemlerindeki teknik merak, 1990'larla birlikte ticarileşme ve genel kabul görmesiyle çok boyutlu bir mahiyete bürünmüştür. Artık sadece teknik bir ağ olmanın ötesine geçen internet, tüm dünyadaki kullanıcılar için temel bir iletişim ve ticaret aracı haline gelmiştir. Küresel çapta yaygın bir gözetim

aracı olma özelliği kazanan internet, ulusal sınırları aşarak küresel bir karakter kazanmıştır. Dolayısıyla internetin "küresel bir güç alanı" olarak tanımlanması, onun günümüzdeki rolünü ve etkisini doğru bir şekilde yansıtmaktadır (Radu, 2019, s. 1).

İnternet yönetişiminin açıklanmasında bazı tanımlar ve kurumlar öne çıkmaktadır. Ancak bu tanımlamalar internet yönetişiminin sınırlarının belirlenmesi için oldukça "teknik" kalmaktadır. Halbuki internet yönetişimi, yukarıda özetlendiği kadar yalın ve teknik kalıplara sığdırılamayacak kadar geniş bir konuyu kapsamaktadır. İnternet yönetişimi, yalnızca kuralların yasalara uygun şekilde uygulanması anlamına gelmez. Zira teknik standartlar çoğu zaman konuya dahil olan herkes arasında fikir birliği yoluyla oluşturulur. Bugün internet yönetişimi üzerine yürütülen tartışmalarda genellikle yönetişimin teknik mi, politik mi olduğu noktasında bir uzlaşma sağlanamamasının en önemli nedenlerinden birini bu ikilem oluşturmaktadır (Akyeşilmen, 2018a).

İnternetin başlangıcında teknik unsurların ön plana çıkması, siber uzayın nasıl şekillendiğini ve geliştiğini anlamak için elzemdir. Ancak, DeNardis ve Mueller gibi yazarlar, zamanla siber güvenliğin, internet politikası ve yönetişimi tartışmalarında baskın bir tema haline geldiğini, diğer önemli konuları gölgede bıraktığını ve hatta "kendi başına bir yaşam" sürdüğünü vurgulamaktadırlar. Bu, siber güvenlik politikasının, ifade özgürlüğü, erişim, açıklık ve kalkınma gibi konuların yanı sıra küresel teknik altyapı ve çok paydaşlı yönetişim konularını kapsaması gerektiği anlamına gelir (2020, s. 191; 2017, s. 416).

DeNardis'in (2020) vurguladığı gibi, "siber" terimi genellikle siber savaş, siber çatışma ve siber güvenlik bağlamında kullanılırken, "internet" terimi daha çok küresel teknik altyapı, çok paydaşlı yönetişim ve ifade özgürlüğü gibi konuları içermektedir. Bu ayrım, internet politikası ve yönetişimi tartışmalarında farklı perspektif ve önceliklerin var olduğunu göstermektedir. Benzer şekilde Mueller'in (2017) işaret ettiği gibi, siber güvenlik, internet politikası tartışmalarında o kadar baskın bir konu haline gelmiştir ki, bu durum diğer önemli konuların göz ardı edilmesine neden olmaktadır. Bu, siber güvenlik politikalarının geliştirilmesinde dengeli bir yaklaşımın benimsenmesi gerektiğini, yani hem teknik hem de politik unsurların dikkate alınması gerektiğini göstermektedir.

Venables (2021), siber uzayı çok yönlü bir yaklaşımla ele almayı amaçlamaktadır. Siber uzayın yalnızca teknolojik yönlerini değil, aynı zamanda coğrafi, siyasi ve zamansal boyutlarını da kapsayarak, bu alanın dinamik doğasını modellemeyi hedeflemektedir. İlk olarak, siber uzayın çeşitli özelliklerini ve kullanım şekillerini inceleyerek, bu ortamın temel bileşenlerini tanımlıyor. İkinci olarak, siber uzayı bir iletişim ortamı olarak ele alıp, veri akışının kaynağından hedefine kadar olan yolculuğunu detaylandırıyor. Üçüncü ve son olarak, güvenlik boyutuna odaklanarak, siber tehditler ve bu tehditlere karşı siber güvenliğin çok boyutlu ve insani yönlerini vurguluyor. Böylece, Venables siber uzayı sadece teknolojik bir fenomen olarak değil, aynı zamanda coğrafi, siyasi ve zamansal yönleri barındıran bir alan olarak görmektedir.

Sonuç olarak internet yönetişimi, hem teknik hem de politik boyutları olan karmaşık ve çok boyutlu konulardır. Teknik altyapı ve güvenlik önlemlerinin yanı sıra, ifade özgürlüğü, erişim, açıklık ve kalkınma gibi konuları içeren geniş bir perspektiften ele alınmalıdır. Bu, sadece güvenlik araştırmacıları ve devletler tarafından değil, aynı zamanda sivil toplum, özel sektör ve akademik çevreler tarafından da katılımcı ve kapsayıcı bir yaklaşım gerektirir. Teknik çözümlerin etkin bir şekilde uygulanabilmesi için, politik ve teknik konuların birbiriyle entegre edilmesi gerekmektedir. Bu entegrasyon, çoğu zaman zorlu olabilir ve çözümlerin etkinliğini sınırlayabilir. Bu nedenle "işbirliği" faktörü kaçınılmazdır. Ancak bu işbirliğini yalnızca teknik düzeyde gerçekleştirip politik düzeyi göz ardı etmek, eksik ve sorunlu bir yaklaşımı temsil edecektir. Zira bu süreç, hem teknik hem de politik boyutları kapsayıcı bir yaklaşım gerektirir. Bu, sadece güvenlik açıklarını kapatmakla kalmayıp, aynı zamanda dijital gelişmelerin toplum üzerindeki geniş etkilerini de yönetebilecek bir yönetişim modelinin inşası anlamına gelir.

2.2.1.4.İş Birliği/Çıkar İkilemi

2019'da BM Genel Sekreteri tarafından başlatılan BM Yüksek Düzeyli Dijital İşbirliği Paneli'nin hazırladığı bir raporda geçen "siber karşılıklı bağımlılık çağı" ibaresi oldukça önemlidir. Bu ibarede, siber uzayın yalnızca cihazları veya insanları değil, yönetişimde söz sahibi olan diğer bütün paydaşları da birbirine bağladığı ifade edilmektedir. Burada geçen "siber karşılıklı bağımlılık" ibaresinin farklı anlamları bulunmaktadır. Burada hiçbir devletin ve hiçbir paydaşın tek başına hareket edemeyeceği ifade edilmektedir. Bunun yanında, internetle ilgili tüm politik ve teknik

konuların birbiriyle bağlantılı olduğu kabul edilmektedir. Bu durum, siber yönetişimin paydaşları için en büyük zorluklardan birini teşkil etmektedir. Rapor; bireyler, kurumlar, şirketler ve devletlerin dijital gelişmeleri tek başına yönetemeyeceklerini kabul ederek "işbirliği" faktörünü zorunlu kılmıştır. Bu bağlamda küresel sorunların ve güvenlik açıklarının "birbirine bağlı ve bağımlı" olduğunu savunmaktadır (UN News, 2019).

Panelde de vurgulandığı gibi, siber uzayın doğası gereği, cihazlar, insanlar ve yönetişimde söz sahibi olan diğer tüm paydaşlar arasında derin bağlantılar kurulmaktadır. Bu bağlantılar, hiçbir devletin veya paydaşın izole bir şekilde hareket edemeyeceği bir ortam yaratırken, internetle ilgili tüm politik ve teknik konuların birbiriyle iç içe geçmiş olduğunu da göstermektedir. Siber uzaydaki her bir bileşenin diğerleriyle olan karşılıklı bağımlılığı, teknik bir karmaşıklık yaratır. Dolayısıyla bir noktada yapılacak bir değişiklik veya güvenlik açığı geniş çapta etkilere sebebiyet vermektedir.

Devletlerin düştüğü en büyük yanılgı, siber alanı fiziksel alandakine benzer bir motivasyonla yönetmeye çalışmalarıdır. Fiziksel uluslararası sistemde merkezi bir otoritenin bulunmadığı anarşi ortamı ve uluslararası hukuk mekanizmasının tepesinde yer alan BM Güvenlik Konseyi'ndeki sürekli üyeler arasında yer alan güç mücadelesi nedeniyle küresel yönetişimin işlemez hale gelmiştir. Oysa siber alanda bu durum çok farklı bir şekilde tezahür etmektedir. Siber alandaki güç mücadelesi de, işbirlikleri de çok yönlüdür ve çok fazla aktörü ilgilendirir. Zira siber alanda işbirliğinin önemi, sadece devletler arası çıkar çatışmalarından kaynaklanmaz; devlet dışı aktörlerin katılımı ve bu işbirliğine olan hayati ihtiyacı da kapsar. Özellikle devletlerin egemenliklerini öne sürerek devlet dışı aktörlere eşitlik tanımamaları, işbirliği çabalarında önemli bir engel teşkil eder. Bunun yanında, devletlerin siber alanı hukuk dışı bir mecra olarak görmeleri ve buna göre hareket etmeleri de işbirliği ve ortak bir siber güvenlik anlayışının geliştirilmesini zorlaştırır.

Zorlu ancak umut verici bir yaklaşım, kamusal ve özel çıkarları uzlaştırmak, bunları birbirleriyle çatışmaktan ziyade tamamlayıcı olduğu alanları bulmaktır (Senges & Horner, 2009, s. 15). Kritik altyapının korunması için kamu-özel sektör işbirliği

1990'lara kadar uzanmaktadır.[47] ICANN örneğinde olduğu gibi, devletlerin, şirketlerin ve bireylerin işlevsel uluslararası yönetişim modelleri geliştirmek için birlikte çalıştığı çok paydaşlı modeller mevcuttur. Kamu ve özel sektör arasındaki etkileşim, birçok gelişmiş ekonomide siber güvenlik ilişkisinin temelini oluşturur. Ancak bu ilişki karmaşıktır. Devletin rolünü haklı çıkarmadaki zorluklar, mahremiyet endişeleri ve devlete aşırı güven konusundaki tereddütler göz önüne alındığında, gerçek çok paydaşlı yönetişim ve temsil yöntemlerine ihtiyaç vardır (Valeriano & Maness, 2017, s. 267). Arner vd. (2021), büyük ekonomiler arasındaki farklılıkların artması, teknolojik ve jeopolitik rekabet ve çatışmaların yükselmesi sonucu veri akışlarında ve ilgili yönetişim çerçevelerinde bir parçalanmanın ortaya çıktığını ifade etmektedir. Bu durum, internetin temel altyapısını tehdit etmekte ve küresel işbirliği mekanizmalarını bozarak daha karmaşık bir ilişkiler ağına sebebiyet vermektedir. Bu karmaşık ilişkiler ve çıkar çatışmaları bağlamında devlet ve özel sektör arasındaki etkileşim, siber güvenlik politikalarının etkinliğini belirleyen temel faktör haline gelmiştir.

Bu alanda ortaya çıkan çıkar çatışmaları, farklı aktörlerin işbirliğini ve ortak bir zeminde buluşmasını zorlaştırmaktadır. Devlet denetim organları, genellikle doğrudan sorumlu oldukları kamu kurumlarını denetler. Bu denetimler genellikle yalnızca kamu kurumlarına odaklanır ve özel sektör ortaklarını kapsamaz. Bu durum, özel sektör ortaklarının kamu kurumlarıyla yakın işbirliği içinde olsalar bile, denetimden kaçınmalarına olanak tanıyabilmektedir. Almanya Parlamentosu'nun yabancı devletlere gözetleme teknolojileri satışını araştırması, bu sorunun bir örneğini göstermektedir. Bu soruşturma, Alman hükümetinin son on yılda gözetleme teknolojilerini ihracat lisanslarıyla en az 25 ülkeye sağladığını ortaya çıkardı. Bu ülkelerin çoğu, insan hakları ihlalleriyle uzun süredir tanınıyordu. Soruşturmanın bir sonucu olarak, Alman hükümeti insan haklarına zarar veren gözetleme teknolojilerini düzenlemek için uluslararası düzeyde daha fazla lobi yapma sözü verdi. Benzer şekilde İsveç'in siber güvenlik stratejisi de özel aktörlerin oynadığı önemli rolü kabul etmiştir. Ancak

[47] 1997'deki Marsh Komisyonu (resmi adıyla Başkanın Kritik Altyapı Koruma Komisyonu), kritik altyapının korunması konusunda kamu ve özel sektör arasında işbirliğinin önemini vurgulayan bir dönüm noktası oluşturdu. Bu komisyon, kritik altyapıların korunması gerekliliğine dikkat çekmek ve bu alanda bir strateji geliştirmek amacıyla kuruldu. Komisyon, kamu ve özel sektörün bir araya gelerek, kritik altyapıları oluşturan sistemlerin ve varlıkların güvenliğini sağlamak ve bu altyapıların sürekliliğini garanti altına almak için çalışmalar yürütmüştür. Bu çabalar, özellikle siber güvenlik alanında olmak üzere, kritik altyapıların korunmasında yeni bir dönemin başlangıcı olarak kabul edilir. Belgeye ulaşmak için bkz: DTIC. (1997). Securing, Protecting Critical U.S. Infrastructures. https://apps.dtic.mil/sti/citations/ada342375.

parlamento komitelerinin bu aktörleri yeterince denetlemesine izin veren yetkileri bulunmadığından etkin denetim mümkün değildir. Bununla birlikte, stratejik ilkelerin belirlenmesi ve sivil toplumun katılımı gibi iyi uygulamalar da mevcuttur. Bunlar, İsveç'in siber yönetişimde hesap verilebilirliği ve şeffaflığı artırmasında önemli rol oynamaktadır (DCAF, 2019, s. 15-16).

İnternetin düzenlenmesi ve siber güvenlik konusundaki uluslararası tartışmalar, yukarıda bahsedilen denetim sorunlarının bir yansımasıdır. Özellikle, devlet ve özel sektör arasındaki işbirliğinin sınırlarını ve denetim mekanizmalarının etkinliğini vurgulayan bu sorunlar, internetin düzenlenmesi konusunda da benzer zorluklara yol açmaktadır. Bu nedenle interneti düzenleme meselesi uluslararası düzeyde birden fazla aktör ve çıkarı içeren jeopolitik bir çatışmanın merkezinde yer alsa da, devlet boyutundaki çıkar çatışmaları daha belirgindir ya da nispeten daha "görünür" bir formdadır. Özellikle hükümetlerarası zirve ve platformlara yansıyan büyük çaplı tartışmalar, devletlerin diğer aktörlerden ziyade birbirleriyle de büyük bir çatışma halinde olduğunu göstermiştir. Zira önde gelen tüm büyük güçler, yanı sıra daha düşük düzeyde demokrasiye veya otoriter rejimlere sahip ülkeler, bu yeni iletişim boyutunun kontrolünü elinde tutmaya kararlı görünmektedir. Bunun nedeni, internetin yasal rejimine ilişkin tartışmaların, ulusal ve uluslararası politika yapıcı organların gündeminde zorlayıcı ve tartışmalı bir konu olarak kalmaya mahkûm olmasıdır (Lucchi, 2014, s. 855). Bu tartışmaların temel nedeni, internetin demokratik ve otoriter rejimler için farklı anlamlar ifade etmesidir. Demokratik rejimler için internet, ifade özgürlüğü ve bilgi edinme özgürlüğünün önemli bir aracıdır. Otoriter rejimler için ise internet, muhalefeti kontrol etmek ve baskılamak için kullanılabilecek bir araçtır. Bu durum, fiziksel alanda da olduğu gibi bir güç mücadelesine dönüşebilmektedir. ABD, AB, Çin ve Rusya gibi aktörler teknolojik liderlik için rekabet etmekte ve siber uzaydaki ulusal çıkarlarını korumaya çalışmaktadır. Bu nedenle siber yönetişim üzerinde şiddetli bir "çatışma alanı" vuku bulmuştur.

Siber uzayın karmaşık doğası ve iç içe geçmiş sorunları göz önünde bulundurulduğunda, uluslararası işbirliği ve çok paydaşlı yaklaşımların önemi daha da belirginleşmektedir. Teknolojinin sınırları zorlayan gelişimi, ulusal sınırların ötesindeki etkileşimleri artırmakta ve bu da siber güvenlik, veri koruma ve internet yönetişimi gibi konularda ortak standartlar ve politikalar geliştirmenin zorunluluğunu ortaya koymaktadır. Devletlerin, özel sektörün ve sivil toplumun bu süreçteki rolleri, karmaşık

ve birbiriyle bağlantılı sorunlara çözüm bulmada kritik öneme sahiptir. Bu çerçevede, BM Yüksek Düzeyli Dijital İşbirliği Paneli'nin vurguladığı gibi, "siber karşılıklı bağımlılık çağı"nda işbirliği ve çok paydaşlı diyaloglar, siber uzayın yönetişimi için en etkili yol olarak öne çıkmaktadır. Sürdürülebilir ve kapsayıcı bir dijital gelecek inşa etmek, bu tür bir işbirliğine bağlıdır.

2.2.2. Siber İyi Yönetişim Mümkün Mü?

Yukarıda bahsedildiği üzere siber uzay, ulusal sınırları aşan ve çeşitli aktörlerin faaliyet gösterdiği küresel bir alandır. Bu durum, siber uzayın yönetişimini karmaşıklaştırır. Siber uzayın yönetişimi, farklı roller ve sorumluluklara sahip birçok farklı aktör tarafından karakterize edilir. Siber uzayda politika oluşturma ve düzenleyici çerçeve geliştirme süreci, bu kadar çok sayıda aktör tarafından yönlendirildiğinde karmaşık, külfetli ve etkisiz olabilmektedir. Üstelik bu zorluklar siber uzayda iyi yönetişim ilkelerinin etkili bir şekilde nasıl uygulanacağına dair bilgi eksikliği ile birleştiğinde, kötü yönetişimle sonuçlanabilmektedir (DCAF, 2019, s. 12). Olası bir kötü yönetişim, bu sınırsız alanın negatif güvenlik yaklaşımlarıyla parçalanmasına sebebiyet verecektir. Tam da bu noktada yukarıda sorulan "Peki bunca sınırsızlığın arasında pozitif bir 'sınırlılık' mümkün müdür?" sorusunun yinelenmesi elzemdir.

Bu sınırlılığın sağlanması için iyi yönetişim, siber uzayın etkili ve sorumlu bir şekilde yönetilmesini sağlamada önemli bir rol oynayabilir. Küresel siber iyi yönetişim, birçok temel unsuru içerir ve bu unsurların her biri, etkin ve adil bir yönetişim yapısının oluşturulmasında kritik öneme sahiptir. İyi yönetişim, şeffaflık, demokrasi, hesap verebilirlik, katılımcılık, hukukun üstünlüğü, etkililik ve verimlilik, eşitlik ve adalet gibi temel ilkeleri kapsar. Bu bağlamda küresel siber iyi yönetişimin mümkün olup olmadığını tartışırken bu unsurların detaylı bir şekilde incelenmesi gerekir.

İyi yönetişim, insan haklarına ve hukukun üstünlüğüne saygı gösterilmesini sağlamaktır. İyi yönetişimin amacı; demokrasiyi güçlendirmek ve yönetimde şeffaflığı ve kapasiteyi teşvik etmektir. Bu yönüyle iyi yönetişim, uluslararası gündemin önemli bir bileşeni haline gelmiştir. Siber yönetişim de küresel iyi yönetişimin bir bileşenidir (Akyeşilmen, 2018b). Zira siber alanda internete adil erişim, insan hakları, internetin sorunsuz ve güvenli bir şekilde çalışmasının sağlanması gibi konuların tamamı internet yönetişimi ile ilgili konulardır. Bu bağlamda siber uzay yönetilebilir mi? Siber uzayda

iyi yönetişim mümkün mü? Temel hak ve özgürlükler herkes için nasıl garanti altına alınabilir? Bu soru(n)lar uzun yıllara dayanan tartışma konularını temsil etmektedir.

Nye'a göre siber uzay, çoğu zaman yönetilmeyen, kanunsuz Vahşi Batı'ya benzetilse de, pratikte hem özel hem de kamusal birçok yönetişim alanını kapsamaktadır (Nye, 2010, s. 14). Nye'ın bu tespiti, anarşik bir sınırsızlık manzarasındaki görünmeyen sınırlılığa işaret eder. Yani siber uzay görünüşte sonsuz ve kontrolsüz gibi gözükse de, sınırları olan bir alandır. Çünkü gerçekte siber uzayın mimarisi, kişisel gizliliğin korunması, fikri mülkiyetin güvence altına alınması, siber güvenliğin sağlanması, dijital eşitlik ve erişimin teşvik edilmesi gibi çeşitli amaçları kapsayan düzenleyici çerçeveler tarafından desteklenmektedir. Ancak yine de siber uzay, halihazırda küresel olarak kabul görmüş ortak kurallar, standartlar, kontrol mekanizması veya koruma sisteminden yoksundur. Bunun nedeni, siber mahkeme, polis veya parlamento gibi, siber uzaydaki insanların faaliyetlerini küresel ölçekte koruyacak ve teşvik edecek ortak bir "yargı" sisteminin olmamasıdır. Bu nedenle ulus devletlerin veya AB veya OAS gibi bölgesel örgütlerin tek başına bu hakları koruyamayacağı, hatta uygulayamayacağı veya savunamayacağı görülmüştür (Mihr, 2016, s. 315). Bugün bakıldığında siber suçlarla mücadele için çok az araç ve mekanizma vardır. Yalnızca birtakım ulusal ve bölgesel çerçevede alınan önlemlerle işlenen suçlar önlenmeye çalışılmaktadır. Bu nedenle siber uzayın doğası gereği yönetilemez olduğu düşüncesi hâkim olmuştur. Bu ise siber uzayın istikrarı için bir sorundur. Zira bu durum, hukukun üstünlüğünün tanınmadığı bir kaos ortamına işaret eder.[48] Dolayısıyla çözüm, insan hakları normlarına, iyi yönetişime ve çok paydaşlı ilkelere dayalı küresel bir yönetişim sistemidir.

Bu doğrultuda uluslararası insan hakları normları ve standartları, siber uzayda yönetişim sistemleri oluşturmak için temel ve rehber olarak kullanılabilir. Ayrıca dijital teknolojilerin dinamik doğası, siber uzaydaki evrilen tehdit ve fırsatlara etkili bir şekilde yanıt verebilmek için bu yönetişim mekanizmalarının sürekli adaptasyonunu ve yeniden formüle edilmesini gerektirmektedir. Bu karmaşık yönetişim manzarası, çeşitli paydaşların siber uzayı yöneten normları, kuralları ve standartları şekillendirmede kritik bir rol oynadığını göstermektedir. İşbirlikçi ve çok katmanlı bir iyi yönetişim

[48] Ancak bazıları için siber uzayın düzenlemelerden muaf olması onun doğasının bir parçasıdır. Çünkü düzenlemeden muaf bir siber uzay, öz-düzenlemenin önünü açar, ki onlara göre bu olması gereken nihai durumdur (Barlow, 1996; Johnson & Post, 1998; Johnson vd., 2004).

yaklaşımı aracılığıyla bu aktörler, kolektif olarak daha düzenli, güvenli ve adil bir dijital dünyanın inşasına daha fazla katkıda bulunabilirler.

İnternet üzerinde yerleşen bu "kolektif" bilinç, interneti herkese ait bir ağ yapmaktadır. Aynı zamanda internetin ulusal sınırları aşan niteliği, onun "küresel bir kamu malı" olarak adlandırılmasının esas sebebini oluşturur (Canazza, 2018; Raymond, 2012; Surman, 2016). Zira küresel bir kamu malı olarak internet herkese açıktır ve her yerden erişilebilir. Bu bağlamda küresel yönetişim mekanizmaları, uluslararası düzenlemelerin teşvik edilmesine gereken önemi göstermelidir. Raymond ve Smith (2013), küresel internet yönetişimi için stratejik bir vizyona duyulan ihtiyacı dile getirmişlerdir. Kritik internet kaynakları, erişim, insan haklarının korunması, güvenliğin sağlanması, veri koruma, gizlilik standartları ve dijital bölünme gibi sorunlar, üstesinden gelinmesi gereken kilit konulardır. Bunun yanında yasal bir düzenleyici çerçeve oluştururken, farklı paydaşların çıkarlarını göz önünde bulunmak gerekir. Burada sağlanacak denge, yönetişim mekanizmasının istikrarı açısından önemlidir. Nitekim internetin kendisi dahi, uluslararası hukuk sisteminin kabulünü ve güvenilirliğini artırma potansiyeline sahiptir. Bu küresel perspektif, internet yönetişiminin nasıl şekillendirilmesi gerektiği konusunda da yol göstericidir.

Bugün özelikle normatif normlar göz önünde bulundurularak internet yönetişimi için en iyi model belirlenmeye çalışıldığında, eşitlik, açıklık ve çok paydaşlılık ilkelerinin somutlaştırıldığı bir modelin öne çıktığı görülebilir (DeNardis & Raymond, 2017, s. 494). Çok paydaşlı yönetişim, bünyesinde üç etkili unsur barındırır. Bunlardan birincisi, altyapı kapsamında değerlendirilen sınırsız ve serbest inovasyondur. İkincisi, daha çok yönetişim kapsamına giren merkezi olmayan yönetişim kurumlarıdır. Üçüncüsü ise, açık ve kapsayıcı süreçleri kapsayan "insan" faktörüdür. Bu doğrultuda çok paydaşlı karar almanın, internetin evrimini mümkün kılan kolektif bir karar alma süreci olarak ortaya çıktığı söylenebilir (Internet Society, 2020, s. 1). İlk olarak çok paydaşlı yönetişim modelleri, siber güvenlik, veri koruma ve internet yönetişimi gibi önemli konularda bir araya gelen çeşitli kesimlerin işbirliğini öne çıkarır. Bu yaklaşım, karar alma sürecine çok yönlü bakış açıları getirerek daha adil ve dengeli politikaların şekillendirilmesine olanak tanır. Bunların her biri, yönetişim sürecinin daha kapsayıcı, şeffaf ve etkileşimli olmasına katkıda bulunur.

Bu sürecin merkezinde insan haklarının korunması ve teşvik edilmesi bulunmaktadır. Zira iyi siber yönetişim, insan haklarını teşvik eder ve teknolojiler aracılığıyla korur (Mihr, 2016, s. 315). Teknolojilerin insan haklarına saygılı bir şekilde geliştirilmesi ve kullanılması gerekmektedir. Örneğin, gözetleme teknolojileri kişisel verilerin korunmasını ihlal etmemeli ve ifade özgürlüğünü kısıtlamamalıdır. Bu bağlamda iyi yönetişimin temel ilkelerinden biri olan şeffaflık, birçok durumda halkın güvenini kazanmak ve kamu kurumlarının hesap verebilirliğini sağlamak için önemlidir. Şeffaflık; bireylerin, kurumların ve devletlerin eylemlerinin açık ve anlaşılır bir şekilde raporlanmasını gerektirir. Bu, veri koruma politikalarından güvenlik ihlallerine kadar geniş bir yelpazede uygulanabilir. Bu nedenle şirketlerin kullanıcı verilerinin nasıl toplandığını, kullanıldığını ve paylaşıldığını açıkça belirtmesi gerekmektedir. Ayrıca devletlerin siber güvenlik tehditlerine ilişkin bilgileri ve alınan önlemleri kamuoyu ile paylaşması şeffaflığın başka bir boyutunu oluşturur. Örneğin, Wikileaks'in gizli belgeleri yayımlaması ve Edward Snowden'ın NSA izleme faaliyetlerini ifşa etmesi, şeffaflık ve mahremiyet meselelerini küresel gündeme taşımıştır. Bu olaylar, devletlerin ve büyük teknoloji şirketlerinin faaliyetlerine dair kamuoyu denetiminin önemini vurgulamış, aynı zamanda ulusal güvenlik ve bireysel özgürlükler arasındaki dengeyi sorgulatmıştır (Opper, 2011; Stone vd., 2012).

Ancak tam şeffaflık her zaman mümkün olmayabilir ve bazen güvenlik nedeniyle kısıtlanabilir. Bu durum, bireyler, devletler ve hizmet sağlayıcıları arasında güven ve açıklık kültürünün geliştirilmesi konusunda çelişkiye sebebiyet verebilir. Oysa şeffaflığın sınırlanması, ancak istisnai durumlarda ve ulusal mevzuatla açıkça tanımlanmalıdır. Bu nedenle güvenlik ihlalleri meydana geldiğinde, etkilenen kullanıcılara zamanında ve açık bir şekilde bilgi vermek, güven inşa etme ve zararı azaltma açısından kritik önem taşır. Buna ek olarak, açık kaynak kodlu yazılımın kullanımı, geliştirme süreçlerinin şeffaflığını artırarak kullanıcıların güvenliğini ve mahremiyetini korumaya yardımcı olacaktır. Örneğin, AGİT'in siber doktrini, strateji ve tehditler hakkında ulusal görüşlerinin paylaşılması veya siber güvenlikle ilgili ulusal programlarının paylaşılması gibi güven kazanıcı eylemler iyi bir uygulamadır (DCAF, 2019, s. 17-18).

Şeffaflığın siber alanda uygulanması, teknolojik ve politik zorluklara rağmen, iyi yönetişimin sağlanması için mümkün ve gereklidir. Ancak bu, tüm paydaşların güçlü yasal çerçeveler ve etik standartlar çerçevesinde katılımını gerektirir. Etkili bir şeffaflık

mekanizması, güven ve güvenilirlik inşa eder ve paydaşların haklarını korur. Bu nedenle şeffaflık, siber iyi yönetişimin sadece mümkün değil, aynı zamanda zorunlu bir unsuru olarak görülmelidir. Bununla birlikte, özellikle özel sektör paydaşının maddi kaygıları ve devletlerin ulusal güvenlikle ilgili endişeleri, bu ilkenin tam anlamıyla uygulanmasını güçleştirir. Ancak, bağımsız denetim mekanizmaları ve hukuk çerçevesinde belirlenen sınırlar, bu zorlukların üstesinden gelmeye yardımcı olabilir. Açık standartlar ve protokollerin teşvik edilmesi, siber alanda işbirliğini artırarak şeffaflığı destekler. Bu anlamda atılacak ulusal adımlar, uluslararası alan için emsal teşkil edecektir. Örneğin Brezilya, 2014'te internetin kullanımını düzenleyen ve interneti özgür, demokratik bir alan olarak koruyan, kullanıcı gizliliğini garanti altına alan ve ağ tarafsızlığını savunan geniş kapsamlı bir yasayı yürürlüğe koydu. Bu, şeffaflık ve demokrasiyi siber alanda teşvik eden önemli bir adımdır (Cgi.br, 2014).

Demokrasi açısından siber alanda iyi yönetişim, bu örneklerde görüldüğü gibi, çeşitli mekanizmalar ve uygulamalar aracılığıyla mümkündür. Ancak, bu, internet erişiminin eşitsiz dağılımı ve sansür gibi zorlukların üstesinden gelinmesini gerektirir. Örneğin, Çin ve Kuzey Kore gibi ülkelerdeki internet sansürü uygulamaları, hukukun üstünlüğü, eşitlik ve adalet ilkelerinin siber alanda nasıl zedelenebileceğinin örnekleridir (Freedom House, 2020,2021; Statista, 2023). Bu tür sansür uygulamaları, belirli bilgilere erişimi engelleyerek ve online ifade özgürlüğünü kısıtlayarak, bu temel ilkeleri işlemez hale getirir. Dolayısıyla siber alanda demokrasi, iyi yönetişimin sağlanmasını hem mümkün, hem de zorunlu kılar. Zira demokrasi, çeşitli paydaşların adil ve eşit bir şekilde temsil edilmesini ve teknolojinin toplumun geniş kesimlerinin yararına kullanılmasını sağlar. Bu sadece teknik bir çaba değil, aynı zamanda sosyal ve politik çaba gerektiren zorlu bir süreçtir. Bu alanda yapılacak uluslararası müzakereler ve konferanslar, farklı ülkelerin ve kültürlerin seslerinin duyulmasını sağlayarak küresel siber alanda demokrasiyi teşvik edecektir. Zira IGF örneğinde görüldüğü üzere bu tür platformlar, internetin küresel yönetişimi üzerine politikaların şekillendirilmesinde bir çeşitlilik ve kapsayıcılık sağlamaktadır.

Diğer yandan siber alanda hukukun üstünlüğü ve bununla bağlantılı olarak eşitlik ve adaletin sağlanması, iyi yönetişimin olmazsa olmaz unsurlarındandır. Bu kavramlar, bireylerin ve toplumların dijital ortamda adil bir şekilde muamele görmesini, haklarının korunmasını ve her türlü eylemin yasal bir çerçeveye dayandırılmasını gerektirir. Siber uzayın fiziksel alandan tamamen ayrılması mümkün olmadığından, kanunlarla

düzenlenmesi gerekir. İnternet üzerindeki her türlü faaliyet, fiziksel alandaki insanlar ve kurumlar üzerinde etkiler yaratır. Bu nedenle internet kullanıcıları, ulusal yasalara tabidir (Johnson & Crawford & Palfrey, 2004, s. 6). Örneğin elektronik ticaretin başarısı, sağlam bir yasal çerçeveye ve internetin temel yapısını ve değerlerini koruyarak online zararlı faaliyetleri düzenlemek için kolektif bir çaba gösterilmesine bağlıdır (Froomkin, 2000). Bu nedenle bireylerden devletlere kadar tüm paydaşlar arasında düzenleyici mekanizmalara yönelik pozitif bir bakış açısının geliştirilmesi elzemdir. Bunun için kullanıcı eğitimi ve farkındalığının artırılması, bireylerin kendi verileri üzerinde kontrol sahibi olmalarını ve şeffaflık taleplerinde bulunmalarını sağlayacaktır. Keza Markle Vakfı ve Greenberg Quinlan Rosner Research tarafından yapılan bir araştırmada, katılımcıların çoğunluğunun internet için bazı düzenlemelerin gerekli olduğuna inandığını ortaya koymuştur. Dolayısıyla, hedef devleti tamamen siber uzaydan uzak tutmak değil, onun gözetimini ve müdahalesini gerektiği kadar hızlı, çevik ve teknik anlamda bilgili bir şekilde gerçekleştirecek yöntemleri bulmaktır (Baird, 2014, s. 16).

Diğer yandan AB'nin Genel Veri Koruma Yönetmeliği (GDPR), hukukun üstünlüğünü, eşitlik ve adaleti siber alanda somut bir şekilde uygulamanın örneklerinden biridir. GDPR, bireylerin kendi kişisel verileri üzerinde kontrol sahibi olmalarını sağlayarak ve veri toplayan kuruluşlara katı kurallar getirerek, eşitlik ve adaleti teşvik eder (Sutherland, 2018, ss. 20-21). Ayrıca, siber suçlarla mücadelede ulusal ve uluslararası düzeyde işbirliği, hukukun üstünlüğünün siber alanda nasıl uygulanabileceğinin bir başka örneğini teşkil ederken, suçluların yargılanması ve cezalandırılmasında sınır ötesi zorlukların üstesinden gelmeye yardımcı olur. Siber uzay, insan hakları ilkelerinin, normlarının ve standartlarının fiziksel alanda olduğu gibi uygulandığı sınırsız bir kamusal alan olarak tanımlanabilir. Ancak, bu alanda hala uygulanabilir kuralların eksikliği, bir "siber mahkeme" veya "siber polis" gibi küresel ve ulusötesi bir yargı organının olmamasından kaynaklanmaktadır (Mihr, 2016, s. 314).

İnternet erişiminin evrensel bir hak olarak kabul edilmesi ve dijital bölünmenin azaltılması çabaları da, eşitlik ve adalet ilkelerinin siber alanda nasıl tezahür edebileceğinin altını çizer. Bu, herkesin bilgi ve teknolojiye eşit erişimine olanak tanır ve sosyo-ekonomik farklılıkların dijital ortamda derinleşmesini önler. Örneğin Hindistan'daki çeşitli teknolojiler ve başarılı projeler aracılığıyla dijital bölünmeyi önleme çabaları bu noktada önem arz etmektedir (Rao, 2005). Dolayısıyla siber alanda

hukukun üstünlüğü, eşitliğin ve adaletin sağlanması, güçlü yasal çerçeveler, uluslararası işbirliği ve teknolojiye adil erişimin teşvik edilmesi yoluyla mümkündür. Açık ve şeffaf bir yönetişim yapısı, bireylerin ve kurumların hesap verebilirliğini artırarak hukukun üstünlüğünü, eşitliği ve adaleti destekler. Bu çabalar, siber alanda iyi yönetişimin sadece mümkün olmakla kalmayıp, aynı zamanda bireylerin güvenliğini ve refahını korumak için zorunlu olduğunu göstermektedir.

Hesap verebilirlik unsurunun siber alanda tezahürü de pratikteki çeşitli yansımalarla kendini gösterir. Facebook-Cambridge Analytica vakası gibi örnekler, veri gizliliği ve hesap verebilirlikle ilgili önemli sorunları ortaya çıkarmıştır. Facebook'un 87 milyondan fazla kullanıcının kişisel bilgilerini Cambridge Analytica'ya teslim etmesi, kapsamlı bir küresel gizlilik yasasının acil bir küresel ihtiyaç olduğunu göstermiştir. Teknolojinin toplumsal etkisi ve vatandaşların gizlilik hakları üzerindeki risklerin minimize edilmesi için gizlilik politikalarının acilen geliştirilmesi gerekmektedir (Isaak & Hanna, 2018, s. 56). Cambridge Analytica vakası gibi olaylar, Amerikan gizlilik yasalarının ne kadar yetersiz olduğunu ortaya çıkarırken, GDPR gibi yasaların ne kadar etkin olduğunu göstermiştir. Cambridge Analytica skandalı, GDPR'in korkulduğu gibi karmaşık bir bürokrasi yerine, zamanının ötesinde bir düzenleme olduğunu kanıtlamıştır (Houser & Kimberly & Voss, 2018, s. 1). Bu anlamda ABD yasalarının gevşek kısıtlamaları altında faaliyet gösteren bu şirketler için GDPR, yeni bir hesap verebilirlik mekanizmasının inşasını zorunlu kılmaktadır.

Katılımcılık, herkesin yönetim süreçlerine katılmasını ifade eder ve iyi yönetişimin en temel unsurlarından birini temsil eder. Özellikle küresel internet yönetişimi konusunda, BM'nin desteklediği IGF gibi platformlar, devletlerin, özel sektörün ve sivil toplumun bir araya gelerek internet politikaları üzerine müzakere etmelerini sağlar. Kumar ve Mowshowitz (2008), IGF'nin internet erişimi ve özgürlüklerini nasıl geliştirdiğini incelemekte ve forumun internet yönetişiminde katılımcılık ilkesini teşvik etmedeki rolüne dikkat çekmektedir. Diğer bir örnek, her ne kadar küresel mahiyette olmasa da, katılımcılığı teşvik etmesi bakımından önem arz eden AB'nin Dijital Hizmetler Yasası (DSA) ve Dijital Pazarlar Yasası (DMA)'dır. Bu yasalar, dijital platformlarda kullanıcı katılımını artırmayı, büyük online platformların aşırı güç kullanımını önlemeyi, rekabeti korumayı ve kullanıcı haklarını güçlendirmeyi amaçlar (Chiarella, 2023, s. 50). Bu örnekler, siber alanda katılımın önemini ve çeşitli zorlukların üstesinden gelmede katılımı destekleyen yasaların etkili olduğunu gösterir. Zira katılımcılık, dijital

dünyada adil muamele, hakların korunması ve her türlü eylemin yasal bir çerçeveye dayandırılması sürecine katkıda bulunmaktadır.

Eğer siber uzay hem fırsatlar sunan hem de riskler barındıran bir alan olarak kabul ediliyorsa, işbirliğini ve iyi vatandaşlığı desteklemek amacıyla ortak değerler, ilkeler ve davranış normlarına dayalı bir düzenleyici çerçeve oluşturulması gereklidir. Bu amaçla, davranış standartlarını tanımlayacak, belirli eylemleri yasaklayacak ve yargı yetkisiyle ilgili kuralları belirleyecek kapsamlı bir uluslararası anlaşma üzerinde mutabakata varılması önem taşır (Tsagourias, 2015, ss. 28-29). Böylesi bir mutabakata yönelik düzenleyici yaklaşımlar, farklı paydaşların hak ve çıkarlarını dengelemeli, demokrasilerin kurumsal sınırlarına ve yasal çerçevelerine saygı göstermeli ve ilgili tüm paydaşların politika oluşturma süreçlerine katkıda bulunmasına izin vermelidir. İnternet sınır ötesi bir ağ olmasına rağmen, internet düzenlemelerinin çoğu ulusal düzeyde yapılmaktadır. Bu durum, çoğu zaman teknoloji şirketlerinin ulusal sınırların ötesinde faaliyet göstermesini zorlaştırmaktadır. Ayrıca veri yönetişimi söz konusu olduğunda, farklı veri koruma rejimleri arasındaki uyuşmazlıklar dijital alanın bölünmesine yol açabilirken, siber uzayın bütünlüğünü de tehdit eden bir sorun olarak gündeme gelmektedir (IGF Report, 2019). Bu zorluklar, ulusal yasal ve düzenleyici çerçeveler arasında daha fazla birlikte çalışabilirlik ve uyumlaştırma yoluyla çözülebilir.

Sonuç olarak internet, günümüzde küresel bir sistem olarak işlev görmekte ve bu nedenle, Rosenau'nun sistemlerin varlığını sürdürebilmeleri için gerekli gördüğü işlevsel gerekliliklerin bir benzerini karşılaması gerekmektedir (1992, s. 3). İlk olarak internet, dış zorluklarla, örneğin siber saldırılar, bilgi hırsızlığı ve diğer siber tehditlerle başa çıkabilmelidir. Bu zorluklar, ulusal ve uluslararası siber güvenlik protokollerinin geliştirilmesi, güçlü şifreleme yöntemlerinin kullanılması ve sürekli güvenlik güncellemelerinin yapılması gibi çeşitli araçlarla belli bir düzeyde aşılabilir hale gelecektir. Bu tür önlemler, internetin güvenli bir şekilde işlemesini ve kullanıcıların güven içinde faaliyetlerini sürdürebilmesini sağlar.

İkinci olarak, internet üzerinde faaliyet gösteren farklı aktörler arasındaki iç çatışmaların yönetimi de oldukça kritik bir konuyu temsil etmektedir. Bu durumda online topluluklar, sosyal medya platformları ve e-ticaret siteleri arasındaki anlaşmazlıklar; çatışmaların adil ve etkili bir şekilde çözülmesi, dijital diplomasi,

kullanıcılar arası arabuluculuk hizmetleri ve online etik kurallarının oluşturulması gibi yöntemlere başvurularak giderilebilir.

Son olarak, internetin sürekli gelişimi için gerekli kaynaklar sağlanarak çerçeve hedeflerle politikaların belirlenmesi gerekmektedir. Geniş bant erişiminin genişletilmesi, yenilikçi teknolojilere yatırım yapılması ve açık internet standartlarının teşvik edilmesi gibi çeşitli stratejilerin izlenmesiyle bu mümkündür. Tüm bu faktörlerin sağlanması, yukarıda bahsi geçen iyi yönetişim ilkelerinin normatif bir çerçevede benimsenmesine bağlıdır. Kısacası iyi yönetişim mümkündür, ancak paydaşların iyi yönetişim ilkelerini uygulamak için istekli olması gerekir. Zira siber uzayın doğasından kaynaklanan zorlukların aşılabildiği, iyi uygulama örneklerinde net bir şekilde görülmektedir. Dolayısıyla burada kilit faktör, işbirliği unsurlarının artırılarak çok paydaşlı bir zemine oturtulmasıdır. Bunun için paydaşların realist bir güvenlik yaklaşımıyla değil, normatif bir yönetişim çerçevesinde hareket etmesi beklenir. Adil ve eşitlikçi çok paydaşlı yönetişim bir modeli, bu tür politika ve hedeflerin belirlenmesinde devletler, özel sektör ve sivil toplum örgütleri gibi farklı aktörlerin katılımını sağlayarak, internetin küresel ve demokratik bir şekilde yönetilmesine olanak tanıyacaktır.

Değerlendirme

Çalışmanın ikinci bölümü, internet yönetişiminin karmaşık ve çok boyutlu bir küresel sorun olarak neden önemli olduğunu ayrıntılı bir şekilde ortaya koymuştur. Teknik altyapılardan politik meselelere, siber güvenlikten insan haklarına kadar geniş bir yelpazede konular ele alınarak, siber uzayın yönetilebilirliğinin ve siber iyi yönetişimin mümkün olup olmadığı incelenmiştir. Bu bölümde vurgulanan önemli bir nokta, siber uzayın yönetişimiyle ilgili zorlukların üstesinden gelmek için uluslararası işbirliğinin ve çok paydaşlı yaklaşımların elzem olduğudur. Siber uzayda karşılaşılan teknik ve politik sorunların çözümü, devletlerin, özel sektörün, teknik toplulukların ve sivil toplumun etkili bir şekilde işbirliği yapmasını gerektirir. Bu işbirliği, siber uzayın dinamik doğasına uygun esnek ve evrimsel yönetişim modellerinin geliştirilmesini zorunlu kılar.

İnternetin büyümesiyle ortaya çıkan yönetişim krizi, başlangıçta devlet müdahalesine karşı bir eğilimle karakterize edilmiştir. Piyasa mekanizmaları ve kendi kendine düzenleme, uygun düzeni sağlamak için yeterli görülmüştür. Ancak internetin

yaygınlaşmasıyla birlikte bu yaklaşımın eksiklikleri açığa çıkmıştır. Özellikle kullanıcıların mahremiyet, güvenlik ve çeşitli içeriklere erişim gibi temel ihtiyaçları yeterince korunamamıştır. Bu durum, devletlerin internet politikaları üzerinde daha etkin bir rol oynaması gerektiği sonucunu doğurmuştur. Bu etkili rol, inovasyonu engellemeden, özel sektör, teknik topluluk ve sivil toplumla güç paylaşımını içerecek şekilde uygulanmayı gerektirmiştir. Özellikle artan kullanıcı sayısı ve internetin sosyal ve ekonomik etkileri göz önünde bulundurulduğunda, yönetişim modellerinin evrim geçirmesi ve kamu yararını dikkate alan dengeli bir yaklaşımın benimsenmesi gerektiği ortaya çıkmıştır (Baird, 2014, s. 15).

Küresel dijital yönetişim sorunu, teknik ve politik sorun alanlarının tanımlanmasıyla daha da belirginleşmiştir. Teknik sorunlar, internetin temel yapı taşları olan TCP/IP, DNS, kök bölge, World Wide Web ve blok zinciri gibi alanlarda ortaya çıkmıştır. Bu teknik altyapılar, internetin sorunsuz işleyişi için hayati öneme sahiptir ancak aynı zamanda birçok sorun alanına da zemin hazırlamaktadır. Öte yandan politik sorun alanları; güvenlik sorunları, insan hakları meseleleri ve diğer sosyo-politik konuları içermektedir. Siber güvenlik yönetişimi, siber suçlar ve veri koruma gibi konular, internetin yönetişimini karmaşıklaştıran ve çözüm bulunması gereken önemli meseleler arasında yer alır.

Siber uzayın yönetilebilirliği konusu, bu teknik ve politik sorunların ışığında tartışılmaktadır. Siber uzayın doğası, aktör çeşitliliği, teknik bakış açısı ve işbirliği ile çıkar ikilemi gibi unsurlar, siber uzayın yönetişimini zorlaştıran faktörler olarak öne çıkmaktadır. Bu faktörler, siber iyi yönetişimin mümkün olup olmadığı sorusunu gündeme getirmektedir. Bu bölüm, siber uzayın yönetilebilir olduğuna dair güçlü argümanlar sunarken, yönetişimin başarısının, karşılaşılan zorlukların aşılması ve gereken koşulların sağlanmasıyla doğrudan ilişkili olduğuna dikkat çekmiştir. Siber uzayın yönetilebilirliği ve iyi yönetişimin sağlanabilmesi için siber saldırılara karşı koyma, veri koruma, kullanıcı mahremiyetini garanti altına alma ve açık erişimi destekleme gibi konularda uluslararası normlar ve standartlar geliştirilmesi ve uygulanması gerektiği belirtilmiştir.

Bugün ABD, internetin doğduğu ve geliştiği ülke olarak, internetin özgür ve açık kalmasını desteklemekte ve bu değerleri savunmaktadır. Bu durum, ABD'nin internet üzerindeki düzenlemelerde özgürlüğü ve açıklığı vurguladığı anlamına gelir. Öte

yandan, Çin ve Rusya gibi otoriter ülkeler, interneti kendi siyasi ve ekonomik çıkarları doğrultusunda kontrol altına almaya çalışmaktadır. Çin, internet erişimini kısıtlamak, sansür uygulamak ve muhalefeti kontrol etmek için çeşitli önlemler almaktadır. Benzer şekilde, Rusya da interneti kontrol altına alarak erişimi kısıtlamak, sansür uygulamak ve muhalefeti denetlemektedir. Diğer taraftan, AB, internetin özgür ve açık kalmasını desteklemekte ve bu doğrultuda çalışmaktadır. AB, internetin temel haklara ve değerlere saygılı bir şekilde düzenlenmesi için çaba harcamakta ve bu konuda öncü bir rol üstlenmektedir.

Tüm bu nedenlerle internet yönetişimi, maddi ve ideolojik birçok faktörü içeren karmaşık bir konudur. Bu karmaşıklık, konu üzerine yapılan tartışmaların sorunsuz bir şekilde yürütülmesini güçleştirmektedir. Kararların ve yaklaşımların paydaşlar arasında büyük bölünmelere yol açtığı, bazı yönleriyle teknik koordinasyon meselesi olmasına rağmen, politik, ticari, hukuki ve kültürel sonuçları olan bir alan olduğu gözlemlenmiştir. İnternet yönetişiminin politik bir yönü olduğunu ve devletlerin ulusal çıkarlarını teşvik etmeye devam edeceğini kabul etmek gerekmektedir. Bu noktada farklı ve bazen çelişen çıkarların uzlaştırılması, küresel koordinasyon eksikliği ve kapsayıcılık eksikliği gibi zorluklarla karşılaşılmaktadır. Bu bağlamda internet yönetişimi, internetin tüm kullanıcılar için faydalı bir platform olarak gelişmeye devam etmesi için önemli bir konu olmaya devam etmekte iken, bu konuda daha fazla tartışma ve işbirliğine ihtiyaç duyulmaktadır.

İnternetin "düzenlenebilir" potansiyelinin yanında "düzenlenemez" potansiyeli de vurgulanmıştır. Genel olarak düzenleme, mevzuat aracılığıyla oluşturulan kuralların izlenmesi ve uygulanması süreci olarak kabul edilir. Düzenlemeler bir hakkı yaratır, sınırlandırır veya kısıtlar. Siber uzayın yönetişimi ve düzenlemesi, belirli bilgilere erişimi kısıtlamakta veya kontrol etmektedir. İnternet düzenlemesi, verilerin sansürlenmesi ve IP adresi kontrolü gibi internetin kontrol unsurlarını kapsamaktadır. Ancak bu kontrol mekanizmalarının uygulanması genellikle internette insan hakları gibi sorunların meydana gelmesine sebebiyet vermektedir. Dolayısıyla bu durum paydaşları "sorun içerisinde sorun" ile karşı karşıya bırakmaktadır.

Sonuç olarak, ikinci bölüm, siber uzayın yönetilebilirliği ve siber iyi yönetişimin mümkün olduğunu savunurken, bu başarının, karşılaşılan zorlukların üstesinden gelinmesi ve gereken koşulların yerine getirilmesine bağlı olduğunu vurgular. Küresel

siber yönetişimin sağlanması, sadece mevcut sorunların çözümü değil, aynı zamanda siber uzayın potansiyelini tüm kullanıcılar için en iyi şekilde açığa çıkarmak için de kritik bir öneme sahiptir. Bu nedenle, devam eden işbirliği ve diyalog, siber uzayın yönetişimi ve iyi yönetişimin sağlanması yolunda önemli adımlardır.

BÖLÜM III: SİBER HUKUK BAĞLAMINDA DİJİTAL YÖNETİŞİM

Bu bölümün konusunu, işleyen küresel bir siber hukuk mekanizmasının mümkün olup olmadığı sorusu oluşturacaktır. Siber alan fiziksel alandan çok daha karmaşık olmasına rağmen –ki fiziksel alan daha az karmaşık olduğu halde uluslararası hukuk mekanizması pek çok noktada işlevsiz kalmaktadır– böyle bir mekanizmanın oluşturulması mümkün müdür? Siber uzay normlarının yükselişinde rol oynayan küresel ve bölgesel mekanizmalar hangileridir? Bugün siber hukuk mekanizmasının önündeki en büyük engel paydaşların işbirliğinden kaçınmaları mıdır? Siber alanda bir hukuk mümkün ise bu hukukun niteliği konusundaki farklı yaklaşımlar nelerdir? Bölümde bu sorular, diğer bütün bölümlerde olduğu gibi bütün paydaşların perspektifleri ve yaklaşımları göz önünde bulundurularak "normatif" bir bakış açısıyla değerlendirilecektir.

Bölümde uluslararası hukukun siber uzaya uygulanabilirliği konusuna geniş bir yer verildiği belirtilmelidir. Bunun sebebi, mevcut ve somut bir mekanizmanın işlerliğinin sorgulanmasının gerekli olmasıdır. Aynı zamanda alternatif bakış açılarının anlam kazanması açısından da gereklidir. Genel literatürde bu konuya kısıtlı yer verildiğinden, bu çalışmada konuya eğilim nispeten fazla olmuştur. Bu durumda bu çalışmanın ana soru/sorunlarından birinin kaynağı ortaya çıkmaktadır. Geleneksel uluslararası hukuk, bu yeni savaş ve çatışma anlayışına ayak uydurmaya yetkin ve ehil midir? Yoksa tamamen bu alana özgü yeni bir hukuk mekanizması mı inşa edilmelidir? Daha doğrusu böyle bir hukuk mekanizması – uluslararası siber hukuk – mümkün müdür?

3.1. Yükselen Bir Disiplin Olarak Siber Hukuk

20. yüzyılın başlarından itibaren barış disiplini olarak yükselen uluslararası ilişkiler, devletlere çatışmaları nasıl önleyecekleri konusunda yol gösterdi. İkinci Dünya Savaşı'ndan sonra savaşı önlemek için BM kuruldu. Bir ticaret anlaşması olarak kurulan AB, zamanla Avrupa'yı barışçıl bir bölge haline getirme misyonu edindi. NATO ile oluşturulan transatlantik ittifak, güvenliği sağlamak için dengeleyici bir rol üstlendi. Afrika, Asya, Pasifik ve Amerika'da bölgesel örgütler kuruldu. Silahsızlanma ve güvenlik anlaşmalarının uygulanması için uluslararası kuruluşlar oluşturuldu. 1919'da sivil toplum uzmanlığı, Chatham House gibi yapılanmalar aracılığıyla

üniversiteler ve düşünce kuruluşlarına kanalize edildi. Burada amaç, olası bir savaşı önlemek ve barışı tesis etmekti. BM destekli barış süreçleri ve ekonomik kalkınma hamleleri silahlı çatışmaların azalmasını sağladı. Uluslararası ceza mahkemesi, savaş suçları mahkemeleri, yerel adalet komisyonları, silahlı çatışma yasaları ve insan hakları yasaları sivilleri korumaya yönelik girişimler olarak ortaya çıktı. Kısacası bütün sorunların çözümü için gerekli olan mekanizmalar devletlerin işbirliğiyle gelişti. Çünkü ortada bu denli büyük sorunlar vardı ve bunun için bir hukuk mekanizması şarttı. Bu mekanizmaların temelini oluşturan hukukun üstünlüğü kavramı, BM Genel Sekreteri tarafından şu şekilde tanımlanmıştır:

> Hukukun üstünlüğü, Örgüt'ün misyonunun tam merkezinde yer alan bir kavramdır. Devletin kendisi de dahil olmak üzere, kamu ve özel tüm kişi, kurum ve kuruluşların, kamuya açık olarak ilan edilen, eşit şekilde uygulanan ve bağımsız olarak hükme bağlanan ve uluslararası insan hakları norm ve standartlarıyla uyumlu olan kanunlara karşı sorumlu olduğu bir yönetişim ilkesini ifade eder. Aynı zamanda, hukukun üstünlüğü, kanun önünde eşitlik, kanuna karşı hesap verebilirlik, kanunun uygulanmasında adalet, kuvvetler ayrılığı, karar alma sürecine katılım, hukuki kesinlik, keyfilikten kaçınma ve usulen ve hukuki şeffaflık ilkelerine bağlılığı sağlayacak tedbirlerin alınmasını gerektirir (UN Report, 2004, s. 4).

Hukukun üstünlüğü, barış ve istikrarın sağlanmasında önemli bir rol oynamaktadır. Hukukun üstünlüğü olan ülkelerde, bireyler ve kurumlar yasalara saygı duymakta ve bu yasalara göre hareket etmektedir. Bu durum, çatışmaların önlenmesine ve sorunların barışçıl yollarla çözümlenmesine yardımcı olmaktadır.

Peki bugün siber alanda bir hukuk mekanizması şart değil mi? Eğer şart ise neden devletler bu alanda adım atmakta bu kadar çekimser? Uluslararası sistemde merkezi bir otoritenin bulunmadığı anarşi ortamı ve uluslararası hukuk mekanizmasının tepesinde yer alan BM Güvenlik Konseyi'ndeki sürekli üyeler arasında yer alan güç mücadelesi nedeniyle küresel yönetişimin işlemez hale gelmesi, siber alanda da tezahür etmeye devam etmektedir. Bu durum bizi "siber hukuk" gibi uluslararası hukukla hem ilişkili hem de siber alanda ona alternatif oluşturabilecek bir mekanizmanın varlığına duyduğumuz ihtiyaç gerçeğiyle yüzleştirmektedir.

Bu ihtiyaca devletlerin yanıt verememesi, sorunları günden güne derinleştirmektedir. Zira bugün siber tehditler bütün paydaşlar açısından komplike ve çözülmeyi bekleyen

bir sorun alanı haline gelmiştir. Bu sorun alanı, internetin yaygınlaşarak küresel bir mahiyet kazanmasıyla ortaya çıkmıştır. İnternet kullanımındaki hızlı artış göz önüne alındığında, siber normların uygulanması kullanıcılar için güvenli bir ortam oluşturur mu? İnternet, hızla gelişen dünyaya ayak uydurabilen tek şey iken; dünya internetin hızına yetişebilecek mi? Peki hukuk böylesi bir hızla gelişen bu alana ayak uydurabilecek mi?

Bu alanda meydana gelen sorunların her biri doğrudan siber yönetişim ile ilgili olsa da bu sorunların çözümü için gerekli olan küresel işbirliği ortamı henüz oluşturulamamıştır. Oysa ki siber uzayın küresel doğası, bu sorunların etkili ve tutarlı işbirliği yöntemleriyle ele alınmasını gerektirmektedir. Bunun yapılabilmesi için uluslararası yasal çerçeveler, koordinasyon mekanizmaları veya işbirliği yapılanmaları gerekmektedir. İnternetin kötüye kullanımına ilişkin uluslararası bir yasal çerçeve veya koordinasyon mekanizmasının olmaması, siber uzayın istikrarı için risk oluşturmaktadır.

Bu sorunların çözümü için kayda değer uluslararası girişimler olsa da, uluslararası düzeyde yapılan çalışmaların büyük çoğunluğunu bölgesel veya özel çıkar grupları yürütmektedir (ITU, 2005c, s. 27). Bununla birlikte, bu sorunların çözümü için özel sorumluluğa sahip herhangi bir uluslararası veya hükümetlerarası kuruluş bulunmamaktadır (ITU, 2005c, s. 28). Dolayısıyla bu durum, sorunları daha da derinleştirmektedir. Herhangi bir yasal çerçeve olmadan, siber alanın güvenilir bir alan olarak anılması mümkün değildir. Siber suçların bertaraf edilmesi için yasal bir sisteme ihtiyaç vardır (Dutta & Jadav & Tanwar & Sarma & Pricop, 2022). Böylesi bir anlaşmanın yokluğu, devletlerin hukukun üstünlüğünü ve insan haklarını göz ardı eden yaklaşımlar benimsemesine neden olur. Zira devletlerin meseleyi güvenlik yaklaşımıyla değerlendirmeleri, bu mekanizmaları da zayıflatmaktadır (Akyeşilmen, 2018a, s. 301).

Mevcut durum, siber alanın güvenilirliği ve yasal bir çerçevenin oluşturulması ihtiyacını vurgulamakta, aynı zamanda devletlerin güvenlik yaklaşımıyla hareket etmelerinin hukukun üstünlüğü ve insan hakları gibi temel ilkeleri göz ardı etmelerine yol açtığını ortaya koymaktadır. Bu bağlamda siber hukuk, kavramsal bir sorunsal olarak öne çıkmakta ve farklı disiplinler arasında bir köprü görevi görmektedir. Bu nedenle, siber hukukun kavramsal çerçevesini anlamak ve bu alanda karşılaşılan

zorluklara çözümler geliştirmek, siber yönetişimin geleceği için kritik bir öneme sahiptir.

3.1.1. Kavramsal Sorunsal: Siber Hukuk

Siber yönetişimin birçok disiplinle ilişkili olduğunu önceki bölümlerde belirtmiştik. Bu bağlamda hem siber uzayın kendisinin hem de yönetişiminin hukuk, bilişim gibi pek çok konuyla bağlantılı olduğunu söyleyebiliriz. Hofmann ve diğerleri (2017), internet yönetişiminin doğası gereği disiplinlerarası bir alan olduğuna vurgu yapmışlardır. Ancak bilgisayar bilimi, sosyoloji, hukuk ve ekonomi gibi belirli disiplinler, diğer disiplinlere oranla daha iyi temsil edilmektedir. Nitekim internet yönetişiminin her yönü yasal bir bileşene sahiptir. E-ticaret veya siber suç gibi konuların güçlü yasal bileşenleri vardır. Diplo'nun internet yönetişimi sınıflandırmasında yasal sepet şu konuları içermektedir: yargı, uyuşmazlık çözüm biçimleri, telif hakkı, ticari marka, iş hukuku ve aracıların sorumlulukları. WGIG Raporu'nda, telif hakkı ve ticari marka fikri mülkiyet haklarının bir parçası olarak değerlendirilirken; yargı yetkisi ve tahkim sorunlarından da bahsedilmiştir (Kurbalija, 2015, s. 105).

Siber hukukun net bir tanımı olmasa da literatürdeki birtakım tanımlamalara yer vermek gerekir. Siber hukuk; internet, bilgi işlem, siber uzay ve ilgili yasal konularla ilgilenmek için tasarlanmış bir hukuk sistemidir. Siber hukuk, yeni bir hukuk dalıdır. Daha çok siber suçlar, gizlilik hakları, fikri mülkiyet hakları, elektronik ve dijital imza gibi alanları kapsamaktadır (Gurjar, t.y., s. 7). Aynı zamanda yargı yetkisi, veri koruma ve ifade özgürlüğü gibi konuları kapsar. "Bu yönüyle siber hukuk, dijital dünyanın güvenliğini sınırlar ötesinde sağlamak için çok önemlidir ve "siber suçlarla başa çıkmak için geliştirilen yasal bir altyapıdır" ve "siber suçların meydana gelmesini önlemek için siber uzay üzerinde bir kalkan görevi görür" (Jigsaw Academy, t.y.). "Diğer bütün hukuk alanları gibi sosyal, ekonomik, siyasal ve kültürel boyutuyla siber hukuk da dinamik bir alandır" (Akyeşilmen, 2018a, s. 86).

"Siber hukuk kelimesi, siber uzaya girişi kontrol eden, siber uzaya erişim sağlayan, insanların siber uzaya erişmesini sağlayan donanım ve yazılımı oluşturan veya kendi cihazlarını kullanarak 'online' olup siber uzaya giren kişi ve kurumları etkileyen tüm durumları, kanun maddelerini ve anayasal hükümleri kapsar" (Roy, 2012, s. 143). Bu yönüyle siber hukuk, siber suçlarla ilgili tüm bilgileri içeren bir hukuk sistemidir. Bu

sistem, suçların cezaları, internet özgürlükleri, siber güvenlik ve gizlilik gibi konularda düzenlemeler içerir (Kumari vd., 2022, s. 210).

Siber hukuk, mülkiyet veya sözleşme gibi belirli bir hukuk dalı olmaktan çok, fikri mülkiyet, gizlilik, ifade özgürlüğü ve yargı yetkisi gibi birçok yasal alanın kesiştiği bir alandır. Siber hukuk, internet üzerindeki insan etkinliklerinin yarattığı zorlukları, fiziksel dünyadaki yasaların çerçevesi içinde ele almayı amaçlar. Elektronik ticaretin büyümesi, elektronik ticaretin başarısı için hayati öneme sahip olan yasal altyapıyı daha da güçlendirecek canlı ve etkili düzenleyici mekanizmaların ihtiyacını ortaya koymuştur. Tüm bu düzenleyici mekanizmalar ve yasal altyapılar siber hukukun kapsamı içindedir (Sheakh, 2012, s. 10).

Bugün ortak bir siber hukuk tanımı geliştirilememesinin en büyük nedeni, alan üzerinde bir hukuk mekanizmasının yokluğudur. Yapılan anlaşmalar genellikle ikili veya bölgesel çapta olmuş; küresel bir anlaşma henüz oluşturulamamıştır. En kapsamlı uluslararası kuruluş olan BM bile, yalnızca düzenlediği forumlar, konferanslar veya raporlarda yüzeysel bir şekilde siber hukuka değinmiştir. Siber hukuka yönelik bu çabasızlık, alanın doğasında var olan anarşiyi hiper anarşi düzeyine taşımakta ve çatışmaları derinleştirmektedir (Akyeşilmen, 2018a, ss. 60-61). Ancak bu durum, internet yönetişiminin uluslararası veya ulusal yasaların kapsamı dışında kaldığı anlamına gelmemektedir. Antlaşmanın yokluğu söz konusu olsa da, yönetişim yapısının temel unsurlarının birçoğu bir anlaşma çerçevesine dayanmaksızın yasalara uygun olarak uygulanabilmektedir. Sözleşmelere dayalı özel hukuk araçları görece baskın bir rol oynamaktadır. Uyuşmazlıklar ise hukuk mahkemelerinde dava açılmasıyla değil, çeşitli alternatif uyuşmazlık çözümleri (alternative dispute resolution – ADR) gibi yargı dışı mekanizmaların devreye girmesiyle çözüme kavuşturulmaya çalışılmaktadır (Bygrave & Michaelsen, 2009, s. 93).

Ramirez ve Choucri tarafından belirtildiği üzere siber güvenlik terminolojisinin standardize edilmesi, farklı disiplinler arasında iletişimi geliştirecek ve küresel internet yönetişimi yasalarının oluşturulmasına yardımcı olacak bir adımdır. Bu, teknik ve teknik olmayan paydaşlar arasındaki etkileşimi ve evrensel internet yönetişimi yasalarının tasarımını kolaylaştıracak bir unsurdur (2016, s. 2216). Diğer tüm yasalar gibi siber hukuk da siber uzaydaki aktörlere alanı nasıl kullanmaları gerektiğine yönelik

bir kurallar dizisi sunmalıdır. Siber hukukun amacı, kişilerin, kuruluşların ve devletin verileri ve mülkiyetleri için güvenli bir ortam sağlamaktır.

3.1.2. Siber Hukukun ve Normların Yükselişi

1990'ların ortasına kadar, birçok devlet internete ve yönetişimine dair sorunlara karşı ilgisiz kalmıştır. 1990'ların ikinci yarısına kadar internet, devletlerin planlarının tamamen dışındaydı. Ağda yürütülen faaliyetler (özellikle saldırılar) için birkaç yasama girişimi dışında herhangi bir çalışma söz konusu değildi (Bygrave & Michaelsen, 2009, s. 118). Bugün ise siber hukuk, bölgesel ve küresel birtakım mekanizmalar aracılığıyla gelişim göstermeye başlamıştır. Ancak bölgesel mekanizmaların küresel mekanizmalara oranla çok daha gelişmiş olduğunu, küresel bir mekanizmanın henüz mevcut olmadığını belirtmek gerekir.

ABD, Çin ve Rusya gibi başlıca siber güçler, siber uzaydaki davranışlarına ilişkin anlaşmaları resmileştirmeye başlarken, son on beş yıldır gayri resmi kısıtlı davranış biçimlerini zaten kullanmaktadırlar. Bu aşamada önemli olan, bu normatif sonuçları kurumsallaşmış sonuçlara dönüştürmektir. Kurumsallaşmış sonuçlar, siber uzaydaki davranışları düzenleyen resmi kurallardır. Bu kurallar, uluslararası anlaşmalar, yasal düzenlemeler ve uluslararası kuruluşlar tarafından belirlenen politikalar aracılığıyla oluşturulur (Valeriano & Manesss, 2018, s. 268). Siber hukuk ve norm oluşturma, ulusal ve uluslararası düzeyde giderek artan bir öneme sahip olup, çeşitli kurumsal çabalarla şekillenmektedir. Bu bağlamda, uluslararası kuruluşlar, devletler, özel sektör ve sivil toplum kuruluşları arasında işbirliği içinde bir dizi kurumsal sonuç ortaya çıkmıştır:

3.1.2.1. Küresel Mekanizmalar

Bugüne kadar, özellikle siber tehditleri ele alan ve her şeyi kapsayan bir uluslararası hukuk anlaşması veya bu alanda uluslararası teamül hukukunun temelini oluşturabilecek yekpare bir devletlerarası anlaşma yoktur. Ancak, daha önce de belirtildiği gibi, uluslararası hukukun siber uzay operasyonlarına uygulandığına dair genel kabul görmüş bir devlet görüşü vardır (UNGGE Report, 2021). Bu noktada BM, küresel internet yönetişimi alanında önemli bir rol oynamaktadır. 1999 yılında BM tarafından siber uzayın uluslararası güvenlik bağlamında ele alınmasıyla, siber güvenliğin küresel önemi resmi olarak tanınmaya başlandı ve bu durum yasal çerçevelerin oluşturulmasını zorunlu kıldı (Yongping, 2023, s. 61).

Zaman içinde, Estonya ve İran gibi ülkelerde yaşanan önemli siber saldırılar, siber tehditlerin fiziksel alan üzerindeki potansiyel etkilerini ve politik boyutlarını ortaya koymasıyla nispeten yavaş ilerleyen bu süreç yasal çerçeveye duyulan ihtiyacın aciliyetiyle hızlanmaya başladı. 2007'de Estonya, 2008'de Gürcistan ve 2010'da İran'daki siber saldırılar ile birlikte devletlerarası casuslukla ilgili açığa çıkan bilgiler, BM'de bu konudaki momentumun artmasına neden oldu (Henderson, 2015, s. 466). Bu durum, uluslararası toplumun siber tehditlere karşı koymak için artan işbirliği ve ortaklık ihtiyacını ortaya koymuştur. Bu doğrultuda BM, siber güvenlikle ilgili çeşitli uzman grupları ve çalışma grupları kurarak konuyu daha detaylı ele almaya başladı. Bu kapsamda geliştirilen UNGGE ve OEWG gibi çalışma grupları, siber alanda devlet davranışlarına ilişkin kılavuz ilkeler geliştirmiştir. Bu ilkeler, devletlerin uluslararası hukuka uymalarını ve siber alanda barışçıl işbirliğini teşvik etmeyi amaçlamaktadır.

Bunun yanında BM, siber suçlarla mücadeleye yönelik uluslararası kuralları tartışmak ve bu konuda bir platform oluşturmak amacıyla her yıl konferanslar düzenlemekte, siber suç mevzuatı, soruşturma, elektronik deliller ve uluslararası işbirliği gibi konuları ele almaya başlamıştır. Bu kapsamda BM'nin Siber Suçlarla Mücadele Sözleşmesi, Mayıs 2021'den itibaren üye devletlerce müzakere edilen ve Genel Kurul'un onayı ile siber alanda bağlayıcı bir uluslararası anlaşma olma potansiyeline sahip bir girişimdir. Bu sözleşme, siber suçların önlenmesi, soruşturulması ve faillerinin yargılanması alanında uluslararası işbirliğini artırarak önemli bir küresel yasal çerçeve sunmayı hedeflemektedir. Ancak, insan hakları üzerindeki olası olumsuz etkileri ve baskıcı devletlerin kötüye kullanım riskleri de dikkate alınmaktadır (Wilkinson, 2023). Zira yeni taslak, ifade özgürlüğüne yönelik tehditler, geniş çapta gözetim yetkileri ve sınır ötesi baskının kolaylaştırılması gibi endişeleri artırmaktadır (Rodriguez, 2023). Antlaşma müzakereleri, devletler arasında sözleşmenin kapsamı ve insan haklarının sözleşmedeki yerine dair devam eden anlaşmazlıklarla karakterize edilmiştir. Bu müzakerelerin son oturumu, 2024 Ocak ayında New York'ta yapılması planlanmaktadır ve sözleşmenin 2024 yılında tamamlanması öngörülmektedir.

Bunun yanında, BM çatısı altında gerçekleştirilen internet yönetişimi konferansları, ifade özgürlüğü, ırkçılıkla mücadele, çocuk suçlarına karşı koruma, insan haklarının geliştirilmesi ve siber uzayın sürdürülebilir gelişimi gibi konuları ele alarak, internetin ve siber uzayın karşı karşıya olduğu zorluklarla başa çıkmanın yollarını tartışmaktadır. Özellikle İfade Özgürlüğü Konferansı, Irkçılık Konferansı, Çocuk Suçları Konferansı,

İnsan Haklarının Geliştirilmesi ve Korunması Konferansı ve IGF gibi etkinlikler, uluslararası işbirliğinin önemini vurgulayarak, çeşitli siber güvenlik sorunlarına karşı koymak için ortak çözümler üretme amacını gütmektedir. Bu etkinlikler, dünya genelinde internet kullanımının getirdiği fırsatları ve riskleri ele alarak, dijital çağın temel meseleleri üzerine küresel bir diyalog kurmayı hedefler. "İyilik için Yapay Zekâ Küresel Zirvesi" gibi özel etkinlikler ise, yapay zekanın sürdürülebilir kalkınma üzerindeki potansiyel katkılarını keşfetmek ve bu teknolojilerin etik, güvenilir ve insan merkezli bir şekilde geliştirilmesini sağlamak için çoklu paydaşlar arasında işbirliği ve anlayışı derinleştirmeye odaklanır (Li vd., 2021, ss. 3686-3688).

Küresel anlamda BM'nin yaptığı birtakım yüzeysel çalışma dışında herhangi bir mekanizmadan söz etmek mümkün değil. Bunun yanında ITU tarafından başlatılan WSIS, daha çok internet yönetişim konularına eğilmiş olup, hukuk konusunda ciddi adımlar atamamıştır. Bunun en önemli nedeni burada devletlerin ITU üzerinde devlet egemenliğinin güçlendirilmesi ve devlet odaklı yeni bir oluşumun yaratılması şeklinde taleplerde bulunmuş olmalarıdır (Fidler, 2013a). Bu durum, küresel bir hukuk mekanizmanın oluşmasının önündeki engellerden birini teşkil etse de BM çerçevesinde bazı yumuşak hukuk mekanizmalarının oluşum aşamasında olduğu söylenebilir (Akyeşilmen, 2018a, ss. 92-93).

Aktif siber savunma faaliyetleri, uluslararası yasal zemine oturtulmaya çalışılırken, bölgesel ile uluslararası mekanizmaların iç içe geçtiği görülmüştür. 2001 tarihli Budapeşte Siber Suç Sözleşmesi de böyle bir mekanizmadır. Başlangıçta bölgesel bir sözleşme olarak başlayan sözleşmeye bugün 68 ülke taraf iken; 15 ülke, imzacı olmuş veya katılım daveti almıştır (CoE, t.y.). 2003 yılında ise AB, bu tür eylemlere karşı mücadelede önemli bir adım atarak "Siber Suçlar Sözleşmesi'nin Bilgisayar Sistemleri Aracılığıyla İşlenen Irkçı ve Yabancı Düşmanlığı Nitelikli Eylemlerin Suç sayılmasına İlişkin Ek Protokol"ü kabul etmiştir. Bu protokol, ırk ayrımcılığı, yabancı düşmanlığı gibi nefret suçlarının yanı sıra internette ayrımcılık, şiddet teşviki ve belirli ırk, renk, soy, veya ulusal kökenlere karşı ayrımcılığı teşvik eden zararlı içeriklerin izlenmesi ve cezalandırılması konusunda AB'ye önemli sorumluluklar yüklemektedir (CoE, 2003).

Sözleşme, ülkelerin siber yasalara dayanak oluşturmaları için bir çerçeve sağlamıştır. Ortaya çıkış sürecine bakıldığında; Avrupa Konseyi ve ABD, 1990'ların sonlarında siber faaliyetler hakkında küresel bir yasa fikrini ortaya koymuştur. Burada ulusal yasaların homojenleştirilmesi fikri gündeme gelmiş ve uluslararası bir anlaşmaya

duyulan ihtiyaç vurgulanmıştır. Sözleşme, bu fikrin bir çıktısı olarak ortaya çıkmıştır. Böylece, taraf devletlerin siber alandaki yasalarını birtakım kurallar ışığında formüle etmiştir. Bu formülasyon şu şekilde özetlenebilir:

- Her ağ, yetkili bir erişim düzeyine sahiptir. Erişim düzeyini aşan kuruluşlar yasayı ihlal eder.
- Verilere ve/veya bilgisayar ağlarına erişimin engellenmesi veya bunlara zarar verilmesi, bilginin özgür bir biçimde paylaşımına aykırıdır ve uygun şekilde cezalandırılmalıdır.
- Dijital cihazlar, fikri mülkiyetin kopyalanmasına izin verse de, fikri mülkiyet haklarını ortadan kaldırmaz. Dolayısıyla kuruluşların fikri mülkiyet haklarına saygı duyması sağlanmalıdır.
- Çocuklara ait pornografik içerikler tamamıyla yanlıştır. Bu tür içerikleri yayınlayan kuruluşlar cezalandırılmalıdır.
- Anlaşmaya taraf ülkeler, bu ilkelerin uygulanması için diğer ülkelerle işbirliği yapmalıdır. Taraf ülkeler, anlaşma hükümlerine aykırı fiiller gerçekleştiren faillerinin iadesi ve kovuşturulması için bilgi paylaşımında bulunmalıdır.
- Bilgisayarların ve bilgisayar ağlarının korunması için kullanılan tedbirlere cezai so4rumluluk yüklenemez.
- Avrupa Suç Sorunları Komitesi (CDPC) taraf ülkeler arasındaki anlaşmazlıkları çözecektir (Barnes, 2018, s. 23).

Budapeşte Siber Suç Sözleşmesi'nin etkinliği hakkında pek çok tartışma ve uzman görüş mevcuttur. Budapeşte Siber Suç Sözleşmesi'ndeki en belirgin zayıflık, taraf devletlerin bazı maddelere çekince koyabilmesidir. Hildebrandt, Budapeşte Sözleşmesini "doğrudan etkisi olmayan bir anlaşmanın en önemli örneği" olarak nitelendirmiştir. Ona göre sözleşme, özellikle iki nedenden dolayı etkisizdir. Birincisi, Avrupa Konseyi'ne üye devletlere hitap etmektedir. İkincisi, taraf devletleri bir dizi cezai suç tedbirini yürürlüğe koymaya zorlamaktadır. Bu yönüyle sözleşme, yasaların ulusal düzeyde uygulanmasını ve ceza kanununda değişiklikler yapmayı gerektirir (2020, s. 10).

Bu konuda Owens, Dam ve Lin, sözleşmenin siber saldırılarla mücadelede uluslararası ceza yasalarının etkinliğini artırdığını öne sürmektedir (2009, s. 34). Goldsmith (2010),

anlaşmaya taraf olan ülke sayısının az olması nedeniyle (o dönemde az bir sayıydı) anlaşmanın etkinliğini yetersiz bulmaktadır. Ayrıca, anlaşmanın uygulama açısından da güçlü bir mekanizmaya sahip olmadığını vurgulamıştır. Goldsmith'in görüşünü destekleyen Lindsay, neredeyse tüm ülkelerin siber güvenliğin küresel bir sorun olduğu konusunda hemfikir olmalarına rağmen, belirsiz tanımlamalar ve zayıf uygulamalar nedeniyle sözleşmeyi etkisiz bulmaktadır (2015, s. 42).

Budapeşte Sözleşmesi, ulusötesi siber suçlarla mücadeleye yönelik uygulamaları belirleyen en önemli uluslararası antlaşmadır. Sözleşme, devletlere danışmaya gerek kalmadan verilere sınır ötesi erişime imkânı sunar. Aynı zamanda siber yasaların uluslararası alanda tartışılması için önemli bir zemin oluşturmuştur. Siber alandaki küresel yasalar, Tallinn Manual 2.0 ile zenginleştirilmiştir. NATO'nun Kooperatif Siber Savunma Mükemmeliyet Merkezi (CCDCOE), Tallinn Manual 2.0 ile devletlerin yasalarına rehberlik etmektedir (CCDCOE, t.y.b). Ancak bu yasalar genellikle erişim düzeyi aşımı gibi konularla ilgilenmektedir. Bu nedenle de savunma açısından sınırlı bir etkisi olduğu söylenebilir. Budapeşte Siber Suç Sözleşmesi ise, aktif siber savunma önlemlerine ve faaliyetlerine izin vermesi nedeniyle bu eksikliği kısmi olarak gidermektedir.

3.1.2.2. Bölgesel Mekanizmalar

Siber hukuk için bölgesel mekanizmaların sayısı nispeten fazla olduğundan bölgesel düzeyde artan bir dinamizmden söz edilebilir (Kurbalija, 2017). Bunlar arasında yukarıda detaylıca incelenen Avrupa Konseyi Siber Suç Sözleşmesi (Budapeşte Sözleşmesi) (2001), Şanghay İşbirliği Örgütü'nün Bilgi Güvenliği Anlaşması (Yekaterinburg Anlaşması) (2009), Afrika Birliği Siber Güvenlik ve Kişisel Verilerin Korunması Sözleşmesi (2014), OECD Online Kimlik Hırsızlığı Rehberi (2008), AB Direktifi (2013), CCDCOE ve Online Özgürlük Koalisyonu (FOC) gibi bölgesel girişimler söz konusudur.

Yukarıda küresel mekanizmalar arasında değerlendiğimiz Budapeşte Siber Suç Sözleşmesi, bazı kaynaklarda bölgesel olarak da geçebilmektedir. Avrupa Konseyi Siber Suçlar Sözleşmesi, tüm dünya milletlerinin imzasına açık olan bir anlaşmadır. Bu anlaşma, devletlerin sınır ötesi bilgi taleplerine yanıt vermeyi amaçlar. Suçun işlendiği ülke, zarara uğrayan ülkenin talebi üzerine depolanan verileri korumak ve karşı ülkeyle paylaşmakla yükümlüdür. Burada amaç, suçluların iadesini ve bilgi paylaşımını

kolaylaştırmaktır. Bu şekilde, Sözleşmeye taraf olan her ülkenin siber suç yasaları işbirliği çerçevesinde uyumlu hale getirilmeye çalışılmaktadır (Goldsmith & Wu, 2006, s. 166).

AB, özellikle siber güvenlik ve gizlilik alanında dünya çapında öncü ve kapsamlı yasal düzenlemeler geliştirmiştir. Bunlardan en bilineni, kişisel verilerin korunmasına yönelik küresel bir etki yaratan Genel Veri Koruma Yönetmeliği (GDPR)'dir. GDPR, AB vatandaşlarının verilerini işleyen, AB içi ve dışındaki tüm kuruluşları kapsar ve uluslararası bir standart olarak kabul edilir. Ayrıca, AB Siber Güvenlik Yasası, üye devletler arasındaki işbirliğini güçlendirerek AB içinde siber güvenlik standartlarını yükseltir. Diğer yandan Europol tarafından kurulan Avrupa Siber Suç Merkezi (EC3), siber suçlarla mücadelede uluslararası bilgi paylaşımını ve işbirliğini teşvik eder. Bu merkez, hem kamu hem de özel sektörü kapsayan masa başı tatbikatlar yürüterek siber savunma kapasitelerini güçlendirir. Diğer önemli bir düzenleme olan NIS Direktifi, üye devletlerin kritik altyapılarını siber tehditlere karşı korumayı amaçlayarak bilgi paylaşımı ve işbirliğini teşvik eder.

Uluslararası alanda, Afrika Birliği'nin Malabo Konvansiyonu, Afrika'da veri koruma ve siber güvenlik konularında kapsamlı bir yasal çerçeve sunar ve siber suçlarla mücadelede işbirliğini hedefler. Asya-Pasifik Ekonomik İşbirliği (APEC) ise, Çapraz Sınır Gizlilik Kuralları (CBPR) Sistemi ile üye ekonomiler arasında kişisel bilgilerin transferi için gizlilik standartları belirler, böylece bölgesel ticareti kolaylaştırırken tüketici gizliliğini korur. OAS, kıta genelinde siber güvenlik işbirliğini ve kapasite gelişimini destekleyen Bölgesel Siber Güvenlik Stratejisi'ni benimsemiştir.

Çeşitli uluslararası girişimler, NATO da dahil olmak üzere, siber uzayda işbirliğini teşvik etmeyi amaçlamaktadır. NATO CCDCOE, yayınladığı Siber Operasyonlara Uygulanacak Uluslararası Hukuk üzerine Tallinn El Kitabı 2.0 ile mevcut uluslararası hukukun siber uzaya nasıl uygulandığına dair en kapsamlı analizi sunmuştur. Kılavuz "resmi NATO görüşünü yansıtmamakla birlikte" NATO, ABD Siber Komutanlığı ve Uluslararası Kızıl Haç Komitesi tarafından desteklenmektedir. Kılavuzu, Five Eyes[49] ülkelerinin siber uzayda mevcut uluslararası hukukun uygulanabilirliğini teşvik etmesinin aracı olarak görenler de mevcut (Pijović, 2021, s. 223). Kılavuz, özellikle yumuşak hukukun bir örneğini teşkil etse de, siber savaşın yasal belirsizliğini kısmi

[49] Avustralya, Kanada, Yeni Zelanda, Birleşik Krallık ve ABD'den oluşan bir istihbarat ittifakıdır. Bu ülkeler, sinyal istihbaratında ortak işbirliği anlaşması olan çok taraflı UKUSA Anlaşmasına taraftır.

olarak ortadan kaldırdığı için önemlidir (Schmitt, 2011). Bunun yanında NATO, 2021'de, internetin otoriter kullanımlarına karşı çıkan ve özgür, açık, barışçıl bir siber uzayı destekleyen bir bildiri yayımlamıştır. Ayrıca, 2022'de, birçok NATO üyesi de dahil olmak üzere 60 ülkenin katılımıyla "İnternetin Geleceği için Bir Deklarasyon" imzalanmıştır (The White House, 2022).

Bu mekanizmalar, siber alanın zorluklarına bölgesel düzeyde yanıt vermek ve siber ortamda güvenliği, istikrarı ve işbirliğini artırmak için önemli araçlar sunar. Her biri, kendi coğrafi alanındaki özel ihtiyaçları ve hedefleri yansıtacak şekilde tasarlanmıştır. Bu düzenlemeler, her ne kadar parçalı bir halde olsalar da küresel siber hukukun gelişmesine yardımcı olacaktır. Ancak bütün bu yapıcı çabalar, uluslararası düzeyde bir siber hukuk anlaşması yapılması için yeterli olamamıştır. Bunun en önemli nedeni, paydaşların bu konuda çıkar odaklı yaklaşmaları ve isteksizlikleridir (Akyeşilmen, 2018a, ss. 93-94).

3.2. Siber Uzayın Uluslararası Hukuk Bağlamında Değerlendirilmesi

Uluslararası Hukuk, devletler ve uluslararası aktörler arasındaki ilişkileri düzenleyen geniş bir yasal çerçevedir ve silah kontrolünden ticarete, çevreye kadar pek çok alanda küresel yönetişimi şekillendirir. Teknolojik ilerlemelerle birlikte siber uzayın yönetişimi giderek daha fazla önem kazanmıştır. Ancak, Budapeşte Siber Suçlar Sözleşmesi ve Afrika Birliği'nin kişisel veri koruması sözleşmesi gibi sınırlı istisnalar dışında, uluslararası hukukta siber uzay için özel düzenlemeler nadirdir. Bu durum, internetin sınırlarını mevcut uluslararası hukukun kapsayıp kapsamadığı konusunda belirsizliklere yol açmıştır. Ancak BM, G20, AB, ASEAN ve OAS gibi kuruluşlar, devletlerin bilgi ve iletişim teknolojileri kullanımında mevcut uluslararası hukukun uygulanabilir olduğunu belirtmiştir (Dixit, 2022, s. 83).

Özellikle son yıllarda, uluslararası hukukun mevcut hükümlerinin siber uzayda da geçerli olduğuna dair artan bir uluslararası kabul söz konusudur (UNGGE Report, 2013; Tallinn Manual, 2013). 2013[50] ve 2015[51] yılında UNGGE, BM Genel Kurulu'na sunduğu yasal olarak bağlayıcı olmayan raporlarda uluslararası hukukun siber alan için

[50] Ayrıca bkz: UNGGE. (2013, Haziran 24). *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, A/68/98. https://digitallibrary.un.org/record/799853.

[51] Ayrıca bkz: UNGGE. (2015, Temmuz 22). *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, A/70/174. https://digitallibrary.un.org/record/799853?v=pdf.

geçerli olduğunu beyan etmiştir. UNGGE 2013 raporu, "uluslararası hukukun ve özellikle BM Şartı'nın uygulanabilir olduğu ve barış ve istikrarın korunması için açık, güvenli, barışçıl ve erişilebilir bir BİT ortamının teşvik edilmesi için gerekli olduğu" konusunda fikir birliğine varmıştır. Bunun yanında, devletleri kendilerine atfedilebilecek uluslararası hukuka aykırı eylemler için yükümlülüklerini yerine getirmeye davet etmiştir (2013, s. 2). Akabinde yayınlanan raporlarda da 2013 raporundaki maddeler yinelenmiştir. Pijović'e göre UNGGE süreci, küresel siber alanda norm inşasının başlangıç noktasını oluşturmuştur. Daha da önemlisi, uluslararası hukukun siber uzaya uygulanabilirliği konusunda bazı temel ilkelerin belirlenmesine zemin hazırlamıştır (2021, s. 221). 2013 tarihli Açık ve Güvenli Siber Uzay İçin Seul Çerçevesi ve Taahhüdü de uluslararası hukukun siber uzaya uygulanabilirliğini ve online insan haklarına saygıyı vurgulamıştır (UNODA, 2013).

Tallinn El Kitabı (2013) da, siber operasyonların hukuki çerçevesini, jus ad bellum (savaşa girme hakkı) ve jus in bello (savaş hukuku) dahil olmak üzere, siber uzaydaki çatışmaların yönetilmesi açısından incelemiştir. Burada "uluslararası hukukun siber uzayı ele almadığı ve bu alanın yalnızca yeni antlaşmalarla düzenlenebilecek yeni bir hukuki alan olduğu" yönündeki görüşün gerçek dışı olduğu belirtilmiştir (Schmitt, 2013, s. 13). Benzer şekilde, Uluslararası Kızılhaç Komitesi (ICRC) 2012 yılında BM Genel Kurulu'na yaptığı bir konuşmada "siber uzayda yasal bir boşluk olmadığını" belirtmiştir. Bu nedenle her yeni teknolojide olduğu gibi siber operasyonların da uluslararası insancıl hukuka, özellikle de ayrımcılık, orantılılık ve ihtiyat kurallarına uygun olması gerektiği ifade edilmiştir (Droege, 2011; Slack, 2016, s. 70).

2014 yılında birçok farklı paydaşın katılımıyla Brezilya'nın São Paulo şehrinde düzenlenen ve internet yönetişimi konularını ele alan büyük bir konferansın sonucu olarak ortaya çıkan NETmundial Yol Haritası[52] da küresel yönetişim için önemli bir konu olan yargı yetkisi sorununu vurgulamıştır. Yol haritasının amacı, gelecek nesiller için internetin sınır ötesi doğasını korumak ve internet üzerindeki yönetişime yönelik kurumsal boşluğu kolektif olarak doldurmaktır. Bu, küresel internet yönetişimi topluluğunun mevcut ve gelecekteki internet sorunlarına yönelik operasyonel çözümler üretmek için internet yönetişim ekosistemini geliştirme ve interneti birleşik ve

[52] Ayrıntılı bilgi için bkz: NETmundial. (2014, Nisan 14). NETmundial draft outcome document. https://document.netmundial.br/net-content/uploads/2014/04/NETmundial-draft-outcome-document_April_14.pdf.

parçalanmamış bir alan olarak koruma arzusuyla uyumludur (de La Chapelle & Fehlinger, 2016, s. 10).

Nisan 2015'te Çin ve Rusya'nın "uluslararası bilgi güvenliğini sağlamada işbirliği" anlaşmasının birçok maddesinde de siber alanda uluslararası hukukun önemine dikkat çekilmiştir (Lewis, 2015). Ulusal ve uluslararası bilgi güvenliğinin sağlanması için uluslararası hukukun geliştirilmesi ve desteklenmesi gerektiği ifade edilmiştir. Bu noktada uluslararası örgütler ve forumların işbirliğine ihtiyaç duyulduğu belirtilmiştir (Government of the Russian Federation, 2015).

5 Mart 2015'te BM bünyesindeki OEWG'nin 193 üye devleti kapsayan raporu bu noktada önem arz etmektedir. Grup, siber uzayda sorumlu devlet davranışına ilişkin normları kapsayan bir raporu fikir birliğine vararak kabul etmiştir. Rapor her ne kadar içerik açısından yetersiz olsa da, bu konudaki ilerlemeye duyulan ihtiyaç göz önüne alındığında önemli bir gelişme olarak değerlendirilebilir. Özellikle BM üyeleri arasındaki mevcut bölünme ve çekişmelere rağmen böylesine bir fikir birliğine varılması önemli bir adım olarak kabul edilebilir. Öte yandan bu rapor, Rusya tarafından önerilmişti. Rusya, halihazırda internet yönetişiminde BM'nin söz sahibi olması gerektiğini ve bu konuda uluslararası bağlayıcı bir sözleşmeyi savunan bir ülkedir. OEWG tarafından hazırlanan bu rapor, fikir ayrılıklarına rağmen bir uzlaşma zeminini işaret etmesi açısından elzemdir (Taylor, 2021).

Nisan 2017'de İtalya'da yapılan G7 Dışişleri Bakanları toplantısında siber konulara dair iki önemli belge kabul edilmiştir. İlk belge olan Ortak Bildiri, kritik altyapı risklerinin yanı sıra demokratik süreçlere müdahaleyi de tanımlamıştır. Burada haksız fiillere karşı önlemler almak da dahil olmak üzere mevcut uluslararası hukukun siber uzayda uygulanabilirliği kabul edilmiştir. Dahası bildiri, devletleri "mevcut uluslararası hukukun devletlerin siber alandaki faaliyetlerine mümkün olan en geniş ölçüde nasıl uygulanacağına ilişkin görüşlerini kamuoyuna açıklamaya" davet etmiştir. İkinci belge olan Siber Uzayda Sorumlu Devletlerin Davranışı Bildirgesi ise, devletlere uluslararası hukukta silahlı saldırıların eşiğindeyken uyguladıkları kuralları hatırlatmaktadır. Bildirge, "Devlet sorumluluğuna ilişkin geleneksel uluslararası hukuk, siber uzaydaki faaliyetlere uygulanabilecek eylemleri devletlere atfetmek için standartlar sağlar" ifadesinin altını çizmektedir (Kurbalija, 2017). G7 toplantısının ardından Temmuz 2017'de Almanya'da düzenlenen G20 Liderler Zirvesi de ağırlıklı olarak dijital

ekonomiye odaklanmış ve siber güvenliğe de atıfta bulunmuştur. Haziran 2017'de Şanghay İşbirliği Örgütü Zirvesi'nden çıkan Astana Deklarasyonu ile siber güvenlik alanında uluslararası bir yasal araç talebi güçlendirilmiştir (Kurbalija, 2017).

Görüldüğü üzere sınırlı da olsa siber alana uygulanmaya çalışılan bir uluslararası hukuk mekanizmasından söz edilebilir. Ancak uluslararası hukukun siber faaliyetlere veya operasyonlara uygulanabilirliği sorunu devam etmektedir. Ancak siber şiddetin günden güne yayıldığı yadsınamaz bir gerçektir. Bu sorunun uluslararası hukuki sonuçlarını çözmek için uluslararası hukukun yasal mekanizmalarına ihtiyaç vardır. Bu durumda uluslararası hukukun öznelerinin verdiği tepkiler önem arz etmektedir. Ancak özneler tarafından verilen tepkinin meşru olabilmesi için bu tepkinin tehlikenin derecesiyle orantılı olması gerekir. Fakat söz konusu siber şiddet olduğunda, barış ve savaş arasındaki sınırlar silinmekte ve mevcut uluslararası hukuk siber alanın doğasıyla sınanmaktadır (Simović & Rašević & Simović, 2020, s. 30).

Uluslararası hukukun siber faaliyetlere uygulanmasını engelleyen faktörler, uygulanmasını teşvik eden girişimlere göre daha fazladır. Antlaşma hukuku, uluslararası teamül hukuku, uluslararası hukuk normları gibi pek çok yasal araç, bilgisayarların icadından çok önce geliştirilmiştir. Dolayısıyla siber operasyonlarla ilgili yasal sorunların büyük çoğunluğu, 1945 BM Şartı'nda ve 1949 Cenevre Sözleşmelerinde geçen konularla bağlantılıdır. Zira devletlerin fiziksel alanda uluslararası hukuka aykırı olarak değerlendirilen suçları siber uzayda da vuku bulmaktadır. Dolayısıyla BM Uluslararası Hukuk Komisyonu tarafından belirlenen normların siber uzaydaki eylemler için de kullanılıp kullanılmayacağı tartışılmaktadır. Ancak bu normlar, yalnızca kabul edildikleri sırada mevcut olan devlet faaliyetleri için değil, genel olarak devlet faaliyetleri için geçerlidir. Bu nedenle siber faaliyetlere genel uluslararası hukukun uygulanabileceği iddia edilmektedir. Dolayısıyla uluslararası hukukun siber faaliyetler için geçerli olduğu ve bunun hem akademik literatür hem de devletler tarafından onaylandığı belirtilmektedir. Ancak bu durumun zorluğuna da dikkat çekilmektedir. Zira uluslararası hukuk normlarının siber alana uygulanması oldukça zordur. Bu nedenle normların nasıl yorumlanacağı ve uygulanacağı konusunda ciddi sorunlar ortaya çıkmaktadır (Delerue, 2020, s. 13).

Uluslararası hukukun genel kurallarının uygulanması, siber hukukun şekillenmesinde yardımcı olmaktadır. Ancak yeni hukuk mekanizması oluşturulması konusunda yasal

belirsizlik devam etmektedir. Esasen sorun şurada başlamaktadır: Siber faaliyetlerin yarattığı hasar devlet egemenliğini baltalayacak kadar büyük olduğunda hangi hukuk sistemi devreye girmelidir? Bunun da ötesinde, uluslararası toplumun siyasi, ekonomik ve sosyal yaşamı üzerinde hasara yol açacak şekilde büyük olması durumunda hukuk sisteminde statüko sağlanması mümkün olabilecek midir? (Simović vd., 2020, s. 29). Sınırlı sayıda özel düzenleme ve genel hukuk kurallarının siber faaliyetlere uygulanması çabalarına rağmen, mevcut durum belirsizliklerle ve zorluklarla dolu olmaya devam etmektedir.

Bu yeni alan, uzun yıllardır geliştirilmekte olan konuları içermekte veya bunları içerecek şekilde genişlemektedir. Bu doğrultuda uluslararası hukukun egemenlik, yargı yetkisi ve devlet sorumluluğu gibi temel ilkelerini kapsamaktadır. Siber uzay ve uluslararası hukukun kesiştiği başka bir önemli alan ise uluslararası barış ve güvenliğe ilişkin siber faaliyetlerdir. Bu alan, savaş ve çatışmalara kadar geniş bir yelpazeyi kapsarken; siber suç, siber istihbarat ve siber savaş gibi konular artık fiziksel alanda gerçekleşmekte ve siber güvenliğin geleceği, geniş kabul görmüş uluslararası normlara dayanarak şekillendirilmektedir. Bu bağlamda, devam eden bölümlerde özel olarak ele alınacak bu konular, siber uzayın uluslararası hukuk altında daha derinlemesine incelenmesini sağlayacaktır.

3.2.1. Siber Savaş ve Çatışmalar

Konvansiyonel savaşların varlığı insanlık tarihi ile eşdeğerdir. Grotius'a göre şiddet toplumun temellerini sarstığında iki kural yürürlüğe girer. Birincisi, devletin ne zaman silahlı güce başvurabileceğini belirleyen *ius ad bellum* kuralıdır. İkincisi ise, bu gücün nasıl kullanılacağını belirleyen *bello'da ius* kuralıdır (Kolasi, 2017, s. 18). Modern anlamda *ius ad bellum*, 1945 tarihli BM Şartı'nın Madde 2/4 ve 6. Bölümünde açıkça belirtilmektedir *Jus in bello* ise, savaş zamanında uygulanması gereken insancıl hukuk kurallarını ifade eder.

BM Şartı'nın 2. Maddesi (4), herhangi bir devletin toprak bağımsızlığına veya siyasi bütünlüğüne karşı tehdit veya güç kullanımını yasaklar.[53] 51. madde ise kuvvet

[53] Bkz: UN (t.y.). Purposes and Principles of the UN (Chapter I of UN Charter). https://www.un.org/securitycouncil/content/purposes-and-principles-un-chapter-i-un-charter (01.05.2023).

kullanımını “meşru müdafaa” hakkı kapsamında saklı tutar.[54] Bu durumda, siber operasyonların “silahlı bir saldırıya eşdeğer ölçekte ölüm ve yıkım” tehdidiyle sonuçlanması veya yakın bir tehdit oluşturması halinde meşru müdafaa hakkı kullanılabilir mi? Bugüne kadar bazı ulusal mahkemeler bu soruya siber uzayın militarize edilmemesi şartıyla “evet” cevabını vermiştir. Düşman devletlerin seçim sistemini manipüle etmek, parlamentoyu işlemez hale getirmek, finansal sistemlere zarar vermek gibi operasyonları her halükârda suç saymıştır. Bu eylemler, devletlerin iç işlerine müdahale yasağının ihlali olarak görülmüştür (Pijović, 2021, s. 222).

Siber savaş, geleneksel savaşın aksine fiziksel savaş meydanlarında değil, bilgisayar ağları ve internet üzerinden gerçekleşen bir çatışma türüdür. Bu, devletler ve çeşitli aktörler arasında bilgi sistemlerine yönelik saldırılar şeklinde ortaya çıkar. Siber çatışmanın evrensel olarak kabul edilmiş bir tanımı yoktur. Siber çatışma, çeşitli teknolojik araçlar ve insan tabanlı teknikler kullanılarak gerçekleştirilebilmektedir. Bir rakibin bilgisayar sistemlerine zarar vererek, yok ederek veya devre dışı bırakarak gerçekleştirilebilir. En yaygın siber çatışma biçimleri; siber saldırı ve siber casusluk faaliyetleridir. Siber çatışma alanı, çeşitli uluslararası girişimler tarafından araştırılmaktadır. BM Silahsızlanma Araştırma Enstitüsü (UNIDIR), siber güvenlik faaliyetlerinin ulusal, bölgesel ve uluslararası düzeyde incelenmesini sağlayan bir Siber Endeks geliştirmiştir (UNCTAD, 2015, s. 27).

Siber savaşın mevcut uluslararası hukuk çerçevesi içinde açıkça tanımlanmamış olması, nasıl yönetilmesi gerektiği konusunda önemli bir tartışma yaratmıştır. Zira siber savaş, mevcut uluslararası hukuk tarafından açıkça ele alınmamış yeni bir savaş biçimidir. Siber çatışmaların gelecekte nasıl yönetileceğine dair uluslararası toplum henüz bir konsensusa varmamıştır. Geleneksel savaş ilkelerinin siber savaşa nasıl uygulanacağı konusunda hala belirsizlikler bulunmaktadır (Kelsey, 2008, s. 1427). Örneğin, Uluslararası İnsancıl Hukuk’un (IHL) geleneksel savaş koşulları göz önünde bulundurularak oluşturulmuş olması, siber savaş gibi yeni çatışma biçimlerine uygulanabilirliğini karmaşıklaştırmaktadır. İlk olarak, siber saldırıların ne zaman "silahlı çatışma" olarak sınıflandırılacağı ve IHL'nin uygulanıp uygulanmayacağı belirsizdir. Bir siber operasyonun doğrudan fiziksel zarara yol açmadığı durumlar, hukuki bir boşluk yaratmaktadır. İkinci olarak IHL, saldırıların orantılı olmasını ve sivil

[54] Bkz: UN (t.y.). Chapter VII — Action with respect to Threats to the Peace, Breaches of the Peace, and Acts of Aggression. Article 51. https://legal.un.org/repertory/art51.shtml (01.05.2023).

hedeflerden askeri hedefleri ayırt etmeyi gerektirir. Siber alanda, hangi hedeflerin "sivil" veya "askeri" olarak kabul edileceği ve bir saldırının orantılı olup olmadığını değerlendirmek zor olabilir. Üçüncü olarak, bir devletin siber saldırıya uğraması durumunda, karşılık verme hakkı ve bu karşılığın nasıl orantılı olacağı konusu tartışmalıdır. Yine de bu normların siber alana uygulanabilirliği konusunda girişimler devam etmektedir.

Şimdiye kadar hem savaş hem de barış zamanında uygulanabilecek uluslararası kuralları kapsamlı bir şekilde derleyen tek bir girişimden söz edilebilir: *Tallinn Manual* (Simović vd., 2020, s. 28). Tallinn El Kitabı, uluslararası hukukun siber operasyonlara ve siber savaşa nasıl uygulandığını inceleyen etkili bir akademik çalışmadır. CCDCOE tarafından 2009 yılının sonlarında başlatılan bu çalışma, siber çatışmalar bağlamında uluslararası hukukun uygulanmasını ele almak üzere uluslararası bir grup hukukçu ve uygulayıcıyı bir araya getirmiştir. Tallinn'deki CCDCOE himayesinde uluslararası hukuk ve teknik uzmanlardan oluşan bir grup tarafından derlenmiştir. Bu proje, diğer seçkin hukuk akademisyenleri ve uygulayıcılarının yanı sıra Birleşik Devletler Deniz Harp Akademisi'nden Profesör Michael N. Schmitt'in öncülüğünde yürütülmüştür. El Kitabı, siber operasyonlarla ilgili karmaşık hukuki meselelere açıklık getirmeyi amaçlamakta olup, türünün ilk kapsamlı çalışmasıdır.

2013 yılında yayınlanan Orijinal Tallinn El Kitabı, kuvvet kullanma yasağını ihlal eden veya bir devletin meşru müdafaa hakkını kullanmasına uygun olanlar gibi en ciddi siber operasyon biçimlerine odaklanmıştır. Siber tehdit ortamının evrimini takiben, Tallinn El Kitabı 2.0, kapsamı siber savaşın ötesine geçerek barış zamanı siber operasyonları ve devletlerin düzenli olarak karşılaştığı diğer siber olay türlerini içerecek şekilde genişletmek amacıyla Şubat 2017'de yayınlanmıştır. Bu güncelleme, devlet sorumluluğu, deniz, uluslararası telekomünikasyon, uzay, diplomatik ve konsolosluk hukuku ve insan hakları hukukunu da içerecek şekilde bu operasyonlar için geçerli olan uluslararası yasal çerçeveyi kapsamayı amaçlamıştır (CCDCOE, t.y.b).

Tallinn El Kitabı, siber konularla ilgilenen hukuk danışmanları ve politika uzmanları için etkili bir kaynak haline gelmiştir. Bu doğrultuda, halihazırda Tallinn El Kitabının geliştirilmesi için devam eden bir proje bulunmaktadır.[55] 2021 yılında CCDCOE,

[55] Detaylı bilgi için bkz: CCDCOE (t.y.). CCDCOE to Host the Tallinn Manual 3.0 Process. https://ccdcoe.org/news/2020/ccdcoe-to-host-the-tallinn-manual-3-0-process/ (01.05.2023).

mevcut bölümlerin revizyonunu ve devletler için önem taşıyan yeni konuların araştırılmasını içerecek beş yıllık bir girişim olan Tallinn Manual 3.0 Projesini başlatmıştır. Devlet uygulamaları ve devletlerin uluslararası hukuka ilişkin resmi beyanlarına ek olarak, BM ve bölgesel düzeydekiler gibi uluslararası forumların faaliyetleri ve beyanları, akademik çalışmalar ve devletler, özel sektör ve sivil toplumu içeren çok paydaşlı girişimler de dikkate alınacaktır. Bu güncelleme, devletler için önemli olan yeni konular da dahil olmak üzere, siber operasyonların ve devletlerin bunlara verdiği tepkilerin gelişen doğasını yansıtacaktır. Yine Schmitt tarafından yönetilen proje, siber bağlamda uygulandığı şekliyle uluslararası hukukun tarafsız bir şekilde yeniden ifade edilmesini ve El Kitabının herhangi bir devletin veya kuruluşun yasal pozisyonunu veya doktrinini temsil etmeyen tarafsız, bilimsel bir çalışma olarak kalmasını sağlamayı amaçlamaktadır (CCDCOE, t.y.b).

Bu belge, NATO himayesi altında hazırlanan resmi olmayan bir belgedir. Dolayısıyla Uluslararası Adalet Divanı Statüsü'nün 38. maddesinin 1. paragrafında tanımlanan uluslararası hukukun resmi kaynaklarından birini temsil etmez. Ancak belge, siber alanda örf ve akdi hukukun uygulanması konusunda önemli görüşler bildirmiştir. Bu nedenle, uluslararası hukuk ilkelerinin uygulanması, yasal boşlukların doldurulması ve normların yorumlanması için yararlı ve güvenilir bir ek kaynak olarak görülmektedir. Ancak belgenin birçok hukuk uzmanı ve uluslararası hukuk süjesinin hukuki görüşüne uygun olmadığı ifade edilmektedir (Simović vd., 2020, s. 28). Yine de kılavuz, devletlerin birbiriyle çelişen siber yasalarını anlamak için oluşturulan en kapsamlı kılavuzdur. Bu yönüyle Tallin El Kitabı, aktif bir siber savunma önleminin bir başkasının egemenliğini nasıl ihlal edebileceği konusunda ehil sayılabilir.

Diğer yandan GGE de, BM Şartı'nın, siber alanda geçerli olduğunu kabul etmiştir. Yayınladığı bir raporda grup, uluslararası hukuk normlarının siber uzayda da devletler tarafından uygulanması gerektiğini belirtmiş ve buna yönelik tavsiyelerde bulunmuştur (UNCTAD, 2015, s. 27). Bu konuda BM'nin de özellikle siber çatışmalarla mücadele ve siber güvenlik konusundaki faaliyetlerini uygulama konusunda ciddi bir meydan okumaya tabii tutulduğu söylenebilir. BM'nin karşılaştığı zorluklardan ilki, saldırı faaliyetinde bulunan tarafa verilecek yanıtın yine ağlar üzerinden yapılacak olmasıdır. Zira BM, karşı tarafın ağlarının etkisiz hale getirilmesi faaliyetinin bir barış aracı olarak kullanılıp kullanılmadığı konusunda emin olamamaktadır. Dolayısıyla bu eylemin silahlı çatışma yasaları kapsamında bir saldırı anlamına gelip gelmeyeceği konusunda

bir fikir birliğine varamamaktadır. Tartışmanın bir kısmı, ağın yok edilmek yerine etkisiz hale getirilmesinden kaynaklanmaktadır. Bu durumda özellikle ağın yok edilmesi ile etkisiz hale getirilmesi arasında bir ayrıma gidilmeye çalışılmaktadır. Devletler, bir ağın yok edilmesinin silahlı çatışma yasaları kapsamına gireceği konusunda hemfikirdir, Ağın yeniden kurulabilir olması durumunda bunun silahlı çatışma yasaları kapsamında değerlendirilmesi söz konusu değildir. Zira bu durumda operasyon, silahsız çatışma kapsamında değerlendirilecektir. Bu noktada BM, neredeyse her zaman üye devletleri barış operasyonlara destek olmaya çağırmaktadır (Kleffner & Dinniss, 2013, s. 519).

Bu girişimlere rağmen uluslararası hukukun siber savaşın sorunlarını çözmek için yeterli olup olmadığı tartışmaya halen tartışmaya açıktır. Zira siber alan, bütün bu savaş anlayışını değiştirmiş ve savaş algısını genişletmiştir. Siber araçlarla yürütülen gizli veya görünür savaş türleri ortaya çıkmıştır. Bazı durumlarda konvansiyonel araçlarla kombine edilerek yürütülen bu savaş türü, melez veya hibrit savaş kavramlarını genişletmeye başlamıştır (Simović vd., 2020, s. 35). Bu nedenle Siber savaşın sorunlu olması muhtemeldir. Bunun temel nedeni, siber saldırıların zorlayıcı etkilerinin spekülatif olmasıdır. Siber saldırılar geleneksel anlamda şiddetin anlamını değiştirebilirken, doğrudan ve dolaylı etkileri göz ardı edilemez. Örneğin, bir devletin ekonomisini siber saldırı yoluyla ciddi şekilde sekteye uğratmanın ekonomik ve sosyal sonuçları oldukça yıkıcı olabilir. Bu durum, siber güvenliği çevreleyen konuları mevcut kuralların geçerli olmadığı benzersiz bir alan olmaktan öteye taşımaktadır. Siber güvenlik, mevcut istihbarat ve askeri faaliyetlerin bir uzantısı olarak yeniden tanımlanmaktadır. Devletler, siber uzayı devletler arası ilişkilerin mevcut modeline uydurabilmektedir. Ancak siber savaşın sorunları sadece devlet aktörleriyle sınırlı değildir. Devlet dışı aktörlerin buradaki etkileri de göz ardı edilemez. (Slack, 2016, s. 71). Zira siber uzay, devlet dışı aktörlerin uluslararası arenada daha etkin olmasını sağlamış ve devletlerin önemini nispeten azaltmıştır. Bu aktörler, siber savaşlarda farklı roller üstlenmekte, devletlerle çeşitli ilişkiler içinde bulunmakta ve kendilerine özgü denetim mekanizmalarına sahip olmaktadır. Bu nedenle devlet dışı aktörlerin siber alandaki rolleri, uluslararası hukuk başta olmak üzere çeşitli zorluklar yaratmaktadır. Bu durum, silahlı çatışmaları düzenleyen mevcut kuralların bu yeni savaş biçimini nasıl ele alabileceği, siber tehditlere karşı devletlerin nasıl yanıt verebileceği ve bu

tehditlerin kaynağının nasıl belirleneceği gibi konuları gündeme getirmektedir (Bussolati, 2015, s. 102).

Bu alandaki gelişmelere ayak uydurmak ve gerekli düzenlemeleri yapmak için uluslararası işbirliği ve koordinasyonun artırılması gerektiği açıktır. Bu noktada etik ve norm temelli işbirliği mekanizmalarının geliştirilmesi elzemdir. Bunun için BM'nin yanı sıra, Uluslararası Telekomünikasyon Birliği (ITU) gibi teknik kuruluşlar ve bölgesel güvenlik örgütleri de siber güvenlik konusunda işbirliğini artırmak ve etik davranış kurallarını belirlemek için çalışmalar yapabilir. Zira bu alandaki çatışma hukuku ile ilgili net bir çalışma olmasa da birçok ülkenin bunu etik dışı bulduğunu söylemek mümkün (Akyeşilmen, 2018a. s. 251). Örneğin Rusya, 2007'de Estonya'ya, 2008'de Gürcistan ve Litvanya'ya, 2009'da Kırgızistan'a, 2014'ten itibaren ise Ukrayna'ya büyük çaplı siber operasyonlar yürütmüş ve bu operasyonlar Rusya'nın siber alanda çatışmacı ve etik-dışı olarak algılanmasına sebebiyet vermiştir.

Bu algı olumsuz gibi görünse de ziyadesiyle umut vericidir. Çünkü bu özellikle devletler düzeyinde norm temelli girişimlerin desteklenmesini kolaylaştıracak bir unsurdur. Zira bugün siber alanın yönetişimine dair en büyük sorun alanı, paydaşların bu alanın tehditlerine odaklanarak etik ve normatif unsurları göz ardı etmesi ve işbirliği mekanizmalarını geliştirmekten kaçınmasıdır. Bu anlamda siber çatışmaların etik dışı olarak algılanması, zamanla "algı"nın ötesine geçerek bir "yasa" veya bir "norm" inşasına dönüşebilir.

3.2.2. Siber İstihbarat

Siber istihbarat operasyonları, uluslararası hukuku ihlal edebilecek potansiyel unsurları içermektedir. Bu operasyonlar, bir devlete ait bilgisayar sistemlerine yetkisiz erişim sağlama, gizli bilgilerin ele geçirilmesi ve siber saldırılar gibi faaliyetleri içerebilir. Bu tür eylemler, uluslararası normları ve anlaşmaları ihlal ederek diğer devletlerin egemenlik haklarına müdahale anlamına gelebilir, bu da ciddi diplomatik ve hukuki sonuçlar doğurabilir. Bu nedenle, siber istihbarat operasyonlarının yürütülmesi sırasında uluslararası hukuka uyum önemlidir, aksi halde bu tür faaliyetler uluslararası ilişkilerde gerilimlere neden olabilmektedir.

Siber uzayda istihbarat faaliyetleri, fiziksel alandaki gibi devletlerin çıkarları doğrultusunda şekillenmektedir. Bu konuda tespit edilen kişi veya kuruluşlar -şayet vatandaş ise veya faaliyeti ülke içinde gerçekleştiriyorsa- kolluk kuvvetleri tarafından

yakalanabilmektedir. Ancak bu faaliyetler yalnızca devletlere çıkar sağlamak için değil, devletlerin aleyhine de kullanılabilmektedir. Gerçekleşen birtakım "ifşa" olayları, devleti, devlet kurumlarını ve kişileri büyük bir sorunla yüzleştirmiştir.

Edward Snowden ve Julian Assange olayları, bu konuda verilebilecek en belirgin örneklerdir. Bu iki olayda da bireylerin fiziki yollarla elde ettikleri bilgileri siber uzay aracılığıyla kamuoyuna açabilmeleri, siber uzaydaki casusluk faaliyetlerini görünür hale getirmiştir. NATO'nun siber savaş ve rekabetin yasal çerçevesini tanımlayan Tallinn Manual 2.0'ı yayınlamasındaki temel motivasyon kaynaklarından birini de bu iki olay oluşturmuştur. Edward Snowden'ın NSA belgesi sızıntıları, siber uzayı bir dış politika aracı olarak gören Rusya'nın siber alanda daha sıkı kontrol edilmesi gerektiğini göstermiştir. Özellikle Rusya'nın 8 Kasım 2016'da ABD başkanlık seçimlerine yaptığı müdahaleler, istihbarat konusunu gündeme taşımıştır (Kulaç, 2020). Keza Rusya Devlet Başkanı Vladimir Putin'in istihbarat geçmişi göz önünde bulundurulduğunda, bu faaliyetlerin devam edeceği öngörülebilir (Çınar, 2023, s. 300).

UNGGE, istihbaratla ilgili endişelerini defalarca kez dile getirmiştir. İlk UNGGE oturumunda üye ülkeler, devletlerin BİT'i askeri amaçlarla ve istihbarat araçları olarak kullanma potansiyelinden endişe duyduğunu ifade ettiler. Bu endişeler, BİT'in savaş ve terörizmle mücadelede kullanılması, devletlerin birbirleriyle ve vatandaşlarına karşı casusluk yapması ve BİT'in sivil nüfusa karşı kullanılarak insan hakları ihlallerine yol açması gibi çeşitli konuları içeriyordu (Pijović, 2021, s. 220).

İkinci UNGGE oturumunda üye ülkeler bu endişelerini tekrarladı ve devletlerin BİT kullanımına ilişkin normları geliştirmek için daha fazla diyalog yapılması çağrısında bulundu (Pijović, 2021, s. 220). Bu girişimler, devletlerin BİT'i barışçıl ve sorumlu bir şekilde kullanmalarını ve insan haklarını ve uluslararası hukuku ihlal etmelerini önlemeyi amaçlamaktadır. Dolayısıyla UNGGE'nin istihbaratla ilgili endişeleri, BİT'in uluslararası güvenlik ve istikrar için oluşturduğu potansiyel tehditlerin farkındalığını yansıtmaktadır. Bu bağlamda devletler, BİT'i sorumlu bir şekilde kullanmak ve bu teknolojilerin kötüye kullanımını önlemek için birlikte çalışmalı ve uluslararası hukuku ve normları uygulamalıdırlar.

İstihbarat faaliyetleri, bilgi güvenliğinin BM gibi uluslararası kurumlar tarafından sağlanması ihtiyacını da doğurmuştur. Zira bugün bu faaliyetlerden en çok etkilenen devletlerdir. Çünkü uluslararası hukuk, barış zamanı casusluğu için özel bir düzenleme

içermez, bu nedenle siber destekli casusluğa ilişkin özel bir "uluslararası casusluk yasası" yoktur. Ancak, bu, siber casusluğun uluslararası hukuk boşluğunda var olduğu anlamına gelmez. Barış zamanında işlenen casusluktan farklı olarak, silahlı çatışma zamanlarında gerçekleşen siber casusluk, UİH tarafından düzenlenir (Buchan & Navarrete, 2020). Siber uzayda UİH sorunu da devletler arasında önemli bir anlaşmazlık konusudur. UİH'in siber uzaya uygulanabilirliği konusundaki tartışmalar, 2015 UNGGE konsensüs raporu üzerindeki müzakerelerde başladı. Bu raporda UİH'in siber uzaya uygulanabilirliği konusundaki anlaşmazlık, nihai metinde yalnızca "insanlık, gereklilik, orantılılık ve ayrım" ilkelerinin uygulanabilirliğine atıfta bulunulmasıyla kısmi bir çözüme kavuşturuldu (D'Incau & Soesanto, 2017).

Görüldüğü üzere siber istihbarat, uluslararası hukuk açısından tartışmalı bir konudur. Barış zamanı casusluğu uluslararası hukuk tarafından özel olarak düzenlenmemiştir fakat uluslararası hukukun genel ilkeleri bu faaliyetleri sınırlandırmaya çalışmaktadır. İnternet, uluslararası bir alan olduğundan, internette uluslararası hukuk normlarının ve insan haklarının geçerli olduğu savunulmaktadır. Bu nedenle devletlerin ve istihbarat örgütlerinin interneti kullanırken uluslararası hukuk ve insan haklarına saygılı olmakla yükümlü olduğu ifade edilmektedir (Gill & Redeker & Gasser, 2015, s. 7). Ancak bu, internet erişimini, ifade özgürlüğünü, gizlilik haklarını ve kişisel verilerin korunmasını güvence altına alan yeni bir hukuk mekanizmasıyla mümkündür.

Prensip olarak, yeni bir uluslararası hukuk oluşturmak, siber istihbarat gibi tartışmalı konuların uluslararası hukuk tarafından daha iyi düzenlenmesini sağlayabilir. Bu, devletlerin siber istihbarat operasyonlarını yürütme şeklini daha şeffaf ve sorumlu hale getirebilir. Ayrıca siber istihbarat operasyonlarının uluslararası hukuku ihlal etme olasılığını azaltabilir. Ancak pratikte, yeni önerilen yasalar üzerinde fikir birliğine varılması elbette zor olacaktır. Bu, özellikle ulusal güvenlik ve savunma gibi tartışmalı konularla ilgili olduğunda geçerlidir. Zira devletler, kendi ulusal güvenlik ve ulusal çıkarlarını korumak için siber istihbarat operasyonlarını yürütme haklarını daima saklı tutmak isteyeceklerdir. Bu nedenle, yeni yasaların bu çıkarları korumaya yönelik olması ve devletlerin siber istihbarat operasyonlarını yürütme konusunda fazla kısıtlama getirmemesi için uğraş vereceklerdir. Şanghay İşbirliği Örgütü'nün 2015 tarihli "Bilgi Güvenliği için Davranış Kuralları" girişimi, siber istihbarat konusunda bir küresel norm geliştirme çabası olarak nitelendirilse de, daha fazla devlet kontrolünü ve sansürü meşrulaştırdığı görülmüştür (D'Incau & Soesanto, 2017).

Sonuç olarak siber alanda vuku bulan bazı ifşaatlar, istihbarat ajanslarının kişisel verilere sızdığı gerçeğini açığa çıkarmış ve ulusal güvenlik adı altında hukukun üstünlüğünün nasıl zedelendiğine dair somut kanıtlar sunmuştur. Bu durum, hukukun üstünlüğünün insan haklarının korunmasının temel bir unsuru olmasına rağmen, gerçek anlamda bir savunma mekanizması olarak yetersiz kaldığını göstermektedir. Bununla birlikte kolluk kuvvetleri ile istihbarat ve güvenlik ajansları arasında giderek artan işbirliği, hukukun üstünlüğüne yönelik bu zafiyetin, yargı sistemi içinde de benzer bir erozyona yol açabileceği endişesini artırmaktadır. Zira bu durum, temel hak ve özgürlüklerin ihlal edilme riskini artırmaktadır. Ulusal ve uluslararası düzeyde açık yasal çerçevelerin eksikliği, siber alanda hukukun üstünlüğü için ciddi bir risk oluşturmaktadır. Bu nedenle gizli gözetimin meşruiyetini ve kapsamını sınırlandırmak ve bireylere haklarını koruma konusunda etkili araçlar sunmak üzere yasal çerçevelerin oluşturulması zorunluluğu ortaya çıkmaktadır.

3.2.3. Siber Suçlar

Siber suçlar, birçok devletin iç hukukunda tanınmakta ve suç sayılmaktadır. Bir cihaza veya ağa izinsiz erişildiğinde siber suç gerçekleşmiş olur. Dolayısıyla hangi amaçla yapılmış olursa olsun, her siber saldırı, hukuki bir suç unsuru teşkil etmekte ve siber suç sayılmaktadır (Akyeşilmen, 2018a, s. 74). Siber suçların uluslararası mahiyeti, yasal çözümlerin ulusal hukuktan uluslararası hukuka aktarılması sürecini başlatmış ve hukukun küreselleşmesine katkıda bulunmuştur (Simović vd., 2020, ss. 27-28). Hukuk, her ne kadar küreselleşse de, bu durum devletlerin ulusal çerçevede hareket etmesini engelleyememiştir. Zira devletler, yargı yetkisini, yani bir devletin kendi toprakları içindeki kişileri, mülkleri ve koşulları etkileme gücünü kullanmaktan vazgeçememektedir. Bu yetki, uluslararası bir anlaşmayla sınırlanmadığı müddetçe; yasama, yürütme veya yargı yoluyla kullanılabilir (Shaw, t.y.). Bu yetkinin sınırlandırılmasına yönelik endişeler, siber alanda da benzer şekilde tezahür ettiğinden – yani ulusal kontrol mekanizmaları daha cazip göründüğünden – bu alanda uluslararası kaynaklar yok denecek kadar azdır.

Genel itibariyle referans alınan, biri evrensel, diğeri bölgesel olmak üzere iki kaynaktan söz edilebilir. Bunlardan birincisi, evrensel olarak kabul gören Sınıraşan Örgütlü Suçlara Karşı BM Sözleşmesi'nin 14. ve 29. Maddeleridir. Sözleşme, devletleri siber alanda işlenen ulusötesi organize suçlara karşı kolluk kuvvetlerini eğitmek ve diğer

devletlerle işbirliği yapmakla yükümlü kılmaktadır (UN, 2001). Bölgesel nitelikteki kaynak ise, Avrupa Konseyi Siber Suç Sözleşmesi ve Irkçı ve Yabancı Düşmanlığı Eylemlerinin Bilgisayar Sistemleri Aracılığıyla Cezalandırılmasına İlişkin Ek Protokol'dür. Bu belge, imzacı devletleri siber faaliyetlerin yasadışı kullanımını suç saymaya zorlamaktadır. Sözleşmeye göre devletler siber suçları kovuşturmaktan sorumludur (CoE, 2003). Bu bağlamda ceza hukuku ve uluslararası işbirliği, uygun çözümler olarak kabul görmüştür (Simović vd., 2020, s. 28).

Aralık 2019'da 74. BM Genel Kurulu, aldığı bir kararla siber suçların önemine dikkat çekmiştir. Kabul edilen BM kararına göre, "bilgi ve iletişim teknolojilerinin suç amaçlı kullanımına karşı kapsamlı bir uluslararası sözleşme hazırlama" yetkisiyle "açık uçlu geçici bir hükümetlerarası uzmanlar komitesi" kurulması kararlaştırıldı. Siber suç anlaşması oluşturulmasına yönelik süreç, Rusya tarafından başlatılmıştır. Sunulan BM kararı, Genel Kurul'da 79 oyla kabul edilmiştir. Altmış devlet (çoğunlukla Batı ülkeleri) aleyhte oy kullanırken, 33 devlet çekimser kaldı. Batı ve Latin Amerika, daha önceki siber suç tartışmalarının Suç Önleme ve Ceza Adaleti Komisyonu (CCPCJ) aracılığıyla yapılması gerektiği fikrini desteklemişlerdir (Kleinwächter, 2020). Toplantıda Rusya, sözleşmenin amacının 'gelişmiş ve gelişmekte olan ülkeler arasındaki teknolojik uçurumu kapatmak' olduğunu ifade etse de; Rusya'nın esas amacı, Avrupa Konseyi'nin Siber Suçlarla ilgili Budapeşte Sözleşmesi'ne alternatif olarak oluşturulacak yeni bir anlaşmaya liderlik etmektir. Siber uzayla konularda kilit bir konumda olan Çin, Rusya'nın pozisyonuna destek vermiştir (Walker, 2021).

2019'daki BM kararının 2001'den beri geçerliliğini koruyan Budapeşte Sözleşmesi'nin yerine geçebilecek yeni bir anlaşmaya evrilebileceği tartışmaları gündemdeki yerini korurken, 26 Mayıs 2021'de BM Genel Kurulu'nda Rusya tarafından siber suçlarla ilgili yeni bir karar oylamaya sunulmuş ve yeniden üye devletler arasında derin bir anlaşmazlığa sebebiyet vermiştir (Walker, 2021). Ancak yine de, yukarıda da bahsi geçen BM'nin Siber Suçlarla Mücadele Sözleşmesi, Mayıs 2021'den beri müzakere edilen ve siber suçlarla mücadelede uluslararası işbirliğini güçlendirmeyi amaçlayan potansiyel bir uluslararası anlaşma girişimi olarak ortaya çıkmıştır. Müzakerelerin son oturumu Ocak 2024'te New York'ta gerçekleşmiş olup, anlaşmanın 2024 yılı içerisinde tamamlanması beklenmektedir.

Özellikle BM Güvenlik Konseyi daimî üye devletlerinin üzerinde uzlaşabileceği bir uluslararası politikanın geliştirilmesine yönelik ciddi zorluklar söz konusu olmasına rağmen devletlerin büyük çoğunluğu, bu konuda geliştirilecek işbirliğinin uluslararası barış ve istikrara sağlayacağı katkının farkındadırlar. Zira uluslararası politikanın getirisinin, her bir üye devlet tarafından oluşturulan ulusal mekanizmalardan daha yüksek olacağı bilinen bir gerçektir. Bu doğrultuda siber suçlarla mücadele için oluşturulan antlaşmalar gibi uluslararası girişimler, küresel yönetişim üzerinde standartlar oluşturulması açısından önem arz etmektedir.

Önemli olan nokta, devletlerin çıkarlarını gözeten bir mekanizmadan ziyade, küresel internet yönetişimin bütün paydaşlarının haklarını gözeten, insan haklarını ve etik unsurları güvence altına alan kapsayıcı ve adil bir mekanizmanın inşa edilmesidir. Çünkü bugüne kadar geliştirilen veya geliştirilmekte olan mekanizmalar, gerek kapsayıcılık ve adalet açısından; gerekse de insan haklarını gözetme bakımından ciddi eleştirilere maruz kalmaktadır. Örneğin, Budapeşte Konvansiyonu ve BM Siber Suçla Mücadele Sözleşmesi gibi uluslararası sözleşme ve sözleşme girişimleri, yazım ve uygulama aşamaları konusunda eleştirilere maruz kalmaktadır. Budapeşte Konvansiyonu, uluslararası uyumlaştırma girişimlerinde dünyanın en kalabalık ülkelerini dışladığı gerekçesiyle eleştirilere maruz kalırken; BM Siber Suçla Mücadele Sözleşmesi'nin taslağı, ifade özgürlüğüne ve gözetime yönelik tehdit oluşturma potansiyeli nedeniyle eleştirilmektedir. (Dixit, 2022, s. 89; Rodriguez, 2023).

Sonuç olarak, uluslararası işbirliği çerçevesinde siber suçlarla mücadelede önemli adımlar atılmış olmasına karşın, ceza hukuku alanında geniş çapta bir uzlaşıya ulaşılması konusunda zorluklar devam etmektedir. Geleneksel uluslararası ceza hukuku, mevcut suç türlerini düzenleyerek maddi ve usul hukukunu uyumlaştırmaya çalışırken, siber suçlar gibi yeni suç formları bu tür bir uzlaşıyı karmaşıklaşmaktadır. Bazı devletler, bu yeni suç türlerine yönelik uluslararası bir anlaşma oluşturma konusunda istekli olsa da, uluslararası yargı konusundaki deneyim ve bilgi eksikliği, kamuoyunun dışlanması ve ulusal çıkar çatışması gibi faktörler nedeniyle genellikle sınırlı bir uzlaşıya varılabilmektedir (Dixit, 2022, ss. 88-89).

3.3. Siber Hukuka Yönelik Yaklaşımlar

Çalışmanın tamamında vurgulandığı üzere dünya giderek artan bir siber tehdit sorunuyla karşı karşıyadır. Bu sorunla mücadele için daha fazlasının yapılması

gerektiği konusunda neredeyse herkes hemfikir olsa da, sorunun çözümüne yönelik öneriler çok çeşitli yöntem ve teknikleri ortaya çıkarmaktadır. Bazıları, mevcut uluslararası hukuk sisteminin daha etkin bir şekilde kullanılması gerektiğini öne sürmekte iken; diğerleri, mevcut uluslararası hukuk sisteminin yetersiz olduğunu ve yeni bir hukuk mekanizması oluşturulması gerektiği konusunda görüş bildirmektedir. Bunun yanında, kimisi ulusal hukuk düzenlemesinden yana iken; kimisi (belki de en radikal olan görüş bu) zamanla siber normların tıpkı teknik alandaki gibi kendiliğinden gelişeceğini öne sürmüştür.

3.3.1. Uluslararası Hukuk Yaklaşımı

Uluslararası hukuk, devletlerin egemenliğine ve temel prensiplere dayanarak, devletlerin hakları ve sorumluluklarını belirler. Devletlere uluslararası hukuk çerçevesinde tanınan her hak, karşılığında yerine getirilmesi beklenen sorumlulukları da beraberinde getirir. Bir devlet, uluslararası anlaşmaları ihlal ederek veya başka bir devletin toprak bütünlüğüne saldırarak doğrudan bir ihlal gerçekleştirebilir. Bu durum, uluslararası hukukun temel prensiplerine açıkça aykırı olup, ilgili devletin uluslararası toplum nezdinde sorumlu tutulmasını gerektirir. Çünkü uluslararası hukuk, hem 'saldırıyı' (bir devletin diğerine karşı haksız güç kullanması) hem de 'müdahaleyi' (başka bir devletin toprakları içinde haksız yere güç kullanılmasını) yasaklar (Nardin, 2022).

Uluslararası hukuka göre devlet, kendi içindeki yetkili organların, yani yürütme, yargı ve idari organlar dahil, eylemlerinden de sorumludur. Bu sorumluluk, yetkili organların yetkilerini aşan eylemleri dahi kapsar ve ilgili devletin uluslararası hukuka aykırı eylemleri nedeniyle sorumluluğunu ortaya koyar. Özel kişiler tarafından gerçekleştirilen eylemler bakımından devletler, bu eylemleri sonradan benimsemiş olmaları durumunda sorumlu tutulabilir. Bu, devletin, özel kişilerin uluslararası hukuka aykırı eylemlerini onaylaması veya bu eylemleri kendi politikaları olarak kabul etmesi anlamına gelir (Shaw, t.y.).

Bu noktada, uluslararası hukuk yaklaşımını savunanlara göre siber uzay, fiziksel alandan farklı bir alan olmadığından ve sorun alanları aynı olduğundan yeni bir hukuki düzenleme veya yargı mekanizması gerekli değildir. Onlara göre “siber” ve “gerçek” hukuk arasındaki bağlar daha sıkı bir şekilde gelişmiştir (Kulesza, 2012, s. 146). Mevcut uluslararası hukuk norm ve ilkeleri, siber uzaya da pekâlâ uygulanabilir.

İnternetin uluslararası alanda yasal düzenlemesine yönelik iki farklı bakış açısından söz edilebilir. Dar bakış açısı, internetin çalışmasını sağlayan kurumsal düzenlemeleri içerir. Geniş bakış açısı ise, internet ile etkileşime giren uluslararası hukuk kurallarının uygulanabileceği tüm sektör ve alanları kapsamaktadır (Serrano, 2019).

Slack'a göre bu alan karmaşık ve zordur, evet. Fakat katiyen yeni bir anlaşma veya yasal çerçeveyi gerektirecek kadar değil (2016, s. 71). Bu bakış açısına göre, uluslararası hukukun mevcut ilkeleri, devletlerin siber uzaydaki faaliyetlerini düzenlemek için yeterli araçları ve yönergeleri zaten sağlamaktadır. Bu argüman, mevcut uluslararası hukukun esnekliğine ve adaptasyon yeteneğine dayanarak, siber uzayla ilgili zorlukların üstesinden gelmek için yeni bir anlaşmanın gerekli olmadığını ve mevcut yasal çerçevenin uygun şekilde uygulanabileceğini öne sürer. Bu görüş aynı zamanda, siber uzayın özgül dinamiklerini ve sorunlarını ele almak için özel düzenlemeler yapmaksızın, mevcut uluslararası hukuk kurallarının genişletilmesi ve yorumlanması yoluyla siber tehditlere ve zorluklara yanıt verilebileceğini savunur.

Corn ve Taylor, uluslararası hukuku modern uluslararası düzenin temel direği olarak kabul eder ve onun hem devlet hem de devlet dışı siber faaliyetlere uygulanabilirliğinin "sorgulanamaz" olduğunu iddia eder (2017, s. 207). Siber alanda uluslararası hukukla uyumlu alanları tespit etmek mümkündür. Siber alana uygulanan ulusal yasalar düşünüldüğünde, uluslararası alanda da bunun mümkün olabileceği fikri gündeme gelmektedir. Slack (2016), siber uzayın karmaşık doğasına rağmen, mevcut uluslararası yasal rejimlerin yeterli olduğunu savunmuştur. Ona göre uluslararası hukuk siber uzay için geçerli iken; sorunlu olan, nasıl uygulanacağıdır. Bunun çözümü, normatif bir yaklaşıma dayalı olarak, uluslararası "siber" ilişkilerin mevcut siyasi ve stratejik çerçevelerinin inşa edilmesidir.

Serrano'ya göre (2019) de uluslararası hukukun siber alana uygulanabilirliği sadece mümkün değil, aynı zamanda bu yeni ortamın gerçekten küresel olması nedeniyle de zaruridir. Bu konuda atılan adımlar cılız olsa da, bu "yeni tip" zorlukları çözmek için geleneksel anlamda uluslararası hukuk kurallarına ihtiyaç vardır. Bu nedenle, yargı yetkisi ve devlet sorumluluğuna ilişkin geleneksel kalıplar, işlevlerini yeni koşullara uyumlu hale getirmek zorundadır. Bu doğrultuda siber alanda güven ve sorumluluk artırılmalıdır, bu nedenle fiziksel alanda uygulanan mekanizmanın aynısı siber alanda da uygulanmalıdır. İnternet kullanıcılarının daha fazla veya daha az meşruiyet, inanç ve

güvene sahip olması, fiziksel mekanizmanın online ortama uyarlanmasıyla sağlanabilir (Mihr, 2016, s. 328).

Mačák (2017), uluslararası hukukun siber alana uygulanabilirliğini kabul etmiş, fakat çağdaş teknolojik gelişmelerin ortaya çıkardığı zorluklara yanıt vermede yetersiz kalmasının sorumlusu olarak devletleri göstermiştir. Mačák, devletlerin bu hukuk süreçlerine katılım konusunda tereddüt etmelerinin bir güç boşluğu yarattığını iddia etmektedir. Bu boşluğu doldurmak için, Microsoft'un siber norm önerileri[56] ve Tallinn Manual gibi devlet dışı aktörler tarafından yapılan girişimlere dikkat çekmektedir. Bu bağlayıcı olmayan normlar sayesinde, devletlerin hukuk yapma süreçlerinde yeniden merkezi bir rol üstlenebilecekleri ve bu durumun, nükleer güvenlik gibi alanlarda oluşturulan yasal rejimlerle benzer bir yol izleyebileceğini ifade etmektedir. Mačák, aynı zamanda, bu durumun uluslararası siber uzay yönetişiminde bir çöküşe mi yoksa hukuki yaklaşımların yeniden şekillenmesine mi yol açacağının yakın gelecekte belli olacağını belirtmiştir. Yine de mevcut durumda bazı ülkeler, internet teknolojisi ve çevresindeki hızlı değişikliklere karşı koymak ve aynı zamanda kuralları belirleme sürecindeki avantajlarını korumak için, BM Şartı ve uluslararası hukukun mevcut yasal çerçevesi içindeki kurallara düzenlemeler yapılması gerektiğini savunmaktadır. Bu görüşün savunucuları, değişikliklerin çok hızlı ve radikal olmaması gerektiğini, böylece mevcut sistemdeki dengeyi koruyarak, istikrarı sağlayacak şekilde ilerlemek gerektiği fikrini savunmaktadır (Murthy, 2014, s. 2307).

Bugün, siber faaliyetler için uluslararası hukuk mekanizmasını savunanlar dahi, geniş çaplı bir anlaşmaya şüphe ile yaklaşmaktadır. Zira mütemadiyen kendini güncelleyen dinamik bir alan için sabit norm ve kuralların yerleşmesi oldukça zordur. Cenevre Sözleşmelerine benzer çok taraflı bir anlaşmanın doğurabileceği sonuçlar ucu açık ve kestirilemez niteliktedir. Ancak, bu dinamik ve çok yönlü alan için doğan norm ihtiyacı da yakın gelecekte giderilmeye çalışılacaktır. Bu minvalde pek çok adım atılmakta ve bu konuda istekli devletler tarafından faaliyetlere devam edilmektedir (Nye, 2010, s. 18).

[56] Microsoft, Aralık 2014'te "İnternete Bağımlı Bir Dünyada Çatışmayı Azaltmak" başlıklı bir beyaz kitap yayınladı. Bu doküman, özel sektör tarafından sunulan ve online davranışların önemli yönlerini - güvenlik, mahremiyet ve vergilendirme dahil- düzenlemek üzere uluslararası standartlar benimsemeye çağrıda bulunan ilk kapsamlı teklif olarak dikkat çekmektedir. Microsoft'un bu önerisi, yalnızca devletlerin davranışlarını düzenleme iddiasında bulunan ve bilgi iletişim teknolojisi ürün ve hizmetlerinin 'ulus devletler tarafından askeri operasyonların bir parçası olarak kullanılmasını, suiistimal edilmesini veya istismar edilmesini' azaltmayı hedefleyen altı siber güvenlik normu içermektedir (Mačák, 2017, s. 15).

Bu yaklaşım pratikte bir anlam ifade eder mi? Devletler arasındaki konularda bir nebze etkili olacaksa da, bireyler, özel sektör ve kuruluşlar bu noktada eksik kalacaktır. Zira yukarıda da belirtildiği üzere yalnızca devleti bir hukuk süjesi olarak kabul eden bir mekanizma, siber uzaydaki diğer aktörleri göz ardı edeceğinden bir müddet sonra işlemez hale gelecek veya -daha pozitif bir bakış açısıyla- kendini güncellemek durumunda kalacaktır. Zira siber alan, mevcut yasal çerçeveye meydan okumaktadır. Bu nedenle mevcut yasal çerçevenin kullanımı pek çok durumda zorlaşmaktadır.

3.3.2. Ulusal Hukuk Yaklaşımı

Egemenlik, uluslararası hukukun temel bir ilkesidir ve "milletler hukukunun temel anayasal doktrini" olarak kabul edilir (Corn & Taylor, 2017, s. 209). Siber uzay ise, kurgusal yapısına rağmen, gerçek ve somut altyapılara dayanır. Siber uzayın ve internetin fiziksel mimarisini oluşturan bilgisayar ağları ve bileşenleri gerçektir ve devletlerin egemenlik sınırları içinde yer alır. Bu durumda devletlerin toprak egemenliğinin bilgisayar ağlarını da kapsayıp kapsamadığı sorusu gündeme gelmektedir (Delerue, 2020, s. 206).

Tsagourias'a göre, siber uzayın doğası, bir anlaşmanın devletlerin yanı sıra kamu ve özel kuruluşları da içermesini gerektirir. Ancak bu durum, uluslararası hukukun her zaman bir paydaş grubunu meydana getirir. Dolayısıyla Tsagourias, böylesine kapsamlı bir rejim olasılığının düşük olduğunu belirtir. Bunun yerine, mevcut uluslararası kurallar ve ilkelerin siber uzay için geçerli olmaya devam ettiğini ve devletler veya devlet dışı aktörlerin buna uyması gerektiğine dair çağrılar yapıldığını ifade eder. Fakat Tsagourias'a göre, kuşkusuz, uluslararası hukuk devletlerin siber uzaydaki davranışlarını ve çıkarlarını şekillendirmekte ve belki de rasyonelleştirmektedir ancak nadiren ulusal mevzuatın önüne geçmektedir (2015, s. 29).

Siber faaliyetlerin düzenlenmesine yönelik sayısız ulusal girişim söz konusudur (Kulesza, 2012, s. 146). Bugün devletler, siber uzaydaki faaliyetleri stratejik, güvenlik ve siyasi amaçlar için kendi yetki alanları dahilinde şekillendirme ve sınırlama eğilimindedir (Watt, 2017+, s. 60). WSIS'in yaptığı internet yönetişimi tanımında devletlerin politika yapımında "egemen" aktörler olarak kabul edildiğini belirtmiştik. Bu durum, alınan kararların ulusötesi çıkarları göz ardı edebilme ihtimalini artırmakta ve politika kararlarının uygulanması için gereken meşruiyeti zayıflatabilmektedir (van der Spuy, 2017, s. 33).

Chouchri'ye (2014) göre siber uzayın yaygınlığı ve küresel erişimi, onun özel sektör tarafından yönetilmesini gerektirmiştir. Buna rağmen siber alan halen bir devletin veya başka bir ülkenin yetki alanına girmemektedir. Siber alanı oluşturan fiziksel altyapının çoğu, vatandaşlar veya şirketlerin özel mülkiyetidir ancak protokolleri tanımlayan standartların belirlenmesinde devlet kurumları önemli bir rol oynamaktadır. Altyapının büyük bir kısmı özel sektöre ait olmakla birlikte, ulus-devletler kendi egemenliklerini, siber alanın yetki alanlarına giren fiziksel unsurları üzerinde kullanırlar. Devletler, siber uzaydaki faaliyetler üzerinde ulusal yasaları kullansa da bu yasalar çoğu durumda işlevsiz kalmaktadır.

Ulusal yasaların işlevsiz kalması, internet yönetişimi düzenlemelerinde meşruiyet sağlamaya yönelik sorunları ortaya çıkarmaktadır. Bunun en önemli nedeni, internet yönetişim mekanizmalarındaki güç dengesizlikleridir. Çoğu ülke, internet yönetişimini tanımlama veya yönlendirme sürecine nispeten "geç" katılmıştır. Bunun yanında, çoğu devletin yargı yetkisi kısıtlamaları nedeniyle interneti düzenleme kapasitesine veya yeteneğine sahip olmadığına dair argümanlar öne sürenler olmuştur (Lessig, 2006, s. 3). Örneğin, internetin ticari potansiyelinden yararlanmak isteyen bazı ülkelerin bunun için gerekli olan donanıma sahip olmadıkları görülmüştür. En basit şekilde, yüz yüze işlemlerde veya kredi kartı kullanımında bile yasal kurallar ve yaptırım mekanizmaları oldukça yetersizdir (Sadowsky & Zambrano & Dandjinou, 2004, s. 13).

Siber güvenlik için uygulanan yasalar, ülkeden ülkeye ve ilgili yargı yetkisine göre değişir. Aynı şekilde cezalar da işlenen suça göre para cezasından hapis cezasına kadar değişiklik gösterir. Vatandaşların siber güvenlikle ilgili tüm bilgilerden haberdar olmalarını sağlamak için kendi ülkelerinin siber yasalarını bilmeleri çok önemlidir. Özellikle e-ticaret kullanımındaki artış, yanlış uygulamaların önüne geçmek için birtakım düzenleyici uygulamalar getirdi. Örneğin, devlet sınırlarını aşan e-ticari faaliyetler uluslararası sonuçlar doğurduğundan, tüketici haklarının gözetilmesi gibi durumlarda zorluklar meydana gelmektedir. Örneğin ABD menşeili bir şirket, Avrupa'nın gizlilik prosedürlerine maruz kalabilmekte. Benzer şekilde Avrupalı bir şirket, vergileri Avrupa'da mı yoksa ürün gönderdiği ülkede mi ödeyeceğine karar vermek zorunda kalmakta. Bu tür eylemlerin yasal sonuçlarına dair bir standart henüz geliştirilemediğinden, karar mekanizması da işlemez hale gelmektedir (Kulesza, 2012, s. 32). Bu aktörlerden herhangi birinin kuralları veya siber yasaları ihlal ettiği tespit edilirse, mağdur kişi/firma o kişiye karşı işlem yapabilir. Bu nedenle devletlerin çıkar

dengelerini göz önünde bulundurarak siber alandaki hangi faaliyetlere izin vermeleri gerektiğini saptamaları gerekmektedir.

Öte yandan devletler, siber alandaki saldırıları önlemek için yasal çözümler ararken; sivil itaatsizlik, suç faaliyeti ve terörizm arasında ayrım yapmak durumundadır. Sivil itaatsizlik, bir yasayı veya kuralı protesto etmek için yasadışı bir eylemde bulunmaktır. Suç faaliyeti, yasadışı bir şekilde başkalarına zarar vermek veya zarar vermek için yapılan bir eylemdir. Terörizm ise, korku uyandırmak veya siyasi bir amaç elde etmek için şiddet veya tehdit kullanan bir eylemdir. Ancak terörizm tanımı, ülkeden ülkeye değişebilir. Bazı ülkeler, terörizmi sadece şiddet veya yıkımla değil, aynı zamanda korku uyandırmakla da tanımlar. Bu nedenle bu konuda yasal çerçevenin sağlanması oldukça zordur. Keza sivil itaatsizlik gibi eylemlerin ifade özgürlüğünün bir şekli olduğunu savunanlar için bu durum da sorunlu kabul edilmektedir (Mansell, 2004, s. 7).

Gelişmekte olan ülkelerde, fiziksel alandaki yasal işlemlerde internetin de gözetilmesi gerektiği anlaşılmaya başlanmıştır (Sadowsky vd., 2004, s. 13). Halbuki devletler, özellikle internetin ilk çıktığı zamanlarda genellikle interneti, ticareti ve iletişimi kolaylaştıran bir araç olarak görmüşlerdir. Bygrave ve Michaelsen, bu nedenle, devletlerin başlangıçta internet yasalarını hazırlarken siber uzayın doğasını göz önünde bulundurmadıklarını iddia etmiştir. Buna örnek olarak 1995 yılında AB tarafından kabul edilen Veri Koruma Direktifi'ni göstermişlerdir. Onlara göre bu belge, dijital ortamın doğasını dikkate almadan hazırlanmasına rağmen hükümleri dijital alana uygulanabilir düzeydedir. Ancak özellikle Diretif'in 4. Maddesini, AB ülkelerinin yasal veri korumasının AB dışında da uygulanmasını sağlaması gerekçesiyle sorunlu bulduklarını ifade etmişlerdir. Bunu bir örnekle açıklayan Bygrave ve Michaelsen, Hindistan'da AB'den gelen web sitesi ziyaretçilerinin AB üye devletlerinin gizlilik standartlarına uymasını beklemenin gerçekçi olmadığını savunmuşlardır (2009, s. 120). Bu, internetin coğrafi sınırları nasıl aştığını ve mesafeleri nasıl önemsiz hale getirdiğini anlamak açısından kritik bir noktadır.

Sınırlar elbette vardır, fakat bunların belirleyicileri eskisi kadar güçlü değildir. Çünkü internetin sınır ötesi yapısı, geleneksel güç kalıplarına meydan okumuştur. Bu öylesine bir meydan okumadır ki, internet öncesi çağda belirlenen fiziksel coğrafi sınırlar sorgulanmaya başlanmıştır (Sadowsky vd., 2004, s. 13). Bu nedenle, daha önce ulusal

veya bölgesel düzeyde başarılı bir şekilde uygulanabilen politikalar artık işlevsiz kalmaktadır. Bu politikaların internet ortamında ulusal veya uluslararası düzeyde koordine edilmesi oldukça zorlaşmıştır. Zira özellikle yerel düzeyde farklı hukuk sistemlerinin uygulanması, internetin sınır ötesi doğasıyla uyuşmamaktadır. Sonuç olarak, sınırlar arası bu denli bir etkileşimin olduğu bir ortamda yekpare bir uluslararası siber hukuk sistemine ihtiyaç vardır.

3.3.3. Öz-Düzenleme Yaklaşımı

Cerf (2004), internetin inovasyon için eşsiz bir alan oluşturduğunu ve bu inovasyonun, ağın ucundaki kullanıcılar ve cihazlar tarafından yönlendirildiğini belirtmiştir. Cerf'e göre geleneksel iletişim araçları (telefon, radyo, televizyon yayıncılığı, kablolu televizyon ve uydu iletişimi) sıkı bir şekilde düzenlenmişken, internet, bu düzenlemelerin üzerinde, "tabandan gelen" bir fenomen olarak gelişmiştir. İnternet, mevcut altyapıların -telefon hatları, uydu bağlantıları, optik iletim ağları gibi- üzerinde çalışır ve bu altyapıları kullanarak neredeyse sınırsız bir inovasyon ve uygulama geliştirme özgürlüğü sunar. Bu durum kullanıcılara herhangi bir düzenleyici müdahale olmaksızın, ağın ucunda bulunan cihazlar üzerinde çalışan yazılımlar aracılığıyla erişme ve geliştirme imkânı verir.

Öz-düzenleme yaklaşımı, internetin bu özelliklerine uyacak biçimde şekillendirilmiş yasal bir rejim önerisidir. Ancak "İnternet Haklar Bildirgesi" fikri yeni bir fikir değil. Böylesi bir belgenin taslağının hazırlanmasına yönelik ciddi çabalar, 1990'ların ortasında başladı. Bu yaklaşım, kalıcılığa ulaşarak bugün bile geçerliliğini korumaktadır. O dönemde radikal olarak nitelendirilen haklar, bugünün olağanı haline geldi. Gil, Redeker ve Gasser'in "dijital anayasacılık" olarak nitelendirdiği bu girişimler, siber alan için kapsamlı bir haklar, ilkeler ve yönetişim normları oluşturmaya çalışmaktadır (2015, s. 2).

Bu yaklaşımın 1990'larda önde gelen öncüleri olmuştur (Johnson & Post, 1998; Shapiro, 1998; Lessig, 1999a). 1980'ler ve 1990'ların başlarında siber alanın bağımsızlığını savunan liberal fikirler ön plana çıkmıştır (Bygrave & Michaelsen, 2009, s. 125). Johnson ve Post, geleneksel yargı ilkelerinin farklı ve özel bir çözüm gerektiren siber uzay için uygun olmadığını açıkça iddia eden ilk kişilerdi. Siber uzayın belirli alanlarını tanımlamaya, ayrıştırmaya ve korumaya yardımcı olabilecek ilkeleri belirlemek ve sınırlarını yasal ilkelere dayandırmak gerektiğini vurgulamışlardır. Buna

yönelik siber uzayda geçerli olabilecek bir kurallar dizisi önerdiler. “Kod” temelli yaklaşımı temsil eden bu öneri, siber alandaki tüm internet kullanıcıları için ortak kuralları içermiştir. Tüm internet kullanıcıları tarafından paylaşılan temel ortak ilkeler dizisi, siber hukukun temeli olan “vatandaşlık erdemi” ile mümkün olacaktır. Bu yaklaşım, internetin merkeziyetsiz, çeşitli ve karmaşık doğasını yansıtmaktadır (Johnson & Post, 1998, s. 2).

1996'da ABD İletişim Ahlakı Yasası kabul edildi.[57] Bu girişim, Barlow’un Siber Uzayın Bağımsızlığı Bildirgesi’ni yayınlamasına doğrudan vesile oldu. Yasa her ne kadar tepki çekse de, devletle doğrudan bağlantısı olmayan yargı organı tarafından geliştirilmiş olması, yasayı devlet müdahalesinden uzak bir konuma yerleştirmiştir. Bygrave ve Michaelsen, Barlow’un beyanında siber uzayın geleneksel yasaların erişiminin ötesinde olduğunu iddia etmesini eleştirmişlerdir. Onlara göre “internet ve siber uzay hiçbir zaman yasaların erişiminin ötesinde olmamıştır” (2009, s. 121). Kulesza da özerk bir internet yasasının uygulanabilir olmaktan uzak olduğunu ifade etmiştir (2012, s. 146).

Yine o dönemde IETF’nin rolü her şeyin üzerinde kabul ediliyordu. Bygrave ve Michaelsen’in Krol ve Hofmann’dan aldığı örnek, IETF’ye yönelik internet özyönetim tartışmalarını açıklamak için etkili bir benzetmedir:

> Bir kiliseye gidip onun öğretilerini ve felsefesini kabul ederseniz, onun tarafından kabul edilirsiniz ve ondan faydalanırsınız. Beğenmediyseniz, gidebilirsiniz. Kilise hala orada ve hiçbir faydası yok. İnternet de aynen böyle. Bir ağ İnternet'in öğretilerini kabul ederse, ona bağlıysa ve kendisini bunun bir parçası olarak görüyorsa, o zaman İnternetin bir parçasıdır. Hoşlanmadığı şeyleri bulacak ve bu endişeleri IETF aracılığıyla çözebilecek. Bazı endişeler geçerli kabul edilebilir ve İnternet buna göre değişebilir. Bazı değişiklikler dine aykırı olabilir ve reddedilebilir. Ağ, İnternet'e zarar verecek bir şey yaparsa, kötü yollarını düzeltene kadar aforoz edilebilir (Krol & Hoffman, 1993, s. 4).

Diğer yandan, öz-düzenleme yaklaşımında ICANN’in rolünü öne çıkaran argümanlar geliştirilmiştir. Schulz'a göre, bir sosyal normun hukuk normuna, sosyal normatif bir

[57] Ayrıntılı bilgi için bkz: U.S. Department of Justice. (1996). *Department of Justice's Review of Section 230 of the Communications Decency Act of 1996*. https://www.justice.gov/archives/ag/department-justice-s-review-section-230-communications-decency-act-1996.

sistemin de hukuk sistemine dönüşmesi için yargının üç boyutunu yerine getirmeleri ve üç boyutun sınavını geçmeleri gerekir. Schulz'un altını çizdiği üç kural: kural koyma, hüküm ve uygulama. Schulz'a göre ICANN, bu yargı gereksinimlerini karşılayan ve dolayısıyla kendi başına bir hukuk sistemi oluşturmaya hak kazanan normatif bir kurumdur (2007, s. 156). Dolayısıyla ICAAN, normatif bir hukuk sistemiyle hareket etmektedir. Bunun yanında, yumuşak hukuku kullanarak faaliyetlerini yasal bir zemine oturtmuştur. Helfer ve Dinwoodie, "ICAAN teoride yumuşak hukuku uyguluyor olabilir, ancak pratikte de daha sert bir hukuka sahip değildir" der. ICANN, kendi kurallarını koyan, hükme bağlayan ve uygulayan bir hukuk sistemine sahiptir. Bunun yanında, kendi bağımsız kurumlarını oluşturarak kural koyucu, yargılayıcı ve yaptırım yetkisine sahip normatif bir sistem oluşturmuştur (Koukiadis, 2015).

Koukiadis (2015); hukukun üstünlüğü, temsil, meşruiyet, şeffaflık, hesap verebilirlik gibi ilkeleri online kural ve normların oluşturulmasında aktifliğini kaybeden ilkeler olarak değerlendirmiştir. Ona göre kişilik hakları ve kişisel verilerin korunması, özel hayatın gizliliği gibi temel hakların üretilmesinde bu ilkeler geçerliliğini yitirmiştir. Bunun yerine, "*lex digitalis*", olarak kavramsallaştırdığı "hukukun ulusötesileşmesi", "devletsiz küresel hukuk" gibi argümanların önemine dikkat çekmiştir. Özdenetim ve ademi merkeziyetçilik gibi hukuk rejimlerinin varlığına dikkat çekmiş ve bunun meşruluğunu sorgulamıştır. Bunun yanında, "bilginin kendi kaderini tayin hakkı" gibi hakları da temel hak olarak tanımlamıştır.

Bugün, siber alan üzerindeki düzenleyici unsurlar, 1980'ler ve 1990'lardaki liberal çizgiden uzaktır. Bu idealler özellikle devletler nezdinde artık çok az değer görmektedir. O dönemlerde sansür ve filtreleme sistemlerinin kullanılması kesin bir dille reddedilirken; bugün olağan süreçler olarak kabul edilmektedir. Benzer şekilde o dönemlerde siber uzayın geleneksel hukuktan bağımsız olduğu iddia ediliyordu. Ancak bugün bu iddia, büyük bir çoğunluk tarafından sorunlu kabul edilmektedir. Siber uzay ve internet hiçbir zaman tam manasıyla herhangi bir yasadan bağımsız olmamış ve zamanla siber uzay, mevcut yasama sistemlerine daha çok angaje olmuştur. Bu nedenle bu görüşler oldukça radikal olarak nitelendirilebilir. On yıllardır süren tartışmalar bir çözüm sunamasa da, bu konuda da çözümün küresel bir bakış açısından geçmekte olduğu söylenebilir.

3.3.4. Uluslararası Siber Hukuk Yaklaşımı

Siber uzayın yasal düzenlemesi, doğası gereği uluslararasıdır (Kulesza, 2012, s. 31). Diğer bir deyişle siber uzay, doğası gereği kozmopolit ve ulusötesidir. Zaman ve mekândan bağımsız, küreselleşmiş bir alandır. Ulus-devlet egemenliğinin sınırları dışındadır. Bu nedenle siber uzay, hava, kara deniz ve uzay gibi diğer çatışma alanlarından ayrı değerlendirilmelidir. Nitekim siber faaliyetler bu dört alanda gerçekleşmekte ve bu alanlara ilişkin uluslararası hukuk normları ile düzenlenmektedir. Bu nedenle uluslararası hukukun siber uzaya uygulanabilirliği tartışmalı bir konu olmaktadır. Öte yandan, uluslararası siber hukukun geliştirilmesinde deniz hukuku, hava sahası hukuku ve dış uzay hukuku gibi alternatif modellerin referans alınması da bir çözüm getirmemiştir (Delerue, 2020, ss. 12-13). Bu yönüyle uluslararası siber hukuk yaklaşımının savunucularına göre siber uzay, geleneksel yasal düzenin kurallarından ayrı değerlendirilmelidir. E-ticaret işlemleri, telif hakkı ihlalleri, dolandırıcılık, haksız fiiller, gizlilik ihlali gibi sorunlara çözüm bulabilecek yeni kanun koyucu kurumların geliştirilmesi gerekmektedir (Koukiadis, 2015).

Bugün bu yaklaşımın savunucuları, internetin geleceğinden dahi endişe duymaktadır. Zira internet her ne kadar küresel bir ağ olsa da günden güne bu özelliğini yitirme tehlikesiyle karşı karşıya kalmaktadır. Zira internet küreselleştikçe, gelenekselci aktörler tarafından yerelleştirilmeye çalışılmaktadır. Bu da internetin ana işlevinin kaybolmasına sebebiyet verebilecek bir tehditle karşı karşıya olduğunu göstermektedir. "Ağların ağı" olarak nitelendirilen internetin küresel mahiyetini kaybetmesi, kademeli parçalanmasını da beraberinde getirecektir. Bu nedenle, ağın etkinliğini ve birlikte çalışabilirliğini korumak için kapsamlı bir düzenlemeye ihtiyaç vardır. İnterneti yöneten ortak yasal ilkelerin belirlenmesi, kullanıcıların haklarının korunmasını da kolaylaştıracaktır (Kulesza, 2012).

Bu coğrafi sınırsızlık üzerindeki yargı yetkisi konusunda fikir birliğinin sağlanması zordur. Kulesza, siber uzayın doğasına göre uyarlanmış bir uluslararası hukuk mekanizmasının sorunların çözümünde etkili olacağını savunmuştur. Bu noktada Kulesza, uluslararası düzenlemelere ihtiyaç duyulan alanları şu şekilde sıralayarak kategorize etmiştir:

1. İnternet ve telif hakkının korunması: online adil kullanım
2. Alan adları sistemi – İnternet ve Marka Hukuku

3. İnsan hakları ve ifade özgürlüğü
4. Sistem yakınsama – İnternet ve medya
5. Gizlilik hakkı
6. İçerik sorumluluğu
7. Siber suç ve ağ güvenliği
8. Elektronik ticaret (2012, s. 33)

Delerue'ye göre siber hukuk, uluslararası hukukun yeni bir alanı değildir. Siber faaliyetler; kara, deniz, hava ve uzay olmak üzere dört alanda gerçekleşen faaliyetlerdir. Bu nedenle, uluslararası hukukun siber uzaya uygulanabilirliğini sorgulamak gereksizdir (Delerue, 2020, s. 13). Söz konusu konvansiyonel ve nükleer silahlar olduğunda, küresel anlaşmalar nispeten etkili olmuştur. Borghard ve Lonergan (2018), bu anlaşmaların siber alanda etkisiz olduğunu ifade etmiştir.

Lawrence Lessig (1999c), "The Law of the Horse: What Cyberlaw Might Teach" başlıklı makalesinde, Yargıç Frank Easterbrook tarafından eleştirilen "at hukuku" metaforu üzerinden siber hukuk kavramını incelemektedir. Easterbrook, tıpkı atlar için özel bir hukuka ihtiyaç olmadığı gibi, özel bir "siber uzay hukukuna" da ihtiyaç olmadığını savunmuştur. Lessig, siber uzayın kendine özgü yönlerinin özel yasal ilkeler ve çerçeveler gerektirdiğini öne sürerek bu görüşe karşı çıkmaktadır.

Lessig analizini beş bölüme ayırarak siber uzayda düzenleme sorunlarına, düzenleme modeline, hukukun siber uzayı nasıl düzenleyebileceğine dair örneklere, siber uzay ve hukuk arasındaki rekabete ve siber uzay düzenlemesinin fiziksel alandaki hukuk sistemleri üzerindeki daha geniş etkilerine odaklanmaktadır. Lessig, siber uzayda düzenlemeyi anlamanın, düzenlemenin kendisi hakkında hem online hem de fiziksel olarak uygulanabilecek genel ilkeleri ortaya çıkardığını savunmaktadır. Lessig, geleneksel yasal yaklaşımların dijital ortamın getirdiği benzersiz zorlukları ele almak için nasıl uyarlanması gerektiğini göstermek için gizliliği koruma gibi örnekler kullanıyor. Lessig, pornografinin çocuklardan uzak tutulması ve gizliliğin korunması gibi örnekler üzerinden, siber uzayın kendine özgü mimarisinin -ya da kodunun- düzenlemede nasıl önemli bir rol oynadığını göstermektedir. Aynı zamanda, düzenleme için devlet müdahalesinin gerekli olduğunu savunmaktadır.

Börzel ve Risse'nin çalışmasında (2010), devletlerin bu modele ne derece tahammül göstereceği sorusu merkeze alınmıştır. İnternet, geleneksel çok taraflı hükümetlerarası

modellere alternatif olarak gelişen özel ulusötesi kurumlar için bir alan açmıştır. Ancak bazı devletler, egemenlikçi yaklaşımlarını koruyarak, yukarıdan aşağıya modellere dayalı düzenleyici uluslararası kuruluşların inşası için ısrar etmektedir. Eğer bu tür yönetişim modelleri sürdürülebilir olursa, meşruiyet, seçmenler ve etkileri hakkında sorular daha da önem kazanacaktır. Bu durum, uluslararası ilişkilerde işbirliği ve entegrasyon süreçlerinin nasıl işlediğini, devletlerin ve diğer aktörlerin bir araya gelerek karmaşık küresel zorlukları nasıl ele aldıklarını anlamak için bir fırsat sunar. Halihazırda bazı ülkeler, mevcut ağ yönetim kurallarının yeniden tanımlanması gerektiğini doğrudan ifade etmektedir. Bu görüşü savunanlar, küresel internet ortamındaki köklü değişikliklerin, mevcut yasal ve düzenleyici çerçevelerin yetersiz kaldığını ve bu nedenle yeni, daha uygun kuralların belirlenmesi gerektiğini öne sürmektedir. Siber hukuk savunucuları, internetin özel bir alan olduğunu ve bu nedenle özel yasal araçlara ihtiyaç duyduğunu savunur. Bu görüş, teknolojinin istisnai doğası ve internetin geleneksel yasal çerçevelere uymayan bazı temel özelliklerine dayanır (Murthy, 2014, s. 2307; Greenberg, 2016, s. 1501).

Geleneksel uluslararası hukuk anlayışında meşruiyetin temeli coğrafyadan ziyade egemenlik ve normlar üzerine inşa edilmiştir. Hukuka tabi olanlar için meşruiyet, kritik bir konumda yer almaktadır. İç hukukta genellikle meşruiyet coğrafi yakınlık yoluyla mümkün kılınmaktadır. Devletin iradesi, kanun koyucular, mahkemeler ve yürütme aracılığıyla eylemlerin meşruiyeti sağlanmakta ve kanunlar bu yetkiyle uygulanmaktadır. Bu nedenle internet, doğası gereği geleneksel yargı egemenliği kavramı için sorunludur. İnternetin eylemleri ve etkileşimleri yerinden etme becerisi hukukun meşruiyetinin yalnızca devletin kendi coğrafyasında kök salabileceği anlayışını terk etmeyi gerektirmiştir.

Siber hukuk, siber uzayı düzenlemeye yönelik kurallar olarak anlaşıldığında, bu yeni alan için yeni normların geliştirilmesi gerektiği vurgulanmaktadır. Bu noktada anti-tez yürütmek maksadıyla geleneksel hukukun siber uzayda çözüme kavuşturamadığı birtakım sorun alanlarının belirlenmesi gerekir. Bu noktada Akyeşilmen, bu alanları şu şekilde sıralamıştır:

1. Siber uzay soyut bir alan olduğundan onu geleneksel hukuk normlarıyla yönetmek ve düzenlemek oldukça zordur.

2. Siber uzay sınırsız bir alan olup hukukla çizilmiş sınırları dikkate almaz.
3. Siber, her saniye devasa bir trafiğe sahne olur. Saniyeler içinde milyonlarca e-posta, gönderiliyor.
4. Siber, üyelerine anonimlik için büyük bir potansiyel sunar.
5. Siber, daha önce görülmemiş ekonomik verimlilik sunar.
6. Elektronik bilgi siber suçun ana konusu haline gelmiştir.
7. Bir yazılım kaynak kodu, yayınlanmasından saatler içinde tüm dünyaya dağıtılabilir.
8. Kurumsal bilgilerin hırsızlığı geleneksel ceza hükümleri tarafından kolaylıkla karşılanabilir (2018, s. 87).

Değerlendirme yapılırken, ayrı bir sorun kümesi oluşturmak yerine, mevcut kümelere eklenen yeni sorunlara dikkat çekilmiştir. İlgili sorun alanları, internetten önce de var olan sorunlardır. Ancak internetle birlikte sorunların hızı, mahiyeti ve maliyeti büyük ölçüde değişmiştir. Yukarıda sıklıkla değinildiği gibi internetin benzersiz doğası, mevcut yasal ve politik araçların yeterliliğini sorgulatmıştır. Esasen internet yönetişimi sorunları, fiziksel alandaki sorunların birer zorlu tezahürüdür. Bu nedenle sorunların çözümü, uluslararası hukuk ve politikanın geleneksel kalıpları içinde pek mümkün gözükmemektedir (Sadowsky vd., 2004, s. 13).

Siber uzay, fiziksel alandan farklıdır ve farklı bir yönetişim biçimi gerektirir. Bu yaklaşımın etkisi, ICANN'in oluşturulmasında ve bu kuruluşun çalışma biçiminde göze çarpmaktadır. Siber hukuk destekçileri, yargı yetkisi, siber suçlar ve sözleşmelerle ilgili mevcut yasaların internete düzgün bir şekilde uygulanamayacağını ve yeni yasaların oluşturulması gerektiğini savunmaktadır (Kulesza, 2012, s. xii). Bütün bu çabalara rağmen devletler anlaşamadığından ya da çıkarları işbirliği konusunda uyuşmadığından uluslararası hukuk yaklaşımı hakimiyetini sürdürmektedir (Akyeşilmen, 2018a, s. 269).

3.4. Uluslararası Siber Hukuk Mümkün Mü?

Dünyadaki hukuk sistemlerinin tümüne baktığımızda, hepsinin temel motivasyonunun aynı olduğuna şahit oluyoruz: tehdit algısı. Uluslararası alanda baktığımızda savaş ve çatışma hukuku, insancıl hukuk, insan hakları hukuku gibi hukuk dalları bir şeyi koruma motivasyonuyla oluşturulmuştur. Örneğin savaş hukuku, devletlerin iki büyük dünya savaşından sonra birbirlerinden algıladıkları tehditten dolayı ortaya çıktı. Peki

daha önce devletler savaşmamış mıydı? Evet savaşmışlardı, fakat uluslararası sistemde yaşanan "değişim" böyle bir mekanizmaya duyulan ihtiyacı ortaya çıkardı. Benzer şekilde insan hakları hukuku, "insan"ın devletten algıladığı tehdidi minimize etmek için ortaya çıktı. Evet, tıpkı savaşlar gibi insan hakları ihlalleri de ilk çağlardan beri vardı. Ancak, yine 20. Yüzyılda ortaya çıkan o "koruma kültürü" insanı da bu sürecin bir parçası haline getirdi. Uluslararası sistemde "birey" görünür oldukça "insan"ı koruma mekanizmaları da buna paralel olarak artış gösterdi. Benzer durumlar ulusal hukuk mekanizmaları (medeni hukuk, ceza hukuku, idari hukuk vs.) için de geçerlidir.

İşte siber hukuk da tam olarak böyle bir motivasyonla ortaya çıktı. İnternet ortaya çıktı, ticarileşti, küreselleşti, bir tehdit unsuru oldu ve uluslararası sistemin yapısında birtakım dönüşümler meydana getirdi. Dolayısıyla "değişim" ve "tehdit" faktörleri buradaki tarihi misyonlarını da yerine getirmiş oldular. Ziyadesiyle kriminal bir alan için bütün paydaşları koruma motivasyonunun gerekliliği olarak siber hukuk ortaya çıktı.

Üstelik bu alan, her türlü manipülasyonun çok kolay bir şekilde yapılabileceği bir alan. Çünkü bu alanda, fiziksel alandaki anarşik yapılar hiper anarşik yapılarla sınanmaktadır. Bu alanda bilgisayar başında oturan veya elinde telefonu olan herkesin "bir suç makinesi" potansiyeli vardır. Bu da halihazırda fiziksel alandaki suçlular için düşük maliyetli, hızlı ve garantili bir alan açmaktadır. Bunun yanında, anonimlik unsuru alanı domine ettiğinden, kimlik tespiti de mümkün değildir. Bu noktada işleyen bir hukuk mekanizması zaruridir. "Etkin, kapsamlı, çok taraflı, bütüncül ve entegre bir ulusal ve bir küresel hukuk sistemine ihtiyaç vardır" (Akyeşilmen, 2018a, ss. 88-89). Bu bağlamda, siber güvenliği sağlamak için en etkili yol, tüm aktörlerin ve hizmet sağlayıcıların aynı temel prensiplere bağlı kalması ve tarafsız, çok paydaşlı bir küresel uygulama mekanizmasıyla hukukun üstünlüğünün korunmasıdır (Mihr, 2016, s. 329).

Görüldüğü üzere uluslararası siber hukukun oluşturulması noktasında bir çelişkiye yahut paradoksa dikkat çekmeye çalışıyoruz. Yani tehdit algılanan bu alanda siber hukukun oluşturulması ne kadar zorsa, eşit derecede de gerekli. Adeta alanın zorluğu, hukukun zorunluluğunu kamçılıyor. Alan, doğasından kaynaklanan zorlukları gösterdikçe, hukuka duyulan ihtiyaç bir o kadar artıyor. Çalışmanın bu kısmı, siber hukukun mümkün olup olmadığı sorusunu/sorununu zorluk-zorunluluk paradoksunda

cevaplamaya çalışırken; paydaşların perspektiflerini göz önünde bulundurarak olasılıklar üzerinden normatif bir değerlendirmede bulunacaktır.

3.4.1. Zorluklar

Bugün gelinen noktada tüm dünyanın entegre olduğu bu dijital manzaranın karmaşıklığı yönetilemez hale gelmiştir. Artan siber riskler, yeni teknolojilere yapılan yatırımları kısıtlamakta, önemli fırsatların kaçırılmasına neden olmakta ve küresel ölçekte ekonomik büyümeyi etkilemektedir (Keller, 2015). Geleneksel siyaset biçimleri ve yargı mekanizmaları siber uzayın dinamik doğasına uyum sağlamakta zorluk çekmektedir. Yasaların siber alana uygulanabilirliği değerlendirilirken temel sorun, yasaların geçerli olup olmadığından ziyade uygulanabilir olup olmaması ile ilgilidir. Zira yasaların nasıl sonuçlandığı veya nasıl uygulandığı sorusu daha önemlidir. Siber suçları minimize etme amacıyla kurulan Budapeşte Konvansiyonu gibi yapılanmalar, Batılı devletler tarafından hazırlanmış bir antlaşma olması ve gelişmekte olan ülkelerin neredeyse hiç katılım sağlamamış olması nedeniyle sayısız eleştiriyle karşı karşıya kalmaktadır (Goldsmith, 2010; Hildebrandt, 2020; Dixit, 2022). Bununla birlikte, anlaşmanın neredeyse yirmi yıllık olması nedeniyle, hükümlerinin yeni suçlarla başa çıkmak için çok eski olduğu da savunulmaktadır (Dominic, 2020). Dolayısıyla bu durum, geliştirilen mekanizmaların da işlevsiz olarak addedilmesine sebebiyet vermektedir.

Siber uzayın sınır tanımayan doğası, geleneksel hukuk uygulamalarının karşılaştığı zorlukları artırmaktadır. Siber alan, herhangi bir fiziksel sınır tanımayan geniş bir bölgeyi kapsar ve bu durum, devletlerin uygun davranış kuralları konusunda net yönlendirmelere ihtiyaç duyduğunu gösterir. Sosyal medya platformlarında, örneğin Facebook veya Twitter'da, bir ülkenin yasalarını ihlal eden içeriklerin yayımlanması, çeşitli soruları gündeme getirir. Almanya gibi bir ülkede yasaklanmış bir içeriğin başka bir ülkede serbestçe erişilebilir olması durumunda, bu içeriğin yönetimi nasıl ele alınmalıdır? Ayrıca, bir devlet, başka ülkelerde faaliyet gösteren şirketler ve kendi vatandaşlarının kişisel verilerine nasıl bir yaklaşım sergilemelidir?

Veriler ve siber faaliyetler, farklı yargı alanları arasında hızla hareket edebilme kapasitesine sahiptir. Veriler ve siber faaliyetlerin fiziksel sınırlardan bağımsız olması, bir siber suçun yerinin, suç işlendikten sonra bile değişebileceği anlamına gelir. Bu durum, suçun işlendiği yargı alanının belirlenmesini güçleştirir ve suçluların – hatta

suçun kendisinin – tespit edilmesini engeller. Diğer yandan, siber alanda, çok sayıda farklı aktörün bulunması, denetim kurumlarının yetki alanlarını belirsizleştirebilir ve bazı bölgelerin denetimsiz kalmasına yol açabilir (DCAF, 2019, s. 13-14).

Devletlerin düzenleyici müdahalelerinin etkinliği ile teknoloji şirketlerinin kendi kendini düzenleme kapasiteleri arasında kronikleşen bir tartışma söz konusu. Bu tartışma, özellikle büyük teknoloji firmalarının siber uzayı şekillendirmedeki rolünü ve devlet müdahalesinin bu süreçteki etkinliğini sorgular. Teknoloji şirketlerinin geniş etki alanı ve hızlı inovasyon kapasitesi, devlet düzenlemelerinin sınırlarını test ederken, bu şirketlerin kendi iç düzenlemelerini yapma eğilimleri, etkili bir denetim mekanizması olarak öne çıkmaktadır. Bu durum, düzenleyici çerçevelerin yeterliliği ve teknoloji şirketlerinin sorumluluklarının boyutu hakkında devam eden bir tartışmayı beslemektedir.

Diğer yandan, hükümetlerarası kuruluşlar, siber uzay ve internet kullanımı için uluslararası standartlar belirlemeyi amaçlasalar da, şimdiye kadar bunu başaramadılar. Bunun nedeni, devletlerin yetkilerinin ve yaptırım mekanizmalarının genellikle devlet sınırlarında sona ermesi ve insan haklarını koruma yetkilerinin tamamen devlet egemenliğine ve devletlere dayanmasıdır. Hükümetlerarası kuruluşlar ve uluslararası mahkemeler, insan haklarını uygulamak bir yana, korumak için genellikle yalnızca sınırlı önlem ve araçlara sahiptir.

Birbirine zıt bu kadar aktörün varlığı söz konusu iken de, internet üzerinde etkili yasal düzenlemeler yapılması oldukça zorlaşmaktadır. İlk olarak, siber uzaya özgü bir hukuk modelinin geliştirilmesi, hukukun uluslararası boyutta uygulanabilirliği sorununu beraberinde getirir. Siber uzayın sınırsız ve küresel doğası göz önünde bulundurulduğunda, farklı yargı alanlarındaki mevzuatlar arasında uyum sağlamak büyük bir zorluk teşkil eder. Ulusal düzeyde geliştirilen siber hukuk modelleri, diğer ülkelerin yasalarıyla çatışabilir ve bu da uygulamada tutarlılık ve etkinlik sorunlarına yol açar. Örneğin, Lessig'in (1999c) vurguladığı siber uzayın özgünlüğü, artık gündelik hayatımızın ayrılmaz bir parçası haline gelmiş durumda. Bu entegrasyon, siber uzayın "özel" bir alan olarak değerlendirilmesini zorlaştırmaktadır. Geleneksel hukukun dijital ortamın zorluklarına adapte olması gerektiği fikri, günümüzde daha çok “entegre etme” bağlamında anlaşılmaktadır. Yani siber uzay için bir hukuk mekanizması oluşturulması fikri gündeme geldiğinde dahi, esas anlaşılan geleneksel hukukun bu alana

uyarlanmasıdır. Örneğin, gizlilik ve veri koruma mevzuatları (GDPR gibi) hem online hem de fiziksel ortamlarda bireylerin haklarını koruma altına almak için geliştirilmiştir. Bu, siber uzay için özgü bir hukukun varlığından ziyade, mevcut hukukun genişletilmesi ve adapte edilmesi anlamına gelmektedir.

İkinci olarak, teknolojinin hızlı gelişimi, herhangi bir siber hukuk modelinin hızla eskimesine neden olabilir. Hukukun teknolojik yeniliklere ayak uydurması genellikle zaman alırken, siber alanın dinamik doğası göz önüne alındığında, bugün geçerli olan düzenlemeler yarın yetersiz kalabilir. Bu, siber hukukun sürekli bir güncelleme ve revizyon sürecine ihtiyaç duyacağının habercisidir, ki bu da hem yasama organları için hem de uygulayıcılar için büyük bir meydan okuma oluşturur. Yapay zekâ etiği ve metaverse gibi yeni sorunlar, yeni hukuki düzenlemeler gerektirecektir. Tıpkı bir bilgisayarın güncellenmediği takdirde verimli kullanılamaması gibi, güncellenmeyen bir hukuk mekanizması da verimsiz kalacaktır. Dolayısıyla siber hukukun teknolojik gelişmelerin hızına ayak uydurabilmesi için dinamik ve esnek bir yaklaşım gereklidir.

Üçüncü olarak, siber uzaya özgü bir hukuk modeli geliştirmenin, yasal düzenlemelerin teknik detaylara fazla odaklanmasına ve temel haklar ile özgürlüklerin göz ardı edilmesine yol açabileceği söylenebilir. Örneğin, yukarıda da değinilen güvenlikleştirme faaliyetlerinin bir gereği olarak, siber güvenlik önlemlerinin artırılması adı altında bireysel gizlilik haklarının ihlal edilmesi veya ifade özgürlüğünün kısıtlanması gibi sorunlar ortaya çıkabilir.

Sonuç olarak, siber uzaya özgü bir hukuk modeli geliştirilmesi gerekliliği, teorik olarak anlaşılabilirken, pratikte uygulanabilirlik ve esneklik ile ilgili ciddi zorluklar barındırmaktadır. Bu nedenle, siber hukukun geliştirilmesi, yalnızca yasal düzenlemelere odaklanmak yerine, birazdan "olasılıklar" başlığında değineceğimiz gibi uluslararası işbirliğinin esas alındığı gibi çok paydaşlı bir yaklaşımı gerektirmektedir.

3.4.2. Zorunluluklar

Uluslararası siber hukukun gelişmesinin önünde yukarıda ifade edilen çok sayıda zorluk olsa da, bu alana özgü bir hukuk mekanizmanın geliştirilmesi artık elzem değil, zorunludur. Nasıl ki siber tehditlerin artması siber güvenlik mekanizmasını ortaya çıkardıysa, o tehditlerin eyleme dönüşmüş hali (siber suçlar, siber terörizm, siber çatışmalar) de siber hukuk mekanizmasını zorunlu hale getirdi. Küresel doğası nedeniyle siber uzay, suçlulara farklı ülkelerde birden fazla kişiyi etkileme olanağı

sağlayabilir duruma geldi. Dolayısıyla bu durum, suçların soruşturulması noktasında küresel bir mekanizmaya ihtiyaç duyulduğunu göstermektedir. Yargı alanındaki sorunların çözümü konusunda devletler ve devlet dışı aktörlere ayrı ayrı sorumluluklar düşmektedir (Raymond, 2016a, s. 125). Bugün gelinen noktada tehdit algılanan alanlar ziyadesiyle çeşitlenmiştir. Bireylere, devletlere, şirketlere, kuruluşlara yapılan her bir saldırı tehdidin farklı bir boyutunu ortaya çıkardı. Fakat sonuç aynıydı: işleyen bir uluslararası siber hukuk mekanizması oluşturulmalıydı. Siber yönetişimin bütün paydaşlarını eşit derecede koruma görevini üstlenebilecek bir mekanizmanın varlığına duyulan ihtiyaç, alan yaygınlaştıkça daha fazla hissedilmektedir.

Siber hukuk, -dünyadaki e-belgelerin yasal olarak tanınmasını sağlar. Gerçekleştirilen faaliyet ve gerçekleştirildiği alan "sanal" iken; faaliyeti gerçekleştiren aktörler ve bağlı oldukları yasal mekanizma "gerçek"tir. Dolayısıyla siber uzaydaki her faaliyet, gerçek ve tüzel kişileri bağlamakta ve buna uygun yasal bir çerçeve sunulmaktadır. Ancak esas sorun, yasal çerçevenin sınırıdır. Eğer çerçeve ulusal ise, yalnızca ulusal sınırlar dahilinde işlev görecektir. Fakat siber uzay ulusal değildir. Dolayısıyla ulusal alanın sınırlarının ötesine geçen bir alan için uluslararası bir mekanizma şarttır.

Siber hukukun mümkün olup olmadığı sorusu şu sorunları da gündeme getirmektedir: Devlet, devlet kurumları ve karar alıcılar olmadan meşru bir internet yasasından söz edilebilir mi? Siber hukuk kurallarının belirlenmesinde hangi ilke ve kriterler dikkate alınmalıdır? Her şeyden önce, siber uzayla ilgili yapılan çalışmalarda dikkat edilmesi gereken en önemli husus, bu alanın ulus-devlet odaklı ve gelenekselci yaklaşımların çok uzağında olduğu gerçeğidir. Her şeyden önce şunu bilmek gerekir ki, siber alanı domine eden devletler değil, özel sektördür. Bugün internetin sağlayıcıları özel şirketlerdir. Bu durumda gelenekselci bir hukuk anlayışı da geçerli olmayacaktır. Uluslararası hukuku bu alana entegre etmek isteyen gelenekselcilerin şunu göz önünde bulundurması gerekir: "Uluslararası hukukun süje olarak kabul ettiği tek aktör devletlerdir". Bu durumda bu kadar aktörü bünyesinde barındıran bir alana uluslararası hukuku uygulamaya çalıştığımızda, diğer bütün aktörleri gözden çıkarmamız gerekir. Hem de siber uzayda gerçekleşen bunca zararlı faaliyet uluslararası iken ve bütün aktörleri etkileyebilecek mahiyette iken. Dolayısıyla bir hukuk mekanizması oluşturulmadan önce alanın doğasının iyi tanımlanması ve ona göre adımlar atılması gerekir.

Ancak yine de, siber uzaydaki sınır ötesi sorunların hiçbiri yeni olmadığından, eski mekanizmaların işlerliği üzerine düşünmek gerekir (Akyeşilmen, 2018a, s. 292). Geleneksel yargı mekanizmaları, siber uzay üzerinde etkisiz değildir. Bu mekanizmalar, siber faaliyetlerde birtakım caydırıcı unsurlar taşımakta ve faaliyetlere sınırlama getirebilmektedir. Çatışma, terörizm, casusluk gibi sorunlar her zaman var olmuştur. Yalnızca bugün gerçekleştikleri alan ve gerçekleştiren aktörler açısından bir değişim söz konusu.

Geleneksel yargı mekanizmaları, siber uzay üzerinde etkisiz değildir. Bu mekanizmalar, siber faaliyetlerde birtakım caydırıcı unsurlar taşımakta ve faaliyetlere sınırlama getirebilmektedir. Bunun yanında internet, devlet temelli hukukun otoritesinden bağımsız ve özgür bir alan olarak yükselmeye başlamıştır. Devletler bu konuda önlem amacıyla mahkemeleri yetkilendirerek interneti kendi coğrafi bölgeleriyle sınırlandırma yoluna gitmiştir. Bu noktada hukukçular, yeni ortaya çıkan "İnternet Yasası" gibi kavramları anlamaya çalışmışlardır. Hukukun öngörülebilirlik özelliğinden faydalanarak, internetin en azından “düzenlenebilir” olduğu kanaatine varmışlardır. Bununla birlikte, internetin ve küreselleşen güçlerin devlet egemenliğinin temeline nasıl meydan okuduğu açıklanamadığı için, hukukun siber alana uygulanması konusundaki ilerlemeler halen yeterli değildir.

Devletler, bu zorluğun altından kalkabilmek adına teknoloji ve özellikle küresel iletişimdeki gelişmeleri yakından izlemekte, kendi yasal düzenlemelerini yürürlüğe koymakta ve etkili politikalar geliştirmeye çalışmaktadır (Akdeniz, 2004, s. 2). Ancak devletlerin siber savaş ve siber saldırı terimlerinin tanımlanması noktasında da ortak bir paydada buluşamamaları bunun önünde engel teşkil etmektedir. Örneğin, Çin ve Rusya gibi büyük güçler, siber tehditleri bilgi güvenliği üzerinden değerlendirerek, dikkatlerini daha çok ihlal edilen içeriklere doğru yöneltmişlerdir. ABD ve Avrupa ülkeleri ise bu durumu siber güvenlik çerçevesinde ele alarak, ifade özgürlüğünü önemsediklerini dile getirmektedir (Bendiek, 2014, s. 14).

Uluslararası kuralların oluşturulmasında her ülkenin kendi önerileri olsa da, küresel düzenin sürdürülebilirliği için genel olarak kabul gören uluslararası kurallara ihtiyaç duyulduğu görülmektedir. Çin, WSIS ve IGF gibi platformlarda aktif bir rol oynayarak küresel mevzuat sürecini kolaylaştırma çabalarını hızlandırdı. Bu, Çin'in uluslararası internet yönetişimi konusunda etkili bir aktör olma arzusunu ve çabalarını gösterir.

ABD, temel kavram ve ilkeleri belirleyen Ulusal Siber Stratejiyi kabul etmiş ve siber uzayın yönetişiminde önemli bir adım olarak 2014 yılında ICANN'in yönetimini devretmiştir. Bu, ABD'nin siber uzaydaki yönetişim ve politikaları şekillendirme konusunda kendi yaklaşımını ve stratejisini uygulama niyetini gösterir (Murthy, 2014, s. 2307).

Bu bağlamda ulusal, bölgesel ve küresel hukuk mekanizmalarının birbiriyle bağlantılı olan yapılar olduğunu da belirtmemiz gerekir. Birini diğerinden ayrı düşünmek mümkün değil. Dolayısıyla işleyen bir siber hukukun ilk şartı, bu üç hukuk sistemi arasındaki koordinasyondur (Akyeşilmen, 2018a, s. 91). Etkin bir siber hukuk mekanizması, tıpkı yönetişim için gerekli olan unsurlara bağlıdır. Her şeyden önce bütün paydaşları bünyesinde barındırmalı ve hepsine alan tanımalıdır. Bu noktada en makul çözüm, siber alandaki ticari, siyasi, sosyal etkileşimlerin uluslararası düzeyde düzenlenmesidir.

3.4.3. Paydaşların Perspektifleri

İnternetin getirdiği öngörülemeyen sorunlar, ulusal ve uluslararası yasa yapıcıları zorlamaktadır. Bu tür sorunları gerek devlet gerekse de devlet-dışı aktörlerin üstlendikleri rollerden bağımsız düşünmek neredeyse olanaksızdır. Bu nedenle aktörlerin üstlendikleri roller ve bu rollerin işlevinin ne denli etkili olduğuma bakılmalıdır.

Aktörlerin çeşitliliğinden kaynaklı siyasi, ekonomik ve kültürel farklılıklar, siber hukukun oluşturulmasına dair sorunlar üzerinde uzlaşmaya varılmasını engellemektedir. Buna rağmen, her bir paydaş grubu, internetin gelişimine katkıda bulunacak yapıcı bir fikir geliştirme potansiyeline sahiptir. Aktörlerin çıkarları da uluslararası düzenlemenin önünde bir engel teşkil etse de çoğunlukla gerekli ve "olması gereken" bir unsur olduğu için çıkar odaklı yaklaşımlara alternatif argümanlar üretilmelidir. Bu alanda devlet dışı aktörlerin güçlendirilmiş rolü dikkate alındığında siber suçlar, siber casusluk ve siber terörizm gibi sorunların çözümü için uluslararası işbirliğine ihtiyaç vardır. Ancak aktörlerin büyük çoğunluğunun alana güvenlik odaklı yaklaşımı, sorunların kaynaklarından birini daha oluşturmaktadır.

Devletler siber alanda birbirleriyle rekabet halindedir. Ancak siber uzay, ulus-devletten başka her türlü yeni aktöre olanak tanır. Oysa devlet, geleneksel yaklaşımlar tarafından meşru ve yasa yapabilen tek aktör olarak addedilmiştir. Meşruiyet, karar alıcıların

hesap verme sorumluluğunun bir sonucu olarak doğmuştur. Max Weber'e göre devlet, meşru güç kullanımı tekelini elinde bulunduran mekanizmadır. Meşruiyet, hem usule hem de esasa ilişkin boyutlara sahiptir. Usul söz konusu olduğunda, devlet dışı bir aktörün yasa yapma sürecine dahil edilip edilmeyeceği sorunsalı gündeme gelir. Karar alıcılar, meşruiyetlerini desteklemek için siyasi ve mali hesap verebilirlik mekanizmalarını işaret ederler. Bu nedenle yasa yapma yetkisine sahip aktörler, eylemlerinin hesabını parlamentolar, mahkemeler veya diğer kamu denetim organları önünde vermek zorunda kalabilirler (Koukiadis, 2015).

Lawrence Lessig (1999a) ise, bir egemenin başkaları üzerinde ne tür iddialarda bulunabileceği ile siber uzay üzerinde ne tür iddialarda bulunabileceği sorunsalını birbirinden ayrı tutmaktadır. Lessig, burada fiziksel alan ile siber alan egemenliği arasında bir ayrıma gitmektedir. Peki uluslararası alanda yerleşmiş olan hukuki ve yasal düzenin siber alan üzerindeki yansıması ne şekilde olacaktır? Bir kritik nokta, uluslararası hukukun siber alanı düzenleme konusunda karşılaştığı zorlukların, fiziksel sınırların ötesinde bir etki alanı yaratmasıdır. Uluslararası hukuk, temelde egemen devletler arasındaki ilişkileri düzenlemeye yöneliktir ve bu yüzden, fiziksel sınırlarla tanımlanmış egemenlik kavramına dayanır. Ancak siber uzay, fiziksel sınırları aşan bir yapıya sahip olduğundan, geleneksel egemenlik kavramları bu yeni alana uygulandığında yetersiz kalır. Ayrıca, siber uzay üzerinde egemenlik iddialarının, uluslararası hukukta yerleşik olan egemen eşitlik ilkesi ve devletlerin iç işlerine karışmama ilkesi ile çatışma potansiyeli taşıdığı da eleştirilebilir. Devletlerin siber uzayda uyguladıkları yasal düzenlemeler, diğer devletlerin iç işlerine müdahale olarak algılanabilir ya da uluslararası hukukun temel prensiplerine aykırı düşebilir.

Keza bugün ABD, Çin ve Avrupa ülkeleri internet üzerinde çeşitli kontrol mekanizmaları inşa etmeye çalışmaktadır. ABD nispeten özgür ve açık bir modeli savunurken, Çin daha çok siyasi kontrol sağlayabileceği bir model öngörmektedir. Çin ve Rusya'nın desteklediği, uluslararası telekomünikasyona odaklanan ITU merkezli rejim, geniş kitlelerin bulunduğu anarşik siber uzayın eylemleri karşısında "küresel" niteliğini yitirmektedir. Bu bağlamda ortaya çıkan ICANN gibi yeni yönetişim mekanizmaları siber yönetişimde özel aktörlerin önemini ortaya koymaktadır (Levinson & Marzouki, 2015, s. 32).

Devletler, siber güvenlik hukukunun evriminde kritik bir dönemeçte bulunmaktadır. Normatif yaklaşımların artmasıyla birlikte uluslararası yasa yapım süreçlerindeki merkezi rollerini yeniden tanımlama fırsatına sahiptirler. Ancak, siber güvenlik alanının karmaşıklığı ve çok sayıda aktörün varlığı, bu sürecin ne hızlı ne de basit olacağını işaret etmektedir (Mačák, 2017, s. 25). Bugün gelinen noktada yargı yetkisinin kullanılmasına ilişkin geleneksel ilkeler öylesine değişime uğramıştır ki, farklı aktörler için yeni egemenlik ve yetki alanları açılmıştır. Ortaya çıkan bu yeni alanda hukukun uygulanması, karşılıklı etkileşimle mümkün olmuştur. Öyle ki bu aktörlerin etkileşimi işbirliğinin ötesine geçmiş, devletler bazı durumlarda devlet-dışı aktörleri yetkilendirmeye başlamıştır. Bu konuda UNGGE, 2013 tarihli raporunda devletlerin kullandıkları vekil aktörlere de atıf yapmıştır. Bu aktörlerin uluslararası hukuka aykırı eylemlerde bulunmak için kullanılmaması gerektiğine vurgu yapılmıştır (2013, s. 13). Bu durum, devletlerin alanı ulusal güvenlik ve çıkar odaklı bir yaklaşımla ele aldığını kanıtlar niteliktedir.

Hükümetlerarası kuruluşların da siber alana bakış açısı genellikle güvenlik odaklı olmuştur. Onlar da tıpkı ulus-devletler gibi güvenliği hukuku göz ardı eden bir yaklaşım benimsemiştir. Siber hukukla ilgili uluslararası çalışmalar yürüten önemli kurumlardan biri olan ITU dahi, yaptığı siber güvenlik tanımında hukuku ve insan haklarını göz ardı etmiş, bu alanlara herhangi bir referans vermemiştir. ITU, bu yaklaşımıyla siber alanı hukuk dışı bir alan olarak değerlendirmiştir (Akyeşilmen, 2018a, ss. 111-112).

Bu ana kadar BM, ASEAN, AB, AGİT, OAS veya Afrika Birliği gibi bölgesel veya uluslararası insan hakları rejimleri, küresel veri, fikri mülkiyet, gizli bilgi veya özel veri akışının sonuçları ve etkileriyle ancak kısmi olarak ilgilenmiştir. AB gibi bölgesel örgütlerin aldığı önlemler çoğunlukla kendi sınırları içindeki kullanıcıları kapsamaktadır. Bu önlemler küresel düzeyde genel geçerliğe sahip değildir. Benzer şekilde ABD ve Çin gibi ülkeler uzun süredir sınırsız veri akışını ya koruma ya da sınırlama amacıyla ortak bağlayıcı anlaşmalar yapılmasını önermektedir. Ancak bu konudaki teknik mücadele, uluslararası bir rejim anlayışının oluşturulması için yeterli değildir. Sorunların çözümü için BM gibi uluslararası rejimlerde yer alan birkaç devletin ötesinde, etkili kurumlara ihtiyaç duyulmaktadır. Teknik şirketler, internet sağlayıcıları ve arama motorları gibi daha geniş bir siber topluluk olmadan, etkili bir yaptırım mekanizmasının oluşturulması pek mümkün olmayacak

Dijital yönetişimin önemli bir aktörü olan özel sektör, uluslararası sözleşmeleri ve kuralları desteklemeye başlamıştır. Her yasa yapıcı gibi, siber uzaydaki zararlı faaliyetlere yaptırım uygulama ve verilen zararı giderme hakkını talep etmektedir (Kulesza, 2012, s. 31). Bu çerçevede Microsoft, Dijital Cenevre Sözleşmesi'ni önermiştir. Sözleşme; maddi kurallar, teknik ilkeler ve siber saldırıların atfı gibi pek çok sorunlu alana ışık tutmaktadır. Diğer yandan Google, devletlere dijital kanıtların sağlanması için yeni normlar önermektedir. Google'ın bu önerisi, devletlerin işini kolaylaştıracaktır. Zira bugün Google'ın menşei olduğu ABD'nin kolluk kuvvetleri, uluslararası işbirliği talep etmek için geleneksel diplomatik bir kanal olan Karşılıklı Adli Yardımlaşma Anlaşması'ndan (MLAT) geçmek zorundadır. Google'ın bu önerisi, devletlerin ikili anlaşmalar gerektiren MLAT olmadan da teknoloji şirketlerinden dijital kanıt talep etmelerine imkân tanıyacaktır (Kurbalija, 2017).

Teknoloji şirketlerinin menşeinde olan sosyal medya platformları da, şiddet içeren aşırılık ve terörizm gibi yasa dışı faaliyetlerin yayılması için önemli bir platform haline gelmiştir. Bu durum, devletlerin sosyal medya şirketlerinden, bu platformlarda barındırılan içeriği düzenlemesi için baskı yapmasına neden olmuştur. Bu baskıya yanıt olarak, sosyal medya şirketleri, hizmet şartları ve davranış kuralları geliştirerek kendi içerik düzenleme mekanizmalarını oluşturmuştur. Bu kurallar, farklı platformlar arasında farklılık göstermektedir. Örneğin, Facebook, nefret söylemi ve şiddet içeren içeriği yasaklarken, Twitter, bu tür içeriğin belirli durumlarda izin verilebilir olduğunu belirtmektedir (DCAF, 2019, ss. 19-20). Benzer şekilde YouTube'un "Tehlikeli ve Zararlı İçerikler" politikası, Instagram'ın "Topluluk İlkeleri" politikası terörle ilgili içeriklere karşı net bir tavır almaktadır.

Bu alanda çalışan akademisyenlerin de bakış açılarının uluslararası örgütler ve devletlerden daha farklı olduğunu söylemek zor. Zira literatür taraması kısmında da değinildiği üzere alanı domine eden çalışmaların büyük çoğunluğu, güvenlik odaklı bir yaklaşım sunmuş ve hukuk, insan hakları, etik gibi alanları göz ardı etmiştir. Yapılan çalışmalar genellikle siber uzayın teknik boyutunu, alandaki büyük güçlerin siyasetini yahut devletlerin güvenlik anlayışını konu edinmiştir.

3.4.4. Olasılıklar

Siber hukuk mümkün mü? sorusuna bu başlık altında verilecek cevap: evet, mümkün. Peki ama nasıl? Koh, hukukun siber uzaydaki faaliyetlerinin bir "deli gömleği" gibi

değil, aksine "bizi özgür kılan akıllıca kısıtlamalar" olarak görülmesi gerektiğinin altını çizmektedir. Koh'a göre hukuk, meşru eylemleri gerçekleştirmek için gerekli yetkiyi sağlar (2012, s. 11).

Hukuk ve teknoloji, birbirini tamamlayan güçlü yönlere sahip oldukları için düşman değil, müttefik olarak düşünülmelidir. Hukuk, teknolojinin adil ve sorumlu bir şekilde kullanılmasını sağlamaya yardımcı olabilirken; teknoloji ise hukukun daha verimli ve erişilebilir olmasını sağlayabilir (Schrepel & Buterin, 2020, s. 3). Hukuk, toplum düzenini ve adaleti sağlamanın temel aracıdır. Teknoloji ise yeni fırsatlar ve zorluklar yaratmaktadır. Bu nedenle, hukuk ve teknolojinin birlikte çalışarak bu fırsatları maksimize etmek ve zorlukları minimize etmek için bir yol bulmaları önemlidir.

Hukuk, teknolojinin getirdiği yeni riskler ve fırsatlar karşısında evrilmeli ve bu değişikliklere uyum sağlamalıdır. Örneğin, yapay zekâ kullanımının etik ve hukuki boyutları, hukukun belirleyici bir rol oynaması gereken önemli alanlardan biridir. Diğer yandan teknoloji, hukuki işlemleri daha etkin bir şekilde yürütme potansiyeline sahiptir. Örneğin, blok zinciri teknolojisi, sözleşmeler ve diğer hukuki dokümanların güvenli ve şeffaf bir şekilde saklanmasını mümkün kılarak, hukuki süreçlere katkıda bulunabilir.

Hukuk ve teknolojinin sinerjisi, daha adaletli ve sürdürülebilir bir toplum yaratma potansiyeline sahiptir. Bu nedenle, bu iki alanın nasıl entegre edilebileceği ve birlikte çalışabileceği üzerine odaklanmak önemlidir. Bu durum normatif teorinin dayanışmacılık ve çoğulculuk anlayışının küresel adalet üzerinde yarattığı etkiyi akıllara getirmektedir.[58] John Rawls, Halkların Hukuku (1999) adlı eserinde çoğulcu bir küresel adalet görüşünü savunur. Rawls'a göre, ulusları bölen siyasi, ekonomik ve kültürel farklılıklar, herkesin uluslararası düzen için makul bir temel olarak kabul edebileceği ilkelerle tutarlı olması koşuluyla hoş görülebilir.

Tamamen hukuki bir bakış açısıyla değerlendirildiğinde, devletlerin hâlâ uluslararası bir anlaşmaya bağlı olmamayı, egemenlik hakkı olarak seçme özgürlüğü vardır. Ancak uygulamada devletlerin bu egemenlik hakkını kullanması her zaman kolay değildir. Küreselleşen dünyada, devletler karşılıklı bağımlılıklar ve düzenleyici/işbirlikçi

[58] Dayanışmacılık, küresel adaleti tüm insanların temel ihtiyaçlarının karşılanması ve refahının sağlanması olarak tanımlar. Bu yaklaşım, uluslararası işbirliği ve dayanışma yoluyla küresel eşitsizliklerin azaltılmasına odaklanır. Çoğulculuk ise küresel adaleti, farklı kültürlerin ve siyasi sistemlerin barış içinde bir arada var olabilmesi olarak tanımlar. Bu yaklaşım, ulusların egemenliğine ve kendi siyasi sistemlerini seçme özgürlüğüne saygı gösterilmesine odaklanır (Nardin, 2022).

düzenlemeler ağlarıyla gittikçe daha fazla bağlantılı hale gelmektedir. Bu ağlar, devletlerin tek başına hareket etmesini zorlaştırır ve çoğu durumda uluslararası anlaşmalara uymayı teşvik eder. Devletler, resmi ve gayri resmi rejimler ağının bir parçası haline gelmiştir ve bu iç içe geçme hali, önümüzdeki yüzyılda da devam edecektir. Bu durum, geleneksel devlet egemenliği kavramını da etkilemektedir. Devletlerin eskiden sahip olduğu özerklik, artık bu ağların ve rejimlerin sınırlamalarıyla kısıtlanmıştır (Zacher, 1992, s. 60).

Siber uzaydaki bu yeni gerçeklik, uluslararası hukukun yeniden düşünülmesini ve siber faaliyetlerin özgün doğasına uygun yeni normlar ve prensipler geliştirilmesini zorunlu kılar. Geleneksel uluslararası hukuk modellerinin siber uzaya uygulanması, birçok alanda yetersiz kalmıştır. Örneğin, siber saldırılar ve siber savunma konularında meşru müdafaa hakkının yorumlanması, geleneksel hukuk çerçevesinde net bir şekilde tanımlanamamaktadır. Benzer şekilde, siber casusluk, fikri mülkiyet hırsızlığı ve kişisel verilerin korunması gibi konular, uluslararası hukukun mevcut yapısı içinde yeterince ele alınamamaktadır.

Uluslararası hukukun gelişimi, egemen devletlerin birbirleriyle etkileşim kurdukları sınırlı alanlardan, giderek daha karmaşık ve işbirliğine dayalı bir uluslararası düzenin gerekliliklerini karşılamaya doğru evrilmiştir. Bu evrim, özellikle İkinci Dünya Savaşı'nın ardından, devletler arası ilişkilerde derin değişikliklere yol açmıştır. Küreselleşmenin etkisiyle, uluslararası örgütlerin sayısı artmış ve devletler, egemenlik yetkilerinin belirli unsurlarını uluslararası kurumlara devretmeye daha açık hale gelmiştir. Bu durum, hem ekonomik hem de siyasi alanda bölgesel ve uluslararası düzeyde karşılıklı bağımlılığı artırmış, aynı zamanda farklı ticaret blokları arasında rekabeti de körüklemiştir (Shaw, t.y.).

Uluslararası hukukun yetersiz kaldığı alanda siber hukukun mümkün kılınması, mevcut uluslararası hukukun sınırlarını aşarak, siber uzayın karmaşık doğası ve çeşitlilik gösteren aktörleriyle başa çıkacak yeni mekanizmaların ve düzenlemelerin oluşturulmasını gerektirir. Bu yeni çerçeve, devletlerin yanı sıra özel sektör, sivil toplum ve uluslararası örgütleri de içerecek şekilde genişletilmiş bir aktör yelpazesini

kabul etmelidir.[59] Aşağıda, siber hukukun nasıl mümkün olabileceğine dair çeşitli olasılıklar ve bu sürecin üstesinden gelinmesi gereken temel sorunlar tartışılmaktadır:

Çok paydaşlı işbirliği: Yukarıda işbirliğini "zorluk" kategorisinde değerlendirmiştik. Fakat siber hukukun temeli, tüm paydaşların dahil olduğu çok paydaşlı işbirliği modeli olmalıdır. Kuralların uygulanması ve denetimi, çok uluslu şirketlerden sivil toplum kuruluşlarına, devlet organlarından bireylere kadar geniş bir yelpazeyi içeren, geleneksel olmayan bir kuruluşun üstlenmesi gereken bir role işaret eder (Murthy, 2014, s. 2307). Bu işbirliği, siber uzayın yönetişimi, siber güvenlik, veri koruma, siber suçlar ve siber savaş gibi konularda ortak standartlar ve politikalar geliştirmeyi hedeflemelidir. Örneğin, BM bünyesinde siber güvenlikle ilgili uluslararası bir konvansiyon, devletlerin yanı sıra büyük teknoloji şirketlerinin ve diğer ilgili tarafların katılımıyla mümkün olabilir. Bu tür bir konvansiyon, siber suçlarla mücadelede uluslararası işbirliğini güçlendirebilir ve siber savaşın önlenmesine yönelik kurallar koyma potansiyeline sahiptir. Özellikle siber suçlar sınır tanımadığı için, uluslararası adli işbirliği, siber hukukun uygulanmasında hayati öneme sahiptir. Keza BM bunun farkına vardığından, buna yönelik girişimleri zaten başlatmıştır.[60] Bu durumda mühim olan, farklı yargı bölgeleri arasında suçların ve suçluların tespiti için işbirliği mekanizmalarının güçlendirilmesidir. Böylesi bir koordinasyon, siber suçlara karşı etkili bir mücadele sağlayabilir ve siber uzayda hukukun üstünlüğünün desteklenmesine yardımcı olabilir. Bu, hem bölgesel hem de küresel düzeyde, ortak eylem planlarının geliştirilmesine kadar genişleyebilir ve siber tehditlere karşı ortak yanıtların oluşturulmasını sağlayabilir.

Esnek ve Dinamik Yaklaşım: Dijitalleşme, politika yapımında kilit bir role sahiptir ve bu alandaki herhangi bir gelişme, toplum üzerinde derin etkiler yaratabilmektedir. Bu bağlamda siber uzay, gerçek dünyadan tamamen bağımsız bir alan olarak görülmemelidir; aksine, günlük yaşamımızın ve sosyal etkileşimlerimizin bir uzantısı olarak anlaşılmalıdır (Lahmann vd., 2017, s. 15). Bu nedenle siber uzayın doğasından kaynaklanan zorlukları aşmak için, siber hukukun esnek ve dinamik bir yaklaşım

[59] Devlet-dışı aktörlerin olası bir hukuk sisteminde nasıl yer bulacağına dair olasılıklar, özellikle çalışmanın dördüncü bölümünde geniş bir şekilde tartışılmıştır. Devlet-dışı aktörlerin uluslararası hukuk sisteminde artan rollerine ve meşruiyetlerine dair analizler, IGF bağlamında değerlendirilmiştir.

[60] Ayrıntılı bilgi için bkz: UN. (2021, June 29). *Draft: United Nations Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes*. https://www.unodc.org/documents/Cybercrime/AdHocCommittee/Comments/RF_28_July_2021_-_E.pdf

benimsemesi gerekmektedir. Bu yaklaşım, siber uzaydaki hızlı değişimlere proaktif yanıtlar geliştirebilir ve uzun vadede siber hukukun etkinliğini artırabilir.

Geliştirilmiş Diyalog Kültürü: Küresel internet yönetişimi, sadece teknolojik ve ekonomik değil, aynı zamanda sosyal ve etik boyutları da içeren karmaşık bir yapıya sahiptir. Bu nedenle, tüm paydaşların eşit katılımı, internetin demokratik, şeffaf ve adil bir şekilde yönetilmesi için elzemdir. Bunun gerçekleşebilmesi için kazanılması gereken değer, diyalog kültürünün geliştirilmesidir. Bu durum, küresel internet yönetişimindeki temel bir prensibi ortaya koyar: Hiçbir paydaşın dışlanmaması gerekliliği. Bu konuda sayısız örnek vardır. Ancak bu örnekler genellikle devletlerin diğer aktörleri dışladığı durumlara atıfta bulunur. Oysa mevcut durumda işbirliğinden ve diyalogdan kaçınan yalnızca devletler değildir. Özellikle özel sektör ve teknik topluluğun temsilcileri, devletleri ve diğer aktörleri dışlayıcı davranabilmektedir. Buna örnek olarak, Norveç Net Mahkemesi'nin (Nettnemnda) kuruluş süreci verilebilir. 2001 yılı başlarında Norveç, BİT sektörünün desteğiyle, Norveç Net Mahkemesi'nin (Nettnemnda) kurulması kararını aldı. Bu öncü girişim, "İnternet için Etik Kurallar" ilkesini benimseyen ve ilgili anlaşmazlıkları çözmek için bir prosedür sunan dünya çapında ilk program olarak dikkat çekti. Ancak, yerel BİT endüstrisinin kendi kendini düzenleme kapasitesine olan inancı ve devlet müdahalesine karşı çıkışı nedeniyle bu program hayata geçirilemedi (Bygrave & Michaelsen, 2009, ss. 119-120). Bu örnekte görüleceği üzere herhangi bir paydaşın süreçten dışlanması, diğer paydaşların – etik ve normatif bir güdüyle dahi olsa – çabalarının da sonuçsuz kalmasına sebebiyet verecektir.

Siber/Dijital Diplomasi: Bu her ne kadar yalnızca devlet aktörünü içeren bir madde olsa da, siber diplomasi, devletler arasındaki siber güvenlik konularında anlayış ve işbirliğini teşvik eden bir araç olduğundan, hukuk mekanizması üzerinde büyük bir etki yaratabilir. Özellikle güven artırıcı önlemler bağlamında siber uzaydaki gerilimleri azaltmaya ve potansiyel çatışmaları önlemeye yönelik olarak devletlerin niyetlerini ve faaliyetlerini şeffaflaştırabilir. Bu önlemler, özellikle kriz durumlarında iletişim kanallarının açık tutulmasını içerebilir. Böylece, siber suçlardaki atıf ve anonimlik gibi sorunlar minimize edilebilir ve bu durum karşılıklı güvenin inşa edilmesine yardımcı olabilir. Örneğin ABD'nin siber uzayla ilgili yaklaşımı, siber çatışma sorunlarını içeren "akıllı güç" stratejisinin bir parçasıdır. ABD için uluslararası hukuka uymak, daha geniş bir "akıllı güç" yaklaşımının bir parçası olarak görülmektedir. Bu, yalnızca askeri güçle

değil, aynı zamanda diplomatik, ekonomik ve hukuki araçlarla birlikte etkili bir strateji yürütmeyi içerir. Bu yöntemle ABD, diplomasi alanında, uluslararası hukuka uyumu teşvik etmek için birtakım girişimlerde bulunmaktadır (Koh, 2012, s. 10-12).

Teknoloji Tarafsızlığı[61] ve Uyumluluk: Lessig'e göre "siber uzayın düzenlenip düzenlenemeyeceği mimarisine bağlıdır". Devletler, siber uzayı düzenlemek istiyorlarsa, internetin tasarımını değiştirmek için adımlar atmalıdırlar (1999a, s. 17). Böylesi bir değişim gerekli olmasa da, en azından gelişen yeni teknolojiler için uyumlu mekanizmalar oluşturulabilir. Zira yeni bir teknoloji ortaya çıktığında, mevcut yasal çerçevelerin bu teknolojiye nasıl uygulanacağı konusunda belirsizlikler oluşabilir (Greenberg, 2016, s. 1537). Bu nedenle siber hukukun etkili bir şekilde uygulanabilmesi için, teknolojiye özgü düzenlemelerin yanında, teknoloji tarafsızlığına dayalı bir yaklaşım benimsemek de önemlidir. Bu bağlamda, teknoloji tarafsızlığını esas alan bir yaklaşım benimsemek, yasaların zaman içinde geçerliliğini yitirmesini engelleyebilir. Teknolojiye özgü düzenlemeler kadar, teknolojinin özünü anlayıp, ona göre hareket eden yasalar, hızla gelişen bir çağda daha uzun ömürlü olabilir. Ayrıca, bu tür bir yaklaşım, uluslararası alanda farklı teknolojik standartlar ve uygulamalar arasında bir uyum sağlayarak, siber uzayın küresel işlevselliğini artırabilir. Neticede siber hukukun oluşturulması ve uygulanması, sadece bugünün teknolojilerini ve tehditlerini değil, yarının teknolojilerini ve beraberlerinde getirecekleri güvenlik zorluklarını da göz önünde bulundurmalıdır. Kısacası teknolojinin getirdiği potansiyeller kadar, oluşturabileceği riskler de dikkate alınmalıdır.

Eğitim ve Farkındalık: İnternet, hukukun da evrim geçirmesi gerektiğini göstermiştir. Murthy'nin de işaret ettiği gibi, eski hukuk kurallarının birçoğu artık güncelliğini yitirmiş durumda (2014, s. 2307). Ancak bu, sadece yasaların değişmesi gerektiği anlamına gelmez; aynı zamanda internetin nasıl işlediğinin de doğru şekilde anlaşılmasını gerektirir. Asıl mesele, devlet yetkililerinin, özel sektör temsilcilerinin ve tüm toplumun siber güvenlik konusunda eğitilmesi ve bilinçlendirilmesidir. İnsanlar ve kurumlar, siber tehditlerin farkında olmalı ve nasıl korunacaklarını bilmelidir. Bu noktada, eğitim programları ve farkındalık kampanyaları devreye girer. Bu tür programlar, siber tehditlere karşı korunma yöntemlerini, veri koruma ilkelerini ve siber

[61] Teknoloji tarafsızlığı, telif hakkı yasalarında önemli bir ilkedir. Bu ilke, yasal düzenlemelerin belirli bir teknolojiye özel olmaması, fakat genel prensiplere dayanması gerektiğini savunur. Bu sayede, yeni teknolojilerin ortaya çıkmasıyla birlikte yasalarda sürekli değişiklik yapma ihtiyacı ortadan kalkar ve yasal düzenlemelerin uzun ömürlü olması sağlanır.

etik konularını kapsamlı bir şekilde ele alabilir. Böyle bir bilgilendirme süreci, sadece bireylerin ve kurumların siber tehditlere karşı daha bilinçli ve hazırlıklı olmasını sağlamakla kalmaz, aynı zamanda siber uzayda daha sorumlu davranışları teşvik eder. Sonuçta her birey, siber uzayın bir parçasıdır ve güvenliği sağlamak için her birine ayrı roller düşmektedir. Özellikle dijital vatandaşlık projeleriyle bireylerden kurumlara kadar yerleştirilen bir bilinç kültürü, zamanla küresel çaplı bir yargı sisteminin önünü açabilir.

Hesap Verebilirlik: İnternet yönetişimi ile ilgili karar vericiler, kararlardan etkilenenlere karşı hesap verebilir olmalıdır. İnternette uluslararası hukuk normları ve insan hakları geçerlidir. Devletler ve istihbarat örgütleri de dahil olmak üzere interneti kullanan tüm aktörler, yasalara ve insan haklarına saygılı olmakla yükümlüdür (UNCTAD, 2015, s. 7). Uluslararası insan hakları normlarının internet ile ilgili olanlarla uyumlaştırılması ve yeniden teyit edilmesi gerekir. Zira bu haklar fiziksel alandaki haklara benzer tehditlere maruz kalmaktadır. Filtreleme teknolojileri halen gelişme aşamasında olsa da potansiyel olarak ifade özgürlüğünü ve internetin şeffaflığını tehdit edebilecek boyutlara varmıştır (Mansell, 2004, s. 6). Bu nedenle devletlerin siber suç ve terörizm faaliyetlerine karşı koymak için uyguladıkları yasal önlemler, hukukun üstünlüğünü ve insan haklarını korumalı, ifade özgürlüğüne öncelik vermelidir. İnternet erişimine getirilebilecek sınırlamalar, diğer ifade ve iletişim biçimlerine uygulanan sınırlamalar gibi katı koşullar altında olmalıdır. Örneğin, internet erişimi, millî güvenliği veya kamu düzenini korumak için sınırlandırılabilir. Ancak bu sınırlamalar, ifade özgürlüğünü ve bilgi edinme özgürlüğünü ihlal etmemelidir (Lucchi, 2014, s. 854). Aynı zamanda, bu süreçlerin şeffaflığı ve hesap verebilirliği temel alınarak gerçekleştirilmesi gerekmektedir (IGF Summary Report, 2023). Zira günümüzde devlet dışı aktörlerin, devletlerden beklenenlere benzer şekilde kendi örgütlerinde hesap verebilirlik mekanizmalarına sahip olmamaları, günümüzde önemli bir sorundur. Bu durum, özellikle BM gibi uluslararası kuruluşların geçici yönetimleri söz konusu olduğunda daha da belirgin hale gelir (Banks, 2003, s. 297). Siber hukukun etkin bir şekilde işlemesi için, siber uzayda faaliyet gösteren tüm aktörlerin sorumluluk ve hesap verebilirlik ilkelerine uyması gerekmektedir.

Değerlendirme

Bu bölüm, küresel bir siber hukuk mekanizmasının oluşturulup oluşturulamayacağı sorusuna yanıt aramıştır. Siber uzayın fiziksel alandan çok daha karmaşık yapısının, uluslararası hukuk mekanizmalarının bu yeni alanı düzenlemede karşılaştığı zorlukları artırdığı görülmüştür. Bu karmaşıklık, fiziksel dünyada bile uluslararası hukukun pek çok noktada işlevsiz kalmasının ötesinde bir meydan okumayı temsil etmektedir. Bu çerçevede, siber uzay için etkili bir hukuk mekanizmasının mümkünlüğü, siber normların ve düzenlemelerin küresel ve bölgesel mekanizmalar tarafından nasıl şekillendirildiği ve en önemli engellerden biri olarak görülen paydaşların işbirliği eksikliği üzerine yoğunlaşmıştır.

Ayrıca, siber hukukun niteliğine dair farklı yaklaşımlar ve uluslararası hukukun siber uzaya uygulanabilirliği geniş bir şekilde tartışılmıştır. Bu tartışma, genel literatürde bu konunun nispeten az işlenmesine rağmen, mevcut ve somut bir mekanizmanın işlerliğinin ve alternatif bakış açılarının önemini vurgulamaktadır. Geleneksel uluslararası hukukun, siber uzaydaki yeni savaş ve çatışma anlayışına uyum sağlama kapasitesi sorgulanırken, siber alan için spesifik yeni bir hukuk mekanizmasının gerekli olup olmadığı veya bu alana özgü bir uluslararası siber hukukun mümkünlüğü üzerine değerlendirmeler yapılmıştır. Bu bağlamda siber hukuk mekanizmasının oluşturulması ve işleyişinin karmaşık doğası üzerine kapsamlı bir analiz sunulmaktadır. Siber uzayın benzersiz zorlukları ve uluslararası hukukun bu alana uygulanabilirliğinin mümkün olup olmadığı konusundaki sorular, normatif bir bakış açısıyla ele alınmıştır.

Siber yönetişimle ilişkili mevcut sorunların çözümünde küresel işbirliği ortamının oluşturulamamış olması, siber uzayın karmaşık doğasının ve küresel etkileşimin gerektirdiği tutarlı işbirliği ve koordinasyon mekanizmalarının eksikliğinden kaynaklanmaktadır. İnternetin kötüye kullanımını önlemek ve siber uzayın istikrarını sağlamak adına oluşturulacak uluslararası yasal çerçeveler ve koordinasyon mekanizmaları büyük önem taşımaktadır. Bu bağlamda, çeşitli uluslararası girişimlerin varlığına rağmen, siber suçlarla mücadelede bölgesel ve özel çıkar gruplarının öne çıkması, uluslararası veya hükümetlerarası bir kuruluşun özel sorumluluğu altında birleşen bir çabanın eksikliğini yansıtmaktadır. Yasal bir sistemin yokluğu, devletlerin hukukun üstünlüğü ve insan hakları gibi temel ilkeleri göz ardı ederek güvenlik odaklı

yaklaşımlar benimsemesine yol açmaktadır. Bu eğilim, siber hukuk mekanizmalarının zayıflamasına sebebiyet vermektedir.

Siber hukukun ve normların yükselişi, küresel ve bölgesel mekanizmaların çerçevesi içinde ele alındığında, bu alanın hala gelişmekte olduğu ve karşı karşıya olduğu zorlukları aşmak için uluslararası işbirliğinin ve koordinasyonun artırılmasının gerekli olduğu açıktır. Şu ana kadar, siber tehditlere yönelik her şeyi kapsayan bir uluslararası hukuk anlaşması veya bu alanda uluslararası teamül hukukunun temelini atacak bir devletlerarası anlaşmanın olmaması, siber güvenlik alanında bir boşluk yaratmaktadır. Buna karşın, siber uzay operasyonlarına uluslararası hukukun uygulanabilirliği konusunda genel bir devlet görüşünün kabul görmesi ve BM'nin siber güvenliği küresel bir mesele olarak ele alması, önemli adımlar olarak öne çıkmaktadır.

Bölgesel mekanizmaların varlığı ve çeşitliliği, siber hukukun bu düzeyde önemli bir dinamizm kazandığını göstermektedir. Özellikle, Budapeşte Siber Suç Sözleşmesi gibi geniş katılımlı anlaşmalar, sınır ötesi bilgi paylaşımı ve işbirliği konusunda önemli bir temel oluşturmaktadır. Bu anlaşma ve benzer bölgesel girişimler, siber suçlarla mücadelede devletler arası işbirliğini ve yasal uyumu teşvik ederek, siber güvenlik konusunda somut adımların atılmasına olanak tanımaktadır.

Siber hukuka yönelik çeşitli yaklaşımlar, uluslararası ve ulusal düzeyde, öz-düzenleme ve uluslararası siber hukuk kapsamında incelenmiştir, her biri siber uzayın yönetişimindeki zorlukları ve potansiyel çözüm yollarını ortaya koymaktadır. Tüm yaklaşımların incelenmesi sonucunda "Uluslararası Siber Hukuk" olarak adlandırılabilecek yeni, uluslararası ve disiplinler arası bir hukuk dalının temellerinin atılmasına yönelik bir ihtiyacın olduğu sonucuna varılmıştır. Zira "Bu alan, küresel ağın teknik yapısıyla yakından ilgili olan, hukukun tüm dallarıyla örtüşen hem ulusal hem de uluslarüstü çabaları birleştiren alandır" (Kulesza, 2012, s. x). Bu, yeni hukuk dalının biçimine ilişkin tüm tartışmanın temelini bütün tezin konusunu oluşturan "yönetişim" kavramı oluşturur. Alanda yönetişim çalışmalarının başlaması, hukuki boyutunu da görünür kılmış ve bu iki alanı iç içe geçirmiştir.

Bütün bu zorluklar/zorunluluklar/olasılıklar göz önünde bulundurulduğunda, siber hukukun oluşturulamamasının en büyük nedeni -bir yargı mekanizması oluşturması açısından- fiziksel alana oranla dezavantajlara sahip olmasıdır. Doğasından kaynaklanan zorluklar yargı mekanizmasının önündeki en büyük engeli teşkil etse de,

işbirliğinden kaçınan aktörlerin varlığı da azımsanmayacak derecede baltalayıcı bir unsur görevi görmektedir. Zira fiziksel alanda uluslararası örgütler, uluslararası hukuk gibi yapılanmalar olduğundan bunlar düzenleyici görevi görebilmekte. Ancak henüz siber alanda böyle bir düzenleyici mekanizma da mevcut değil. Ve fakat, dinamik ve hızla değişen bir alana hukukun entegre edilmesi elbette zor, ancak mümkün. Fakat bu durumda hukukun da kendini -siber uzay kadar olmasa da- değişimlere paralel olarak güncellemesi beklenir. Neticede diğer hukuk dallarının da yıllar içerisinde gelişim gösterdiği veya yeni alt dallara ayrıldığı görülmektedir. Siber hukuk da zaman içinde "metaverse hukuku", "yapay zekâ hukuku" gibi alt dalları bünyesinde barındırabilir, ancak netice itibariyle hepsinin kaynağı "siber" olduğundan kapsayıcı ve bütüncül bir hukuk dalı olarak kalacaktır.

BÖLÜM IV: YÖNETİŞİM MODELLERİ

Bu bölümde, internet yönetişimi modelleri ele alınacaktır. İlk olarak, öz-düzenleme modeli üzerinden, internetin özerk düzenlenme kapasitesi ve bu süreçte teknik toplulukların üstlendiği kritik roller incelenecektir. Ardından, ulusal model bağlamında devletlerin siber alan üzerindeki egemenlik talepleri ve bu yaklaşımın potansiyel kısıtlamaları tartışılacaktır. Daha sonra, çok paydaşlılık modeli kapsamında, özgürlükçü yaklaşımlar ve ICANN gibi kurumların rolü detaylandırılacak, bu modelin karşı karşıya kaldığı zorluklar ve sorun alanları ele alınacaktır. Çok taraflılık modeline geçildiğinde, ITU'nun rolü ve egemenlikçi modelin karakteristik özellikleri değerlendirilecektir. Alternatif yaklaşımlar bağlamında, Joseph Nye tarafından öne sürülen Rejim Kompleksi Modeli'nin mevcut modeller arasındaki dengeyi ve çeşitliliği nasıl sağlayabileceği incelenecektir. Son olarak ise, bu çalışma tarafından önerilen model olan IGF'nin yapısal özellikleri, işlevleri, katkıları ve toplantılarına dair detaylı bir analiz sunulacak, ayrıca forumun karşılaştığı yapısal ve paydaşlarla ilgili sorunlar incelenecektir. Nihai olarak, IGF'nin hukuki bağlayıcılığının mümkün olup olmadığı, bu bağlayıcılığın olası sorunları ve hukuki çerçevedeki olasılıklar ışığında normatif çözüm önerileri üzerinde durulacaktır. Dolayısıyla bu bölüm, küresel internet yönetişiminin kompleks yapısını aydınlatan bir modelin sorun alanlarını gidermeye yönelik normatif çözümler önermeyi hedeflemektedir.

4.1.İnternet Yönetişimi Modelleri

Yönetişime dair ilk büyük "çatışma alanı", 1998 yılında ITU tarafından başlatılan ve BM Genel Kurulu Kararı 58/83 ile yetkilendirilen WSIS idi (UNGA, 2002). Çalışmada sıklıkla atıfta bulunulan bu Zirve'de devletler, ITU üzerinde devletlerin egemenliğinin güçlendirilmesi ve devlet odaklı yeni bir oluşumun yaratılması şeklinde taleplerde bulunmuş ve bu doğrultuda oluşturulacak bir internet anlaşması hazırlığı yapmışlardır (Fidler, 2013b, s. 843). WSIS'in amacı, bilgi ve iletişim teknolojilerinin gelişimine odaklanmaktı. Burada Güney Afrika, Çin ve Brezilya gibi ülkeler, internet yönetişim düzenlemeleri üzerinde var olan ABD hakimiyetinden rahatsızlıklarını dile getirmişlerdir. Özellikle ICANN için kullanmış oldukları "ABD hükümetinin tek taraflı bir oluşumu" ibaresi, WSIS'i bu memnuniyetsizliğin dile getirilmesinde bir çıkış noktası haline getirmişti (Mueller vd., 2007). Bu devletler, daha geleneksel bir

hükümetlerarası modele duyulan ihtiyaca vurgu yapmaktaydı. Onlara göre ulusal egemenler, mevcut düzenlemeleri onaylama ya da değiştirme konusundaki çok taraflı kararlarda başarısız olmuşlardır. Bu devletlerin karşısında yer alan ICANN, ISOC ve ABD hükümeti; ICANN'in, WIPO anlaşmalarının ve IETF'nin yürüttüğü yönetişim mekanizmalarının amaca uygun olduğunu ifade ederek bu eleştiri ve talepleri küçümsemişlerdir. Bunun üzerine WSIS'in Cenevre'de gerçekleştirilen aşaması, WGIG'in oluşturulmasını zorunlu kılmıştır (Mueller, vd., 2007).

WSIS'in ikinci aşaması olarak bilinen Tunus Gündemi, devletlerin alan adları, IP adresleri, internet protokolleri ve kök sunucuları gibi kritik internet kaynaklarının yönetimi üzerinde bir anlaşmaya varmasını öngörüyordu. Aynı zamanda burada ICANN, hükümetlerarası internet rejimi modeline dönüştürülmeye çalışılmıştır (Kleinwächter, 2013). Benzer şekilde resmî sonuç belgesi olan Tunus Gündemi, ICANN rejimini değiştirmeyi hedeflemekteydi. Sonuç belgesinde yalnızca ABD'nin değil, tüm devletlerin DNS kökü ve internet kamu politikası gözetimi üzerinde eşit rol ve sorumluluğa sahip olması gerektiği belirtilmiştir (Mueller, vd., 2007). Ancak Tunus Gündemi, belirlediği ilkelerin benimsenmesi ve gerekli mekanizmaların inşası konusunda başarılı olamamıştır[62] (Mueller, vd., 2007).

WSIS'i takip eden bir dönemde, 2006 yılında, dönemin yükselen güçleri Brezilya, Rusya, Hindistan ve Çin tarafından kurulan BRIC'in[63] pek çok konuda olduğu gibi siber uzayda da ABD'ye meydan okuduğu iddia edilmiştir. Ebert ve Maurer, bu durumu ABD'nin siber uzaydaki hakimiyetine karşı "uyumlu bir hegemonik karşı hareket" olarak nitelendirmiştir (2013, s. 1055). BRICS ülkeleri ortak bir siber politika oluşturmaya yönelik adımlar atsalar da bu konudaki öncelikleri farklılaşmış ve bu nedenle genel bir yaklaşım oluşturulamamıştır. Bir taraf, uluslararası işbirliğine dayalı hükümetlerarası yaklaşımı tercih ederken, diğer taraf egemenlikçi bir siber politika benimsemeyi tercih etmiştir. Bu farklılıkların en önemli göstergesi olarak, BRICS'in bilgi güvenliğine dair herhangi bir ortak önerisinin veya bir internet yönetişimi organının bulunmaması gösterilebilir. Şimdiye kadar Hindistan, Brezilya ve Güney Afrika'nın işbirliğiyle 2003 yılında Brezilya Bildirgesi'ni ortaya koyan IBSA

[62] Her iki zirve de ICANN üzerinde herhangi bir değişim sağlayamamış olsa da küresel internet yönetişimi için bir çerçeve oluşturma konusunda katkıda bulunmuştur Buradan çıkan en önemli somut sonuç, tartışmanın sürdürülmesi için bir mekanizma görevi gören IGF'nin oluşturulmasıydı (Mueller, vd., 2007).

[63] 2011 yılında Güney Afrika'nın katılımıyla birlikte BRICS adını almıştır.

Koalisyonu, resmi öneriler sunmuştur. Diğer yandan 2011 ve 2015'te ŞİÖ, Bilgi Toplumu Davranış Kuralları'nı BM Genel Kurulu'na sunmuştur (Ebert & Maurer, 2013, s. 1055).

İnternet yönetişimiyle ilgili uluslararası alanda gerçekleşen bir diğer önemli faaliyet, 1988 tarihli Uluslararası Telekomünikasyon Düzenlemeleri'ni (ITR's) gözden geçirmek için 2012 yılında Dubai'de düzenlenen Dünya Uluslararası Telekomünikasyon Konferansı olmuştur. Ancak bu konferans, genellikle internet yönetişimi adına bir "fiyasko" olarak adlandırılmaktadır. Zira burada yaşanan anlaşmazlığın ardından iki yıl boyunca gerçekleştirilen bütün toplantılarda tartışmalar çok daha keskin olmuştur. 2013'te Bali'de sekiz ayrı IGF konferansı düzenlenmiştir. 2014 ise, Güney Kore'nin Busan kentinde düzenlenen Uluslararası Telekomünikasyon Birliği Tam Yetkili Temsilciler Konferansı da dahil olmak üzere her düzeyde bir "toplantılar yılı" olarak tanımlanmıştır (Kleinwächter, 2013).

Görüldüğü üzere burada derin bir şekilde kutuplaşmış küresel bir tartışma ve güç mücadelesi söz konusudur. İnternet kullanımının artmasıyla paralel olarak, internet yönetişimi üzerindeki uzlaşmazlıklar da giderek derinleşmiştir. Bu durum, küresel çapta bir kutuplaşmaya ve çeşitli yönetişim modellerinin ortaya atılmasına sebep olmuştur. Dominic'in (2020) vurguladığı gibi, bu modellerden biri, ABD ve Avrupa tarafından savunulan açık ve özgür interneti temsil eden "Batı modeli"dir. Diğer yanda ise, internetin daha kontrollü kullanımını savunan ve Çin ile Rusya gibi ülkeler tarafından desteklenen "Leviathan modeli" bulunmaktadır.

Özellikle WGIG raporu ve IGF'nin oluşturulması, internet yönetişimi konusundaki küresel tartışmaların çeşitliliğini ve karmaşıklığını gözler önüne sermektedir. Küresel düzeydeki bu tartışmalar, çeşitli yönetişim modellerinin avantajlarını ve sınırlılıklarını değerlendirme ihtiyacını ortaya koymaktadır. Bu kapsamda, internet yönetişimi üzerine yapılan küresel tartışmalar ve çeşitli modellerin değerlendirilmesi, küresel internetin geleceği için hayati öneme sahiptir. IGF ve benzeri platformların, bu tartışmalarda merkezi bir rol oynaması beklenmektedir. Şimdi, bu genel bakışın ardından, farklı yönetişim modellerinin her birinin nasıl bir çözüm sunduğu ve internet yönetişimi tartışmalarında nasıl bir yer tuttuğuna dair detaylı bir inceleme yapılacaktır.

4.1.1. Öz-Yönetim Modeli

1980'lerde ve 1990'ların ortalarına kadar geleneksel hukukun siber alana uygulanması reddedilmiştir. Bunun yanında, internet yönetişiminin devletlerin veya diğer geleneksel egemenlerin doğrudan katılımı olmadan kurulamayacağına yönelik görüşlere de karşı çıkılmıştır. Esasen bu reddetme girişimi, internet yönetişiminin ikinci aşamasının başlangıcını oluşturmuştur. Bu dönem boyunca birçok yönetici ve akademisyen, devlet aktörünü siber alandan uzak tutmaya yönelik yazılar kaleme almıştır. *Technolibertarianism* veya *cyberliberterianism* olarak kavramsallaştırılan bir yaklaşımın öncüleri, bu görüşün birincil savunucuları olmuşlardır. Bu görüş, devlet düzenlemelerini, sansürü veya World Wide Web'e yönelik her türlü kısıtlamayı en aza indirme veya ortadan kaldırma hedefindedir. En çok bilinen siber-liberterler John Perry Barlow, Johnson Post, Julian Assange, John Gilmore ve T. J. Rodgers'tir.

Bu görüşün savunucuları, yaklaşımlarının en önemli gerekçesi olarak siber uzayın "yönetilemezliğini" göstermişlerdir. Bu konuda öne çıkan isim, 1996 yılında yayınladığı "Siber Uzayın Bağımsızlık Bildirgesi" ile tanınan Barlow'dur. Bildirgede Barlow, siber uzayın devlet kontrolünün dışında olması gerektiğini açıkça ilan etmiştir. Bu Bildirgenin açılış paragrafında yer alan şu sözler dikkat çekicidir:

> Endüstriyel dünya devletleri, sizler etten ve çelikten bıkmış devler, ben aklın yeni yurdu siber uzaydan geliyorum. Gelecek adına, sizden geçmişten bizi rahat bırakmanızı rica ediyorum. Aramıza hoş gelmiyorsunuz. Toplandığımız yerde egemenliğiniz yok. Seçilmiş bir hükümetimiz yok ve muhtemelen bir devletimiz de yok, bu yüzden size özgürlüğün her zaman konuştuğundan daha büyük bir otorite ile hitap ediyorum […] Bize hükmetmek için ahlaki bir hakkınız yok ve korkmak için gerçek bir nedenimiz var (Barlow, 1996).

Bu bildiride siber uzay, ayrı bir alan olarak kabul edilmiş ve örtülü olarak buraya ait vatandaşların öz yönetimle yönetildikleri fikri benimsenmiştir. Siber uzay sakinleri (*netizens*) internet iletişiminin üretken, işbirlikçi yönlerini teşvik etmek için çabalayan sorumluluk sahibi bireyler olarak kabul edilmiştir. Hauben (1998), netizenleri ağ yönetimine fayda sağlayan ve ağ üzerinde kolektif bir ortam inşa etmeye çalışan kişiler olarak tanımlamıştır. Bu kişiler arasında, internet mimarisinin geliştirilmesinde kilit rol oynayan teknoloji uzmanları da mevcuttur. Bu durum, netizenlerin kuralsızlığı

savunduğu anlamına gelmez. Zira onların karşı çıktığı devletlerin koydukları kurallardır. Kurallar, siber uzayın ilk zamanlarında genellikle standartların geliştirilmesine yönelik prosedürler biçiminde ortaya çıkmıştır. Bazı durumlarda da temel nezaket ve edep standartlarının korunmasına ilişkin kurallar biçiminde kabul edilmiştir. Bu kurallar, network kelimesinin kısaltılmasından elde edilen "net" ile görgü kuralı anlamına gelen "etiquette" kelimesinin birleşiminden oluşan "*netiquette*" terimi ile ifade edilmiştir. İlk netiquette kuralları, WWW öncesi döneme ait elektronik forumlarda ortaya çıkmıştır (Hambridge, 1995, s. 14).

Barlow'un beyanının internet yönetişimiyle doğrudan ilgili olduğu söylenebilir. Bygrave ve Michaelsen Bildiri'yi ulus-devletlerin siber alandaki egemenliğini kabul etmemesi gerekçesiyle "tehditkâr" olarak da nitelendirmiştir (2009, s. 117). Zira doğrudan internet mimarisinin kontrolü ve denetimi meselesiyle ilgilidir. Barlow'un beyanı, ilk zamanlar internet standartları topluluklarının üyelerinin çoğunluğu tarafından desteklenmemiş olsa da kısa bir süre sonra aksi yönde girişimlerde bulunmuşlardır. Bu doğrultuda, ABD hükümetinden veya herhangi bir ulusal hükümetten bağımsız olarak kritik İnternet kaynakları üzerinde kontrol sağlanması için "kendi kendini yönetme hakkını" savunmaya başlamışlardır. 1997'de ISOC tarafından geliştirilen gTLD-MOU girişimi bunun ilk örneklerinden birini oluşturmuştur. Bu girişim, internet adlandırma ve numaralandırma sistemi üzerindeki yetkiyi, ISOC kontrolü altında olacak yeni bir uluslararası kuruluşa devretmeyi amaçlamıştır. Bunun yanında, IANA'nın oluşturulması ve ardından RFC'ler aracılığıyla IANA'nın yetki kaynağını IAB ve ISOC'a verme girişimleri de buna örnek olarak gösterilebilir.

ABD hükümeti, bu girişimlere rıza göstermedi. Clinton yönetimi, ağın gelişimini sözleşmeler kapsamında finanse ettiğini öne sürerek ABD hükümetinin internet üzerinde nihai yetkiye sahip olduğunu kabul etmiştir. Bu doğrultuda 'gTLD-MOU' girişimini kesin bir dille reddetmiş ve ortadan kaldırmıştır. Bundan kısa bir süre sonra, IANA'nın işlevlerinin hükümet gözetimi altında çalışan bir kuruluş olan New Corporation'a (NewCo) aktarılmasının önünü açmıştır. Nitekim, 1990'ların sonlarından itibaren, diğer ulusal hükümetler de kendi yetki alanlarına giren ccTLD'lerin yönetimi üzerinde daha fazla kontrol sahibi olmaya başlamışlardır. Hatta ccTLD'leri kendi egemenlikleri altında ulusal bir kaynak olarak değerlendirmişlerdir (Bygrave & Michaelsen, 2009, ss. 117-118).

Johnson vd., bu kontrol mekanizmasının nasıl işleyebileceğine dair üç temel model önerir: aydınlanmacı diktatörlük, demokrasi ve merkeziyetsiz karar alma. Her biri, kuralların kim tarafından belirlendiği ve nasıl uygulandığı konusunda farklı yaklaşımlar sunar (2004, s. 6). Aydınlanmacı diktatörlük, tek bir merkezi otoritenin kontrolü altında, hesap verebilirlik ve şeffaflık olmaksızın işleyen yönetim biçimidir. Bu modelde, tek bir yönetici veya grup platformlar üzerinde mutlak kontrol sahibidir. Bu nedenle kararlar da hızlı bir şekilde alınabilmektedir. Demokrasi modelinde merkezi kontrol ile birlikte vatandaşlara resmi hesap verebilirlik söz konusudur. Kullanıcıların karar alma süreçlerine katıldığı, politika ve kuralların kolektif olarak belirlendiği platformlar mevcuttur. Bu modelde katılımcılık ve şeffaflık hâkim olduğundan, karar alma süreçlerinin yavaş olma potansiyeli yüksektir. Son olarak merkeziyetsiz karar alma modeli ise, bireylerin veya grupların kendi kurallarını belirleyip uyguladığı sistemi ifade eder. Açık kaynak projeleri, *peer-to-peer* ağlar gibi merkezi olmayan ağlar hakimdir. Bu durum esneklik ve inovasyon özgürlüğü sağlasa da, koordinasyon ve standardizasyon eksikliği yaratmaktadır (Johnson vd., 2004, s. 6).

Bu bağlamda Johnson vd., temsile dayalı geleneksel demokrasi modellerinden ziyade, merkezi olmayan karar alma süreçlerini savunan merkeziyetsiz karar alma modelini savunur. Onlara göre, internetin doğası, bireylerin ve grupların doğrudan sorumluluk alarak ve güvene dayalı bağlantılar kurarak kendi kurallarını belirlemeleri ve uygulamaları için uygun bir ortam sunar (2004, ss. 6-7). Bu yaklaşım, kimliği doğrulanmış tanımlayıcıların artışı ve antisosyal aktivitelerin daha kolay engellenmesi gibi teknolojik ilerlemelerle desteklenmektedir. Sonuç olarak, online toplumlar, güvenilir kaynaklardan alınan bilgilere dayanarak risk alma eğilimlerini ayarlayabilir ve yanlış yapan bireylere karşı etkili bir şekilde hareket edebilirler. Bu, "sorumlu internet" kavramına doğru bir adım olup, bireylerin ve toplulukların online faaliyetleri üzerinde kolektif bir kontrol ve yönetişim modeli oluşturmasını sağlar. Bu model, hem merkezi hem de merkezi olmayan sistemlerin bir arada var olabileceği ve etkili bir şekilde işleyebileceği yeni bir yönetişim anlayışını temsil eder. Bu çerçevede, devletlerin rolü, büyük online sorunlara karşı koruma sağlama ve aynı zamanda bu tür merkezi olmayan yönetimi destekleme ve teşvik etme yönünde evrilebilir.

Diğer yandan Chang ve Grabosky, öz-düzenlemenin yaygın olarak tanınan üç biçimini ortaya koymuşlardır: tamamen gönüllü öz-düzenleme, zorunlu öz-düzenleme ve kısmi devlet katılımı ile zorunlu öz-düzenleme (2017, s. 538-539). Saf öz-düzenleme nadiren

görülse de, çoğu öz-denetim devletin bir derecede katılımını içerir. ICANN gibi kuruluşlar, devletlerin katılımıyla yapılan öz-düzenlemenin örneklerindendir. Zira ICANN, ABD Ticaret Bakanlığı ile sözleşmeli olup, ABD Hükümeti tarafından denetlenir. Öz-düzenleme, ulusal düzeyde de özellikle kritik altyapı sektörlerinde görülebilir. Örneğin, Çin Hükümeti tarafından desteklenen Çin İnternet Topluluğu, kötü amaçlı yazılımların kötüye kullanımını düzenlemek ve yayılmasını önlemek için öz-düzenleme girişiminde bulunmuştur. Bu tür girişimlerde, sektörün önde gelen şirketleri kötü amaçlı yazılımlarla mücadelede işbirliği yapar. Diğer taraftan, devlet müdahalesi olmaksızın online davranışın düzenlenmesi örnekleri de mevcuttur. ABD'de Amerika Kayıt Endüstrisi Birliği (RIAA) gibi özel kuruluşlar, telif hakkı ihlalleriyle mücadelede kendi düzenleme mekanizmalarını uygulamaktadır. Ancak, bu tür özel düzenlemelerin zayıflıkları ve sınırlamaları da bulunmaktadır.

4.1.2. Ulusal (*Domestic*) Model

Devletlerin sahip olduğu çeşitli yönetim biçimleri (demokratik, monarşik, komünist vb.), internet yönetişimi ve siber güvenlik politikaları üzerinde derin etkiler bırakmaktadır. Wendt'in vurguladığı gibi, devletlerin devlet-toplum ilişkilerinin yapısını yansıtan birçok biçimi bulunmaktadır (1999, s. 201). Bu çeşitlilik, siber alanın yönetişimi konusunda farklı yaklaşımların benimsenmesine yol açar. Örneğin, siber sınırların belirlenmesi ve internet üzerindeki kontrolün uygulanması, devletlerin iç politik yapılarına ve uluslararası ilişkilere olan bakış açılarına göre değişiklik göstermektedir. Devletlerin yönetim biçimleri, siber alanın kontrolü ve yönetimi ile ilgili politikaları şekillendirirken, aynı zamanda bu süreçler, siber alanın küresel doğasının getirdiği meydan okumalarla da etkileşime girer.

İnternet yönetişimi ve siber güvenlik politikalarının geliştirilmesi, devletlerin iç ve dış politikalarının bir yansıması olarak ortaya çıkmaktadır. Bu bağlamda, internetin küresel elektronik ticaretin faydalarından yararlanılmasını sağlama potansiyeli, ulusal çıkarları ön plana çıkarmaktadır. Bu nedenle internet yönetişimi sorunu, bölgesel ve ulusal düzeyde giderek daha fazla derinleşmektedir. İnternet yönetişimi terimi, internetin küresel elektronik ticaretin faydalarından yararlanmak isteyen tüm ülkeler için önemli bir ulusal çıkar alanı olduğunun yaygın olarak tanınmasının bir sonucu olarak özellikle dikkat çeken bir alan haline gelmiştir. Devletlerin bakış açısından internet, hem kullanımı yüksek ekonomik değer vadeden bir teknoloji hem de daha önce icat edilen

diğer tüm telekomünikasyon medyalarından farklı bir meydan okuma olarak görülmektedir (Cerf, 2004).

Devletler, internet yönetişimi üzerinde söz sahibi olmak adına ulusal ve bölgesel alanda kendi kurallarını empoze etmek için "yasal bir silahlanma yarışı" başlatmıştır. Bu tür yönetişim biçimleri, bazı paydaşların ulusal siber alanda hak ihlallerinde bulunmalarına sebebiyet verebilmektedir (Goldsmith & Wu, 2006, s. viii). Ancak ulusal düzeyde giderek daha sık görülen bir diğer yönetişim sorunu/krizi örneği, internetin kapatılması veya kasıtlı olarak kesintiye uğratılmasıdır. İnternetin kapatılması durumlarında genellikle başta sosyal medya platformları olmak üzere tüm ağlara erişim engellenmektedir. Özellikle sosyal medya platformlarından başlanmasının başlıca nedeni, bu platformların politize edilerek siyasi hareketlerde kullanılmaya başlanmış olmasıdır (Ertem & Korhan, 2019, s. 221). Ancak bazı durumlarda internete erişimin engellenmesinin altında meşru sebepler de yatabilmektedir. Kamu düzeni için bir tehdit olarak görülen veya belirli bir hedef kitle için sakıncalı olan yasa dışı verilere erişimin engellenmesi buna örnek olarak gösterilebilir. Ancak çoğu durumda kısıtlamalar uluslararası anlamda yasallık, gereklilik, orantılılık, şeffaflık ve meşruiyet standartlarının dışında gerçekleşmektedir (van der Spuy, 2017, s. 32).

Kesan ve Shah (2005), devletlerin internet standartlarını geliştirmede iki tür etkinliğinin bulunduğunu varsayar. Bu iki etki biçimini "doğrudan" ve "dolaylı" şeklinde kategorize etmiştir. Doğrudan etkilerine örnek olarak, bilgi sistemlerinin kişisel verileri gereksiz yere toplamasını engelleyen mevzuatı gösterilebilir. Dolaylı etkilerine örnek olarak ise, belirli bir sektörün bir sorunu kendi başına çözememesi durumunda bu sektöre yasal müdahalenin uygulanmasını öngören mevzuatı gösterilebilir. İkinci mevzuat, bazı Batı ülkelerindeki İnternet Servis Sağlayıcılarının (ISS) yasa dışı veya saldırgan içeriğe kamu erişimini engelleme çabalarını teşvik etmede etkili olmuştur (Bygrave & Michaelsen, 2009, s. 119).

Uluslararası ve bölgesel örgütler aracılığıyla egemenlikçi modeli oluşturmaya çalışan devletlerin bazıları, aynı zamanda siber alanı kendi sınırları içinde bölgeselleştirmeye de çalışmaktadır. Örneğin Rusya ve Çin'in bu alandaki kontrolü talep etmesi, yalnızca ulusal güvenlik veya ulusal çıkar kaygısıyla değil, liberalizm ile olan tarihsel çekişmeleriyle açıklanabilir. Bu devletlerin çok paydaşlı model karşısında ellerinde bulundurdukları sağlam bir "uluslararası hukuk" kozu bulunmaktadır. Zira geleneksel

uluslararası hukuk, devlet egemenliği ve müdahale etmeme ilkelerinin sürekli olarak sürdürülmesini zorunlu kılmaktadır. Bu devletler de, çok paydaşlı modeldeki özgürlükçü yaklaşımın interneti diğer devletlerin iç işlerine müdahale için bir araç olarak kullandığını iddia etmektedirler. Bu bağlamda siber uzayı, "fiziksel devlet sınırlarına" karşılık gelen "sanal sınırları olan bir bölge" olarak görmektedirler. Dolayısıyla bu bölgeyi kontrol altına almak için uluslararası hukuku bu alana genişletmeyi hedeflemektedirler. Otoriter devletler, özellikle 2010 yılında patlak veren Arap Baharı sürecinde Twitter, YouTube ve Facebook gibi platformlar aracılığıyla dijital teknolojinin baskı altındaki toplumları mobilize etme gücü ile karşı karşıya kalmışlardır. Bu süreç itibariyle bu ülkeler, dijital olan her şeyi, siyasi statükoyu zayıflatabilecek araçlar olarak görmeye başlamışlardır. Bu yaklaşım, kolluk kuvvetlerinin dijital araçların siyasi kullanımını izlemeye başlamasıyla sonuçlanmıştır (Eichensehr, 2015b). Bunun yanında, televizyon ve radyo yayıncılığı gibi devlet tarafından kontrol edilen geleneksel medya ile ilgilenmeyi bırakıp, politik olarak "yıkıcı" gördükleri internetle ilgilenmeye başlamışlardır. Bu yaklaşımlar, özellikle Çin ve Rusya gibi büyük güçler arasında yayılmaya başlamıştır.

Çin'in "egemen sanal bölge" (*sovereign virtual territory*) tanımlamasından "Çin'in Büyük Güvenlik Duvarı" (*Great Firewall of China*) söylemine kadar pek çok yaklaşım, interneti "ulusal anlamda" kontrol etme isteğini yansıtmaktadır (Swaine, 2013, s. 4; Economy, 2019). Benzer şekilde Rusya, Kasım 2019'da ülkenin internet altyapısını "egemen internet" yasasıyla kontrol etmeye yönelik tartışmalı bir attı. Böylece Rus yetkililer, Rusya'daki web sitelerinin ve Rus alan adlarındaki sitelerin resmi olmayan "RuNet" i kriz zamanlarında küresel web'den izole etmelerine olanak tanıyarak, ülkeye giren ve çıkan veri akışlarını kontrol edebilmiştir (Roache, 2021). İran da küresel internetten ayrı, daha sıkı kontrol sağlayabileceği ulusal bir online ağ oluşturmak için gerekli olan teknik temelleri atmıştır. Bu durum, 2009'da hükümet karşıtı protestolar sırasında görüldüğü üzere hükümete internet erişimini kapatma konusunda daha fazla güç verebilmektedir (Iran Focus, 2012). Çin, İran ve Küba gibi ülkeler, internet kullanıcılarına erişim engeli getiren "elektronik duvarlar" inşa etmeleriyle ünlüdür (Schaake, 2012).

İnternete kısıtlamalar getirmeye çalışan devletler, yalnızca "çok taraflılığı" savunan ülkeler değildir. Çok paydaşlı modeli savunan Batılı ülkelerin çoğunun da ulusal çıkarlar söz konusu olduğunda benzer eğilimde bulunduğu gözlemlenmiştir. Açık

internetin savunuculuğunu yapan OpenNet Initiative (ONI), siyasi, sosyal ve güvenlik nedenleriyle internet içeriğini engelleyen 61 ülkeyi listelemiştir.[64] Bu eğilimler nedeniyle "uluslararası hukuk" bağlamında ulus-devletlerin siber uzayda bölgesel egemenliklerini genişletmelerinin mümkün olup olmadığı sorusu ortaya çıkmaktadır.

Bir yandan, internete kısıtlamalar getiren devletlerin çoklu bir yaklaşım izlediği gözlemlenirken, diğer yandan, bu kısıtlamaların uluslararası hukuk çerçevesindeki meşruiyeti sorgulanmaktadır. Shaw (2001), ulusal modele yönelttiği eleştiriyi şöyle bir soruyla taçlandırıyor: "Bu kadar küresel görünen bir ortamda düzenlemeye yönelik ulusal yaklaşımlar işe yarayabilir mi?". Shaw'ın bu soruya cevabı net değil. Ona göre ulusal düzenleme çabalarının, internet gibi küresel bir ortamda ne ölçüde etkili olabileceği belirsizdir. İnternetin kim tarafından düzenleneceği sorusu henüz net bir cevaba sahip değil, ancak şu bir gerçek ki, dünya online olmaya devam ettikçe, internet ABD'nin altyapısına, kültürüne veya politikasına entegre olmaktan çıkacaktır. Bu süreçte internet, farklı ırkların düşünce ve duygu biçimlerindeki çeşitliliği daha iyi yansıtacak bir evrime doğru ilerlemektedir.

İnternetin küresel yapısı, siber sınırların kesin bir şekilde çizilmesini neredeyse imkânsız kılar. Siber saldırılar, sınırların ötesinden kolaylıkla başlatılabilir ve bu, siber sınırlar kavramının sınırlı bir etkinliğe sahip olduğunu gösterir. Siyasi ve sosyal dinamiklerdeki önceki gelişmeler, özellikle devlet dışı aktörlerin ve uluslararası kuruluşların eylemlerinin meşruiyetindeki artış, egemenliğin devlete özgü bir özellik olduğu varsayımını zaten sorgulatmaya başlamıştı. İnternet ise, bu değişim sürecine potansiyel olarak eşlik eden bir faktör olarak ortaya çıkmıştır (Pigatto & Datysgeld & Silva, 2021, s. 5).

4.1.3. Çok Paydaşlılık (*Multistakeholder*) Modeli

İnternet yönetişimi bugün çok sayıda aktörü bünyesinde barındırmaktadır. Aynı zamanda, "çok paydaşlılık" kavramı, bu alandaki mevcut söylemlere hâkim olmaya başlamıştır. Terim ilk olarak 1990'larda politika ve kurumsal karar alma süreçlerine dahil olan aktörlerin sayısını genişletmenin bir aracı olarak ortaya çıkmıştır (Taylor & Hoffmann, 2019, s. 6). Çok paydaşlı yönetişim, tartışmalara ve karar alma süreçlerine çok sayıda gruptan temsilcilerin dahil edildiği bir süreci ifade eder (Hemmati, 2002, s. 2). Çok paydaşlı yönetişimde kolektif alınan kararlar aracılığıyla ortak sorunların ele

[64] Ayrıntılı bilgi için bkz: https://opennet.net/ (03.05.2021).

alınması ve çözümü mümkündür. Teorik olarak çok paydaşlı yönetişim, karar verme sürecini merkezden uzaklaştırır ve demokratikleştirir (Taylor & Hoffmann, 2019, s. 7).

Çok paydaşlılık modeli, internet yönetişimi düzenlemelerinde temel bir ilke olarak kendini göstermiştir. Bu model, devlet ve devlet dışı aktörlerin, politika kararlarını eşit şartlarda müzakere etmeleri ve alınan kararların tüm ilgili tarafların katkılarıyla şekillendirilmesi gerektiği anlayışına dayanır (Epstein & Nonnecke, 2016, s. 143). Bu model, internetin merkezi olmayan, küresel ve açık bir sistem olduğunu ve devletlerin çok fazla kontrol sahibi olmasının sivil haklar ve özgürlükler için tehlike oluşturacağını savunur (Hoxtell & Nonhof, 2019, s. 11). Çok paydaşlı katılım, internet yönetişiminin temel bir unsuru olarak, karar alma süreçlerine çeşitli grupların dahil edilmesini ifade eder. Bu, devlet temsilcileri, özel sektör, sivil toplum, teknik topluluklar ve akademik çevreler gibi farklı paydaşların görüşlerinin, internetin yönetişimi ve politika yapımı süreçlerinde dikkate alınmasını gerektirir (van der Spuy, 2017, s. 25).

Van der Spuy, internetin günlük yaşam için giderek daha önemli hale geldiği bir zamanda, işleyişinin "parçalanmasını" (*splintering*) engellemek için devletler ve diğer paydaşlar arasında küresel işbirliğinin gerekli olduğunu ifade etmiştir (2017, s. 161). Bunun yanında, çok paydaşlı süreçlerin daha iyi anlaşılmasını sağlamak için çok paydaşlı modelde bulunması gereken birtakım değerler sıralamıştır. İnternet evrenselliğini destekleyen bu değerler şunlardır: 1. kapsayıcı; 2. çeşitli; 3. işbirlikçi; 4. şeffaf; 5. eşit; 6. esnek ve ilgili; 7. özel ve güvenli; 8. hesap verebilir ve meşru ve 9. duyarlı (van der Spuy, 2017, s. 69). Etkili bir internet yönetişimi, hesap verebilirlik ve meşruiyet ilkelerinin geçerli olduğu çok paydaşlı bir katılım gerektirmektedir. Çok paydaşlılık, devleti tek aktör olarak gören geleneksel yaklaşımlarla karşılaştırıldığında daha fazla verimlilik, esneklik ve hassasiyet söz konusudur. Aynı zamanda bu yaklaşımda uluslararası düzenlemeler ve hukuk aracılığıyla teşvik edilen demokratik uygulamalar da çok paydaşlılığın gerektirdiği unsurlardır.

ISOC'un (2016) görüşüne göre çok paydaşlı yaklaşımlar, "farklı alanlardan bireylerin ve organizasyonların bir araya gelerek fikir paylaşması veya politika geliştirmesi" anlayışını temel alan bir dizi araç veya uygulama sunar. Fikir paylaşımı ve karar alma dışında, çok paydaşlı yaklaşımların temel bir gerekçesi, "daha iyi, daha kapsayıcı internet yönetişimi"ne yol açması ve "şeffaflığı artırması"dır ve karar alıcılara çeşitli

görüşleri dikkate alma imkânı tanır, bu da demokrasiyi derinleştirebilecek bir yöntem olarak önerilir.

İnternet yönetişimine çok paydaşlı katılım talebi ilk olarak WSIS'te açıkça ifade edildi (ITU, 2005a). Tunus Gündemindeki metin, devlet ve devlet dışı aktörlerin tamamını içermesi nedeniyle internet yönetişimine "çok paydaşlılık" konusunda katkı sağlamıştır (Hubbard & Bygrave, 2009, s. 229). Gündem Raporunun 72. paragrafında BM Genel Sekreteri'nden "çok paydaşlı politika diyaloğu için yeni bir forum" (yani IGF) yaratma talebinde bulunulmuştur.[65] Bunun yanında WSIS için öngörülen BM kararıyla birlikte internet yönetişimi tartışmalarına çok paydaşlı katılım için ilk yasal zemin sağlanmıştır. Başlangıçta "çok paydaşlı" kavramı özel sektör liderliği ile ilişkilendirilirken, tanıma dair herhangi bir netlik sağlanamamıştı. Tunus Gündemi ile birlikte kavramın tanımı diğer paydaşları içerecek şekilde genişletilmiştir. Devletler, özel sektör, sivil toplum ve hükümetlerarası kuruluşların tamamını kapsayan tanım, IGF'nin de katkısıyla akademik ve teknik toplulukları da içeren yeni bir forma bürünmüştür.

Öte yandan NETmundial toplantısı, Brezilya Cumhurbaşkanı Dilma Rousseff ve ICANN tarafından, ABD Ulusal Güvenlik Ajansı'nın gözetleme uygulamalarına dair Edward Snowden'ın ifşaatlarına yanıt olarak Ekim 2013'te düzenlenmiştir. Bu toplantı, çok paydaşlı bir zirve olup, çok paydaşlı internet yönetişiminin geleceği için prensipler ve bir yol haritası belirleyen bağlayıcı olmayan bir "Çok Paydaşlı Beyan" üretmiştir. Bu toplantı, internet yönetişimi süreçlerinin, "aşağıdan yukarıya, tüm paydaşların tam olarak katılımını sağlayacak şekilde, hiçbir paydaş grubunu dezavantajlı duruma düşürmeyecek" şekilde olması gerektiğini vurgulayan bir beyanla sonuçlanmıştır (Belli, 2015, s. 5).

WSIS'ten bu yana birçok uluslararası ve çok taraflı kuruluş, çok paydaşlı katılım ihtiyacını dile getirmiştir. Bunlar; 2008 ve 2011'de OECD; 2014'teki WSIS+10 etkinliğinde UNESCO; 2009'da Avrupa Konseyi; 2010 ve 2014'te ITU; 2011'de Deauville'de G8 ve 2014'te Afrika Birliği şeklinde sıralanabilir. BM Genel Kurulu, WSIS'in 2015'teki on yıllık incelemesinde hem modelinin hem de çalışma tanımının tüm ilgili paydaşların katılımını teşvik ettiğini belirtmiştir (van der Spuy, 2017, s. 22).

İnternet yönetişimine çok paydaşlı katılım, diğer çok paydaşlı katılım örneklerinden birçok konuda farklılaşmaktadır. Bazıları, internetin düzenleyici denetimden veya yargı

[65] Ayrıntılı bilgi için bkz: (ITU, 2005a, s. 17).

mekanizmasından muaf olduğunu ve böyle kalması gerektiğini iddia etmiştir (Johnson & Post, 1996; Barlow, 1996). Oysa internet, hiçbir koşulda kurallardan, kanunlardan veya yasal kısıtlamalardan tamamen muaf bir alan olmamıştır (Holbrook, 2000, s. 761). Pek çok kişi, benzersiz tasarımı ve bileşimi nedeniyle internetin geleneksel olmayan yönetişim biçimlerini gerektirdiğini savunmuştur. Özellikle Westphalian anlayışı benimseyen geleneksel yönetim biçimlerinde hâkim olan devlet aktörünün ağırlığına karşın; demokratik unsurların esas alındığı çok paydaşlı katılımı desteklemişlerdir. Nitekim internet, özellikle çok paydaşlı katılımla eşleşen açık, dağıtılmış, birbirine bağlı, katılımcı ve aşağıdan yukarıya süreçlerle tanımlanır (Internet Society, 2016). Cerf vd., siber alandaki aktör çeşitliliğinin çok paydaşlı bir yönetişim yaklaşımını gerektirdiğini savunmuştur. Ancak Cerf vd., internetin katmanlı modelini kullanarak, kurumların uzmanlık alanlarına odaklanmalarının önemini vurgulamışlardır (2014, s. 1). Örneğin, ITU'nun geniş bant altyapısını teşvik etme çabaları, siber güvenlik ve spam düzenlemeleriyle ifade özgürlüğünü kısıtlamak gibi alanlarda çeşitli çatışma noktalarına yol açabilir. Bu, kurumların kendi uzmanlık alanlarından saparak, internet yönetişimindeki dengeyi etkileyebilecekleri bir durumu göstermektedir. Bu görüş, bu çalışmada paydaşların tanımlanmasında önemli bir çıkış noktasını temsil etmiştir.

4.1.3.1.Özgürlükçü Yaklaşımlar

Dijital otoriterliğin yükselişine karşı internet özgürlüğünü güvence altına almak, demokrasiyi korumanın temelidir. Zira teknoloji, vatandaşları gizli manipülasyon maruz bırakmadan kendi sosyal, ekonomik ve politik seçimlerini yapmaları için güçlendirmelidir (Shahbaz, 2018, s. 2). Bu bağlamda antidemokratik ve otoriter yapıdaki devletlerin internet üzerinde elde etmeye çalıştığı ağırlık çok paydaşlılık bağlamında "özgürlükçü" modeli savunan devletlerce engellenmeye çalışılmaktadır. Çoğu ülkenin hedefi, siber uzayda mahremiyet, güvenlik ve bireysel hakları sağlamaktır. Burada asıl amaç, temel özgürlüklerden ödün vermeden vatandaşlarını korumak için devletlerin endişelerini gidermektir. ABD'nin konuya ilişkin tutumu, Uluslararası Siber Uzay Stratejisi'ndeki bazı ifadelerle aktarılmıştır:

> Tüm internet kullanıcılarının ihtiyaçlarına etkin bir şekilde hizmet eden internet yönetişim yapılarını desteklemek ve internet yönetişimi konularını tartışmak için çok paydaşlı mekanları teşvik edip geliştireceğiz. İnternetin mimarisi, merkezi olmayan, işbirliğine dayalı ve katmanlı olan bir sosyal ve teknik organizasyon halini bünyesinde

> barındırmaktadır. Bu özelliklerin her biri, İnternetin getirdiği faydaların temelini oluşturur. Bu mimari, ekonomik büyümeyi mümkün kılan inovasyon özgürlüğünü besler. Sosyal ve politik büyümeyi ve dünya çapında demokratik toplumların işleyişini mümkün kılan ifade ve örgütlenme özgürlüğünü besler (The White House, 2011, s. 22).

Bu bağlamda ABD, özellikle internetin başlarında ticari anlamda serbestliği sağlayarak internete yönelik "açıklık" ilkesini savunacağının emarelerini göstermişti. Ancak ABD'nin internet üzerinde uygulamaya çalıştığı bu "*laissez faire*"[66] anlayışının internetin ilk çıktığı dönemler için uygun olduğunu, bugünün koşulları göz önüne alındığında bu modelin "yetersiz" olduğunu savunanlar da mevcuttur (Lewis, 2020). Bu yaklaşıma rağmen, orijinal yönetişim yapısından çıkmanın internetin ekonomik potansiyeline zarar vereceğine dair bir korkunun hâkim olduğu bilinmektedir. Her ne kadar ABD ve özellikle Avrupa ülkeleri bu yaklaşımı savunsa da, getirdikleri düzenlemeler internetin büyümesini ve yenilenmesini yavaşlatmaktadır.

AB ise, çok paydaşlı internet yönetişim modeline sadık kalırken, aynı zamanda, bölgesel olarak bazı düzenleyici adımlar da atmaktadır. AB Temel Haklar Şartı'nın 8. Maddesi ile teminat altına alınan temel bir hak olan kişisel verilerin korunması konusu, Avrupa sınırları içinde ve dışında, uluslararası bir egemenlik çerçevesi tanımlama ihtiyacını yeniden gündeme getirmiştir. Avrupa Komisyonu'nun 12 Temmuz 2016'da Gizlilik Kalkanı'nı tanıması ve Güvenli Liman çerçevesinin Avrupa bölgesi dışındaki verilerin eşdeğer korunmasını taahhüt etmesiyle, şiddetli ve rekabetçi tartışmalar başlamıştır. Benzer şekilde AB, Avrupa'da faaliyet gösteren şirketler için bir düzenleyici çerçeve oluşturmak için hareket etmektedir. Bu model, hizmetlerin tek bir ülkede oluşturulduğu, küresel olarak dağıtıldığı ve üçüncü ülkelerde tüketildiği "uygulama ekonomisi" tarafından yönlendirilen yeni bir sınır ötesi erişim modelidir. Dolayısıyla bu durum, internetin doğasından gelen özgürlük fikrini zedelemektedir (Gueham, 2017).

Ancak genel olarak getirdikleri düzenlemelerin egemenlikçi modelin savunucuları kadar katı olmadığı bilinmektedir. Dolayısıyla bugün, internetin yapısının korunması, özgürlükçü ile aşırı düzenlemeyi öngören iki kutup arasında bir "orta yol"un

[66] *Laisses Faire*, "bırakınız yapsınlar" olarak adlandırılan ve ekonomide serbestlik anlayışını öngören bir yaklaşımı ifade eder. Ekonomi üzerindeki her türlü düzenlemeyi reddeden, ekonomik müdahalecilikten uzak bir yaklaşımdır. Bir düşünce sistemi olarak ise, bireyin toplumda temel birim olduğu ve doğal bir özgürlük hakkına sahip olduğunu savunmaktadır.

bulunmasını gerektirmektedir (Lewis, 2020). ABD gibi çok paydaşlılığı savunan ülkelerin birincil amacı, yeni teknolojilerin ulusal sınırlar olmadan nasıl işleyebileceği konusunda bir fikir birliği oluşturmaktır. Bununla birlikte, devlet organlarının yanında sivil toplum kuruluşlarının ve akademinin de görüşlerini alarak uzlaşma sağlamaktır. Bu durum özellikle yüksek düzeyde yatırım, bilim ve sermaye gerektiren ve halihazırda düşük düzeyde devlet tarafından belirlenmiş standartlar belirlemektir. Burada önemli bir aktör olarak ICANN görülmektedir (Gleckman, 2018, s. 21).

4.1.3.2.ICANN'in Rolü

İnternet yönetişimi, teknolojik ilerleme ve internetin sürekli genişlemesi ile birlikte kademeli olarak gelişmiştir. Bu nedenle, ağın merkezileştirilmesinde en önemli paya sahip kurumlardan biri olan ICANN'in gelişimi önem arz etmektedir (Andjelkovic, 2006, s. 9). Taylor ve Hoffman, ICANN'i çok paydaşlı yönetişimin "poster çocuğu" olarak adlandırmaktadır (2019, s. 7). ICANN'in politika oluşturmasının merkezinde, "çok paydaşlı model" vardır. Bu, politika oluşturmaya yönelik topluluk temelli fikir birliğine dayalı bir yaklaşımdır. Buradaki fikir, internetin yapısının sınırsız ve herkese açık olması gerektiğini savunmaktadır (ICANN, t.y.). Bu doğrultuda günümüzde internetin, tarihsel kökenlerinin bir sonucu olarak çok paydaşlılık modeliyle yönetildiği söylenebilir. Devletler, özel sektör, uluslararası kuruluşlar ve sivil toplum gibi aktörlerden oluşan bu modelde aktörler arasında herhangi bir hiyerarşi söz konusu değildir. Devletlerin yanı sıra devletlerarası müzakerelere katılan kamu yararını savunan gruplardan ve iş derneklerinden temsilciler vardır (Mueller, 2010, s. 8).

ICANN'in kuruluş sürecinin temelleri olarak istikrar, işbirliği, aşağıdan yukarıya (*bottom-up*) koordinasyon ve temsil ilkeleri ana hatlarıyla belirtilmiştir (ICANN, 1998). Böylece, ITU'nun ve dolayısıyla ulus-devletlerin ön plana çıktığı uluslararası çok taraflı yönetişim modeli yerine, özel sektörün ön plana çıktığı ve internetin işleyişini yürütme ve denetleme sorumluluğunu ICANN'in devraldığı bir model geliştirilmiş oldu. Bu modelin ABD hükümetinin kasıtlı bir hamlesi olduğu iddia edilmiştir (Mueller vd., 2007, s. 240). Benzer şekilde, ICANN'in "siber özgürlükçü" bir yaklaşıma sahip olduğu iddia edilmektedir. ICANN'in temel özelliği, aşağıdan yukarıya bir yöntemi benimseyerek yayılması ve çalışmasıdır. Bu yöntem; devlet, özel sektör, sivil toplum ve teknik topluluğun internet politikalarını belirlemek için birlikte çalışmasına imkân tanımaktadır. İnternetin bu şekilde yönetilmesi, yalnızca ABD tarafından değil, aynı

zamanda özgür, açık, sınırsız ve güvenli bir interneti için ortak norm ve kuralların oluşturulması gerektiğini savunan Batılı ülkeler tarafından da benimsenmiştir.

ICANN'in interneti "açık" tutmadaki başarısı, ABD yönetiminin desteğiyle mümkün olmuştur. Ancak ICANN, ABD dışındaki devletlerin ulusal veya bölgesel çıkarlarını temsil etmediği gerekçesiyle eleştirilmektedir. Dahası, ICANN ve ABD hükümetinin küresel iletişim endüstrisini tekeline aldığı iddia edilmektedir (Huston, 2004). Mueller vd., ABD'nin ICANN aracılığıyla kendisinin ve devlet dışı aktörlerin egemen olduğu bir yönetişim rejimini başarıyla kurduğunu ifade etmiştir (2007, s. 240).

BM'yi internet yönetişiminden sorumlu kuruluş olarak görmek isteyen ülkeler, ICANN'in şeffaflık ve hesap verilebilirlik ilkelerinden uzak otoriter bir yapıya sahip olduğunu savunmuşlardır. Bu doğrultuda ICANN'in çok uluslu bir yapı tarafından yürütülmesi konusundaki isteklerini sıklıkla dile getirmişlerdir. Nihayet 2011'de Obama yönetimi tarafından bu istekleri dikkate alınmıştır. 2014 yılında yönetim, ICANN'in IANA'nın sözleşmesini denetleme rolünü aşamalı olarak kaldırmaya yönelik planlarını açıklamıştır (Shapira, 2011). Bunun üzerine ABD Hükümeti, IANA işlevlerinin yönetim rolünü küresel çok paydaşlı bir topluluğa dönüştürme niyetini açıkça beyan etmiş oldu. NTIA, ICANN'den tüm paydaşların geçiş sürecinin kararlaştırılması için küresel bir tartışma düzenlemesini talep etmiştir; buna cevaben ICANN, süreci başlatmış ve kolaylaştırmıştır (ICANN, t.y). Sonuç olarak, ABD Ticaret Bakanlığı, DNS sistemi üzerindeki gücünü ve internet yönetiminin önemli bir bölümünü neredeyse 20 yıllık bir devretme süreci ile sona erdirmiş oldu.

ABD hükümeti, ICANN aracılığıyla önemli bir yetkiyi elinde bulundururken, temel politika oluşturma işlevlerini özelleştirmeyi ve uluslararası bir niteliğe kavuşturmayı başarmıştır. Zira ICANN, yukarıda belirtildiği üzere 1 Ekim 2016 tarihinde çok uluslu özel bir yapıya devredilmiştir. ICANN ve NTIA, 6 Haziran 2017'de ortak taahhüt beyanlarını resmen sona erdirmiştir.[67] ICANN ile ABD hükümeti arasındaki ilişki, Ekim 2016'da şu ifadelerle sonlanmıştır:

> Bugün, 1 Ekim 2016, İnternet Tahsisli Sayılar Kurumu (IANA) işlevlerini yerine getirmek için İnternet Tahsisli Sayılar ve İsimler Kurumu (ICANN) ile Amerika Birleşik Devletleri Ticaret Bakanlığı

[67] Yazışmalar için bkz: Strickling, L. E. to Crocker, S. (2017, January 6). *Letter from Lawrence E. Strickling to Dr. Stephen D. Crocker*. ICANN. https://www.icann.org/en/system/files/correspondence/strickling-to-crocker-06jan17-en.pdf.

> Ulusal Telekomünikasyon ve Bilgi İdaresi (NTIA) arasındaki sözleşme resmi olarak süresi doldu. Bu tarihi an, İnternet'in benzersiz tanımlayıcılarının koordinasyonunun ve yönetiminin özel sektöre geçişine işaret ediyor, bu süreç 1998'den beri devam ediyor (ICANN, 2016).

Huston'a göre (2004) ABD ile ICANN arasında sona eren bu ilişki, esasen dünyanın geri kalanına yıllardır ABD'nin küresel internet pazarında interneti geleneksel uluslararası yönetişim süreçlerinden mahrum bıraktığını göstermek için kullanılmıştır. Böylece halihazırda yerleşik olan ABD merkezli işletmelerin konumunun bu sayede güçlendirildiğini ima eden bir mesaj gönderilmiştir. Dönemin ICANN CEO'su Fadi Chehade, ABD'nin ICANN üzerindeki kilit rolünün sona erdirilmesine yönelik ABD Kongresinden eleştiriler yükseldiğini, ancak bu eleştirilerin "küresel yönetim"e (*global stewardship*) geçiş sürecini baltalayamayacağını ifade etmiştir (Phys.Org, 2015). ICANN'in ABD gözetiminden küresel topluluğu daha iyi temsil eden bir organa yönlendirilmesinin internet yönetişimi açısından daha yararlı bir adım olduğunun altını şu ifadelerle çizmiştir:

> Anlaşmanın bizi küresel, bağımsız, tarafsız, iyi yönetilen bir organizasyona yönlendireceğini düşünüyorum. Asla rahat değilim ama iyimserim ve tüm çıkarların dengelendiğine inanıyorum. Bunun mantıklı olduğunu herkes görüyor (Gazete Duvar, 2016).

Nitekim ABD, ICANN'in geçirdiği dönüşüm sürecinde kuruluşun hükümet gözetiminden bağımsızlığını korumasına önem vermiştir. ABD, internet yönetişimi konusunda devletlerin etkin bir rol oynamasını kabul ederken, aynı zamanda ICANN'in saygın bir danışma komitesi gibi hareket etmesi gerektiğini savunmuştur. Bu yaklaşım, özel sektörün internet yönetişiminde önemli bir pozisyon alması gerektiğine ve serbest piyasa prensiplerine dayalı, merkeziyetçi olmayan bir yönetişim anlayışının desteklenmesine işaret ediyordu. Bu bağlamda ABD, çok paydaşlılık modelini desteklemekle birlikte, bu modelin dış pazar dinamiklerinin etkisine açık olabileceği konusunda uyarıda bulunmaktadır (Taylor & Hoffmann, 2019, s. 8).

Sonuç olarak, internet yönetişimi konusundaki tartışmalar sıkça ICANN'e atıfta bulunsa da, bu yönetişimin kapsamı ICANN'in rolünden çok daha geniştir. Cerf'e göre (2004) ICANN, internetin küresel yönetişiminde önemli bir rol oynasa da, internet yönetişimi

çok daha geniş bir alandır ve çok sayıda aktörün katılımını gerektirir. Bu noktada Cerf, ICANN'in yetkilerinin ötesindeki politika konularının ele alınması için uluslararası işbirliğinin önemini vurgular. Zira ICANN, internetin küresel düzeyde gözetiminden sorumlu ana kuruluş olsa da, kuruluşun yetkileri ve kaynakları kasıtlı olarak sınırlı tutulmuştur, çünkü bu tür sorunların ulusal hükümetler veya kuruluşlar tarafından ele alınması hedeflenmiştir. Nitekim bu sınırlılıklar, ICANN'in spam, dolandırıcılık, hırsızlık ve pornografi gibi çeşitli sorunlarla başa çıkma kapasitesini kısıtlamaktadır. Oysa ki internetin küresel elektronik ticareti, dijital imzalar, online fikri mülkiyet koruması ve suçla mücadele gibi çeşitli alanlarda uluslararası prosedürlerin ve politikaların geliştirilmesi gerekmektedir.

4.1.3.3.Sorun Alanları

Çok paydaşlı formül ve "sürekli çok paydaşlı çabalar" ihtiyacı, WSIS'ten bu yana giderek daha fazla tartışılsa da, "çok paydaşlılık" henüz net ve konsensüse dayalı bir tanıma kavuşmuş değildir. Çok paydaşlı katılımcı yönetişim, birçok hükümetlerarası organizasyon tarafından resmi olarak onaylanmasına rağmen, WSIS'in farklı paydaşların katılımına dayalı kapsamlı bir internet yönetişimi rejimi oluşturmayı başaramadığı vurgulanmaktadır. WSIS, çok paydaşlı politika tartışmalarını teşvik etmede kilit bir rol oynayan IGF'nin kurulmasını sağlamış olsa da, çok paydaşlı işbirliğinin nasıl yapılandırılması gerektiği konusunda somut sonuçlar üretmek için henüz kesin bir cevap bulunamamıştır (Belli, 2015, s. 5).

WSIS'te yapılan tanımlamadan yola çıkacak olursak, çok paydaşlı yaklaşımların tartışmalı yönlerinin olduğunu görebiliriz. Özellikle WSIS'te kullanılan "kendi rollerinde" ifadesi bu kapsamda değerlendirilebilir. Yukarıda değindiğimiz üzere WSIS tarafından paydaşlara atfedilen rol ve sorumluluklar, internet yönetişiminin hem teknik hem de kamu politikası konularını ilgilendirmektedir. Tüm paydaşları kapsayan bu yaklaşım, Tunus Gündeminin 35. paragrafında onaylanmıştır. Her bir paydaş grubu için roller ve sorumluluklar ayrıntılı bir şekilde açıklanmıştır. İnternete dair uluslararası kamu politikası sorunları için politika otoritesi ve egemenlik hakkı devletlere ait kabul edilirken; özel sektör internetin teknik ve ekonomik alanlarda geliştirilmesinde önemli kabul edilmiştir. Uluslararası kuruluşlar, internet ile ilgili teknik standartların ve politikaların geliştirilmesi ile görevlendirilirken, sivil topluma özellikle topluluk düzeyinde rol atfedilmiştir. Buna karşılık hükümetlerarası kuruluşların ilgili kamu

politikası konularını koordine etmede "kolaylaştırıcı bir role" sahip olduğu ifade edilmiştir (ITU, 2005a, s. 17).

WSIS tanımının vaat ettiğini yerine getirip getirmediği noktasında da tartışmalar mevcuttur. Örneğin Kleinwächter, pratikte de WSIS'te yapılan tanımın gerektirdiği gibi internet yönetişim sürecinde tüm paydaşlara yer verildiğini belirtirken; WSIS, her ne kadar bütün paydaşların kendi rollerinde katılımlarını destekleyecek bir tanım yapmış olsa da, çok paydaşlılık üzerindeki tartışmaları ve rekabeti azaltamamıştır (2014, s. 17). Halen paydaşlar arasında internet yönetişiminin nasıl işlemesi gerektiğine dair çekişmeli bir süreç mevcuttur. Siber alana uygulandığı şekliyle çok paydaşlılık; yönetişimde kamu, özel sektör ve sivil toplumdan çok sayıda katılımcıyı içeren bir politika modeli olarak tanımlanmaktadır (Raymond & DeNardis, 2015, s. 610). Ancak pratikte küresel internet yönetişiminde çok paydaşlılık daha farklı bir biçimde işlemektedir.

Bazıları, çok paydaşlı internet yönetişiminin mevcut güç dinamiklerini pekiştirdiğini iddia etmektedir. Bu görüşe göre gücün önemli ölçüde yeniden dağıtılmasından ziyade, mevcut durum korunmaktadır. Örneğin devletler, internet yönetişiminde önemli bir güce sahiptir. Vatandaşlarını temsil etme meşruiyeti, onlara diğer paydaşlara kıyasla bir avantaj sağlar. Bu meşruiyet, devletlerin internet politikalarını ve düzenlemelerini dayatmalarına olanak tanır. Özel sektör de internet yönetişiminde önemli bir güce sahiptir. Ekonomik kaynakları ve teknik altyapısı, onlara önemli bir nüfuz sağlar. Özel sektör, internetin altyapısını ve platformlarını kontrol ederek önemli bir güce sahiptir. Sivil toplum, çok paydaşlı İnternet yönetişiminde nispeten daha az güce sahiptir. STK'lar genellikle kaynak eksikliği ve dağınıklık gibi sorunlarla karşı karşıyadır. Bu durum, diğer paydaşlar karşısında dezavantajlı olmalarına neden olur. Dolayısıyla çok paydaşlı internet yönetişimi modeli, mevcut güç dinamiklerini pekiştirmektedir. Devletler ve özel sektör, sivil topluma kıyasla daha fazla güce sahiptir. Sivil toplum, diğer paydaşların çıkarlarına hizmet eden bir rol oynamaktadır (Carr, 2015).

Bazı devlet dışı aktörler online ve fiziksel forumlarda yalnızca katılımcı olarak bulunurken; büyük güçler ve teknoloji şirketleri gibi daha baskın aktörler karar alma ve politika yapma sürecinde daha büyük bir etkiye sahip olabilmektedir (Carr, 2015, s. 650). Bu koşullar altında çok paydaşlı yaklaşımın paydaşlar arasındaki dengesizliği derinleştirdiği söylenebilir. Burada oluşan dengesizlik, en çok ülkelerin kendi

aralarındaki yapısal eşitsizliklerde kendini göstermektedir. Çalışmanın ikinci bölümünde daha detaylı bir biçimde ele alınacak olan bu konu, devletler arasında daha büyük çekişmelere neden olmakta ve etkili bir yönetişim mekanizmasının oluşturulmasının önünde engel teşkil etmektedir.

Çoğu durumda paydaşların çıkarlarının örtüşmediği görülmekte ve bu durum yeni sorun alanları yaratmaktadır. Örneğin Mueller, DNS sistemi üzerindeki mülkiyet hakları çatışmalarının çözümünün önündeki başlıca engellerden biri olarak aktör çeşitliliğini görmektedir (2004, s. 68). Bu tartışmadaki aktörler; internet teknik topluluğu, mevcut alan adı ve adres kayıtları, tescil memurları, ticari marka ve fikri mülkiyet hakları, internet servis sağlayıcıları, insan hakları grupları, hükümetlerarası kuruluşlar ve ulusal hükümetlerden oluşmaktadır. Paydaşların görüşleri konudan konuya değişiklik gösterebilmektedir. Fakat internet yönetişiminde farklı beklentiler, çelişkili çıkarlar ve farklı yaklaşımlar sabit kalmaktadır. IGF'nin karşı karşıya kaldığı zorluklardan biri, farklı aktörlerin ortak bir paydada buluşabilecekleri bir alan sağlamaktır. Bu nedenle "çok paydaşlı diyalog" aracılığıyla bir anlaşma yapmak oldukça zor bir süreçtir. Tüm ilgili taraflar üzerinde uygulanabilecek bağlayıcı nitelikte herhangi bir anlaşma, uluslararası hukuk da dahil olmak üzere uluslararası sistemde yenilik gerektirmektedir.

Devlet paydaş grubu içindeki gelişmiş ve gelişmekte olan ülkeler arasında farklılıklar mevcuttur. Benzer şekilde özel sektör paydaş grubunda da arz ve talep bakımından işletmeler arasında farklılıklar bulunmaktadır. Dolayısıyla temsilci olarak gönderilen aktörlerin yalnızca hangi paydaş sektöründen oldukları değil, nitelikleri de önem arz etmektedir (van der Spuy, 2017, s. 27). Bunu gösteren bir örnek, UNESCO'nun 2015 yılında gerçekleştirilen "Noktaları Birleştir" konferansıdır. Burada bazı katılımcılar çok paydaşlı katılımın tanımında özgüllük olması gerektiğini dile getirmiştir. Bunun yanında, çok paydaşlı katılımın "demokratik" olarak tanımlanması gerektiğini savunanlar da olmuştur. Konferans katılımcılarının çoğu, çok paydaşlı modelin mevcut konulara bağlı olarak değişiklik gösterebileceğini ifade etmişlerdir. Örneğin bazı konularda teknik uzmanların öne çıkması gerekirken, bazı konularda sivil toplum veya devletler öne çıkmalıdır. Burada esasen çok paydaşlı katılımda "rol" esasına göre bir ayrım yapıldığı söylenebilir. Burada önemli olan, demokratik temsil konusunda bir denge sağlanmasıdır. Bu şekilde kaynaklara sahip olmayan bireylerin ve grupların görüş bildirmeleri mümkün olacaktır (UNESCO, 2015, s. 33). Zira bu tür demokratik

süreçlerde farklı çıkarlara eşit erişim imkânı sağlanmaktadır. Burada amaç; tek bir sektörün, çıkar grubunun veya basit çoğunluğun kararlarının uygulanması yerine, bütün katılımcıların çıkarlarının gözetildiği bir karar mekanizmasının oluşturulmasıdır. Elbette bu durum, internet yönetişiminin bütün safhalarında uygulanabilecek bir yöntem değildir. Fakat bu tür uygulamaların birçok durumda etkili olduğu bilinmektedir (van der Spuy, 2017, s. 27).

Bu rol ve sorumluluklar zamana bağlı olarak farklılık arz etse de yönetişim sorununu derinleştirmektedir. Zira bu paydaşlar; politikalar, normlar ve kurallar gibi faktörlerin geliştirilmesi ve uygulanmasında rollerini kendi çıkarları doğrultusunda kullanabileceklerdir. Bu nedenle internet yönetişiminde aktörlerin her birine ayrı bir konuda otorite sağlanmasını yararlı bir formül olarak görmeyen yazarlar mevcuttur. Dolayısıyla çok paydaşlı süreçlerdeki esneklik ve paydaşlara atfedilen rol ve yetkilerin genişliği, internet üzerindeki etki alanıyla uyumlu olarak kabul görmemiştir (van der Spuy, 2017, s. 28). Zira farklı paydaşlar arasında güç dengesizliği, modelin işleyişini zorlaştırmaktadır. Özellikle özel sektörün artan gücü ve sivil toplumun zayıf temsili, modelin meşruiyetini zedeleyebilir. Ayrıca, çok paydaşlı modelin karar alma süreçlerini karmaşıklaştırdığı ve gecikmelere yol açtığı da savunulmaktadır (Carr, 2015).

İnternet yönetişimine yönelik çok paydaşlı yaklaşımların yarattığı diğer bir zorluk, paydaşların bazı alanlarda çok paydaşlı katılım fikrini desteklerken; bazı alanlarda kendi hakimiyetlerini savunmalarıdır. Devletler bazı konularda çok paydaşlı katılımı teşvik ederken; özellikle siber güvenlik politikası konularında tek taraflı karar verme eğilimindedir. Özel paydaşlar bazı durumlarda çok paydaşlı mekanizmalara katılıma ihtiyaç duymayacak kadar güç kazanırlar. Bu nedenle, önemli kararların büyük çoğunluğu özel paydaşlar tarafından alınmaktadır. Bu durum genellikle devletlerin özel sektörle işbirliği yapmasıyla sonuçlanmaktadır. Süreç, normatif düzeyde bile olsa vatandaşları terörizmden koruma adı altında devletler ve özel şirketler arasındaki gizli işbirliğiyle işlemektedir. Bu durum, çoğu zaman serbest bilgi akışını kısıtlayabilecek veya gizlilik hakkını ihlal edebilecek gizli gözetim mekanizmalarının kullanılmasına kadar varabilmektedir (van der Spuy, 2017, s. 31).

Sonuç olarak çok paydaşlılık, internet yönetişiminde başından beri kritik bir rol oynamıştır. Ancak, WSIS sonrası ortaya çıkan model, artık yıpranmış ve eski

görünmektedir.[68] Bu durum, paydaş kategorizasyonunun yeterince detaylandırılmamasından kaynaklanmaktadır. Ayrıca, internetin henüz erişim sağlayamayan ancak internetin toplumsal değişimleri tarafından etkilenen kesimler de göz ardı edilmiştir. İnternet yönetişimindeki karar alma mekanizmaları, talep tarafından ziyade arz tarafına ve "içerideki" aktörlere doğru bir eğilim göstermektedir (Souter, 2021). Bu durum, paydaşların ve kaynaklarının değişken doğası ile daha da karmaşıklaşmaktadır. Küresel şirketler, etkileşimlerini maksimize etmek için büyük miktarda kaynak ayırabilmekte, birçok önemli karar, yönetim kurulu odalarında veya şirketler ile devletler arasında yapılan gizli müzakerelerle alınmaktadır. İnternetin kendisi de evrim geçirmiştir ve pek çok konu, hem çok taraflı hem de çok paydaşlı bir katılımı zorunlu kılmaktadır.

4.1.4. Çok Taraflılık (*Multilateral*) Modeli

İnternet yönetişimi, küresel düzeyde önemli bir tartışma konusu olmasına rağmen bu alandaki bazı yaklaşımlar, devletlerin ulusal güvenliği, ekonomik çıkarları ve sosyal normları çerçevesinde şekillenmektedir. Özellikle çok taraflı modelin savunucuları, devletlerin ve hükümetlerarası kuruluşların internet yönetişiminde daha baskın bir rol oynaması gerektiğini öne sürmektedirler. Bu model, ABD'nin mevcut çok paydaşlı ve Amerikan siber hegemonyasına hizmet eden modeline karşı bir alternatif olarak görülmektedir. Çok taraflı modelin savunucuları, genellikle BM kurumları da dahil olmak üzere çeşitli kanallar aracılığıyla hükümetlerarası bir model oluşturmaya çalışmışlardır (Ebert & Maurer, 2013, s. 1059). Bu yaklaşım, başta Rusya ve Çin gibi büyük güçler olmak üzere benzer düşünen bir grup devlet tarafından desteklenmiştir. Bu devletler, siber uzayda kontrolü sağlamak amacıyla ITU gibi uluslararası kurumlarla stratejik ilişki geliştirme yoluna gitmiştir. Amaçları, ABD'nin internet yönetişimi üzerindeki gücünü ve yetkisini sınırlandırmaktır. Bu doğrultuda ABD'nin güç aldığı kurumları uluslararası bir hükümet kuruluşuna devrederek ABD'nin hegemonyasını sonlandırmayı amaçlamışlardır.

Bu devletler, internet yönetişiminde daha fazla eşitlik talep etmişlerdir. Bu bağlamda, Brezilya Cumhurbaşkanı Dilma Rousseff, 2014 yılında Sao Paulo'da düzenlenen NETmundial toplantısında küresel internet yönetişiminin yeniden değerlendirilmesi

[68] Ayrıca bkz: WSIS. (2003). *Declaration of Principles: Building the Information Society: A Global Challenge in the New Millennium*. International Telecommunication Union. https://www.itu.int/net/wsis/docs/geneva/official/dop.html.

çağrısında bulunmuştur. Rousseff, tüm devletlerin "eşit" katılımını savunmuştur. Bu talep, internetin küresel bir kaynak olması ve tüm devletlerin bu kaynakta eşit haklara sahip olması gerektiği fikrine dayanmaktadır. Ayrıca, ABD'nin internet üzerindeki hâkim gücüne karşı bir denge unsuru oluşturmak için de görülmektedir (Carr, 2015).

Çok taraflı modelin destekçileri, aynı zamanda, devletlerin internet gibi önemli bir alanı yönetmede sivil toplum kuruluşlarından veya özel sektörden daha fazla meşruiyete sahip olduğunu savunurlar. Bu yaklaşım, 'siber uzay egemenliği' fikrini savunur ve bunu diğer ülkelere de ihraç etmeye çalışır (Hoxtell & Nonhof, 2019, s. 11). Özellikle, Çin ve Rus hükümetleri, ABD'nin algılanan teknolojik ve yönetişim hegemonyasına karşı 'İnternet egemenliği' yaklaşımını savunmaktadır (Budnitsky & Jia, 2018). Çin'in WSIS sırasında ulusal hükümetlerin internetin yönetişimine katılması gerektiğini öne sürmesi ve "devlet öncülüğünde, çok partili katılım" ilkesini savunması, internet yönetişiminde çok taraflı bir yaklaşımın önemini vurgulamaktadır. Bu yaklaşım, ABD'nin "tek taraflı sistemi" ve ICANN ile olan sözleşmeye dayalı ilişkisi ile zıtlık oluşturur. ICANN'in yetkileri ve ABD Ticaret Bakanlığı ile olan ilişkisi, ICANN'in aslında sınırsız yetkiye sahip bir ulusal hükümet tarafından kontrol edildiğini ima eder (Zhang vd., 2020, s. 2309).

Hindistan, bu aktörler arasında yer alarak, ulus devletlerin küresel internet yönetişiminde "temel bekçiler" olarak hizmet ettiği bir modeli tercih eden devletlerden biri olarak öne çıkmaktadır. Bu model, hükümetlerarası kuruluşların etkinliğinin devam ettiği bir yaklaşımı desteklemektedir (Murthy, 2014, s. 5). Hindistan da, 2011 ve 2014'teki müzakerelerde, BM sistemi içinde uygun bir mekanizma oluşturulmasını savunan gelişmekte olan ülkelerle birlikte hareket etti. Hindistan, Sao Paulo'daki ikinci zirvede, devlet egemenliğinin önceliğine ve dezavantajlı ülkelere kapasite geliştirme desteği sağlanmasına bağlı olacak hükümetlerarası bir organın kurulmasını önerdi. Ancak, Hindistan'ın bu yaklaşımı, Batılı eleştirmenler tarafından paradoksal bulundu. Eleştirmenler, Hindistan'ın demokratik ve açık bir toplum olmasına rağmen, çok paydaşlı yaklaşım yerine devlet liderliğindeki çok taraflı bir yaklaşımı tercih etmesini eleştirdiler (Murthy, 2014, ss. 10-11).

Bu bağlamda BRICS grubu, altyapı geliştirme, yasal düzenlemeler, ekonomik konular, kalkınma ve sosyal ve kültürel perspektifler gibi internet yönetişiminin beş temel alanında katılımcı ülkelerin çıkarlarını uyumlaştırmak için uygun bir platform olarak

görülmektedir. Ancak, BRICS ülkeleri arasında internet içeriğinin yönetimi konusunda önemli farklılıklar bulunmakta, bu da internet yönetişiminin sosyal ve kültürel yönlerine ilişkin somut kararların eksikliğine katkıda bulunmaktadır. Ayrıca, terörle mücadele ve aşırıcılıkla mücadele gündemi, daha geniş bir siber güvenlik sorunuyla giderek daha fazla örtüşmektedir. BRICS, internet yönetişiminde önemli bir rol oynama potansiyeline sahiptir. Ancak, katılımcı ülkeler arasındaki çıkar çatışmaları ve önceliklerdeki farklılıklar, grubun etkin bir şekilde işbirliği yapma ve küresel internet yönetişiminde önemli bir rol oynama yeteneğini etkileyebilmektedir (Ignatov, 2022).

4.1.4.1.Egemenlikçi Yaklaşımlar

Fiziksel alandaki egemenlikçi yaklaşım, siber alanda da kendini göstermektedir. Bu durumu "dijital milliyetçilik" (*digital nationalism*) olarak adlandıran yazarlar mevcuttur (Budnitskiy, 2018, s. 102). Westphalian devlet egemenliği ilkesi burada da geçerli kabul edilmektedir. Demchak ve Dombrowski'nin (2013) öne sürdüğü "siber-westphalian çağı" kavramı, devletlerin artan siber güç kullanımı ile siber uzayda yeni sınırlar çizme eğilimi üzerine kuruludur. Bu, 1648 Westphalia Antlaşması'nın ardından uluslararası sistemde çizilen fiziksel sınırların bir benzerinin, siber uzayda da oluşturulacağı bir dönemin başlangıcını işaret edebilir. Bu durum, siber uzayın güvensizlik ve çatışmanın hâkim olduğu bir alan haline gelmesine yol açmakta ve bilgi paylaşımını olumsuz etkilemektedir. Özellikle, Çin ve Rusya gibi devletler, siber egemenlik kavramını benimseyerek, internet üzerindeki kontrolü artırmaya yönelik adımlar atmışlardır. Bu, Çin'in Büyük Güvenlik Duvarı ve Rusya'nın internet sunucularını yerelleştirme çabaları gibi girişimlerle örneklendirilebilir.

Bu yaklaşım, internetin küresel erişimini kabul ederken; ulus-devletleri ve ulusal yasaları internetin yöneticileri olarak kabul etme eğilimindedir. Bunun yanında, hükümetlerarası kuruluşların ve uluslararası hukukun küresel internet yönetişiminin temelini oluşturması gerektiğini savunmaktadır. Çok taraflılık olarak bilinen bu yaklaşım, çok paydaşlılığa karşı olmasa da, farklı bir şekilde yorumlanmaktadır. Çok paydaşlılık, internet özgürlüğünü (*internet freedom*) savunurken; çok taraflılık, internet egemenliğini (*internet sovereignty*) savunmaktadır. Diğer yandan, çok paydaşlı yönetişim modeli, kamu, özel sektör ve sivil toplum gibi tüm paydaşların politika yapımına eşit katılımını savunurken; çok taraflılık modeli, devlet dışı aktörlerin müzakere süreçlerine katılımını meşru bir hak olarak tanımlar ancak bağlayıcı politika kararlarının ulus-devletlerin yetkisinde olduğunu savunur (Budnitskiy, 2018, s. 102).

Egemenlikçi model, ITU gibi hükümetlerarası bir kuruluş aracılığıyla Westphalian egemenlik kavramını tezahür etmeye çalışmakta ve siber uzay üzerinde bölgesel kontrol oluşturmayı amaçlamaktadır (Ebert & Maurer, 2013, s. 1060). Özellikle Rusya, yıllardır mevcut çok paydaşlı model içindeki "politika boşluğunu" ve "kurumsal boşluğu" sık sık dile getirmekte ve protesto etmektedir. Kendisiyle benzer düşüncede olan devletleri arkasına alan Rusya, ağın yönetişimi üzerindeki mevcut katılım dengesini değiştirerek devlet egemenliğini yeniden gündeme getirmeyi amaçlamaktadır (Nocetti, 2015, s. 117).

Rusya ile aynı "katı" modeli savunan Çin de bu talebini önemli platformlarda dile getirmiştir. Kasım 2014'te Wuzhen Zirvesi olarak da bilinen Dünya İnternet Konferansı'na ev sahipliği yapan Çin, küresel internet sorunlarının ve politikalarının tartışıldığı bu platformda talebini yinelemiştir. Çin Devlet Başkanı Xi, karşılıklı saygı ve güven koşulları altında Çin'in barışçıl, şeffaf ve çok taraflı olarak yönetilen bir siber uzay için daima işbirliğine açık olduğunu ifade ederken; bunun ancak "egemenliğe tam olarak saygı gösterilmesi" koşuluyla mümkün olabileceğinin altını çizmiştir (Desheng, 2019). Bu amaçla Çin Devlet Başkanı, mevcut uluslararası internet yönetişim sistemini dört ilkeye "siber egemenlik, açıklık, işbirliği ve iyi düzene saygı" olmak üzere dört ilke temelinde reform yapmaya davet etmiştir (Chuanying, 2016).

2015 yılında düzenlenen İkinci Dünya İnternet Konferansı, birincisinden daha hararetli tartışmalara yol açmıştır. Konferansın açılış konuşması sırasında Başkan Xi, "ortak kadere sahip bir siber topluluk oluşturma, siber egemenliğe saygı, siber güvenliği koruma ve siber düzeni inşa etme ilkelerini ortaya koyma" çağrısında bulunmuştur (BBC News, 2015). Bunun yanında, "internet egemenliği " modelini destekleyerek uluslararası toplumu "her ülkenin kendi internet yönetim modelini seçme hakkına saygı göstermeye" davet etti. Xi, her ne kadar tek taraflılığı reddeden çok taraflı bir yaklaşıma dayalı bir internet yönetişim sistemi kurmayı önerdiğini iddia etse de, yaklaşımı teknoloji şirketlerine bir meydan okuma olarak algılandı. Bunun üzerine Uluslararası Af Örgütü, internette sansürü teşvik etmeye çalışması gerekçesiyle teknoloji şirketlerini Çin'in bu tutumuna karşı çıkmaya davet etti (Amnesty International, 2015). O dönemden bu yana egemenlikçi modeli savunan Çin ile özgürlükçü modeli savunan uluslararası kuruluşlar arasındaki gerginlik ve uzlaşmazlık artarak devam etmektedir. Li (2015), Xi yönetiminde ideolojik taleplerin daha agresif

olduğunu ve sansürleme yöntemiyle eleştirel kamuoyunu bastırılmaya çalışıldığının altını çizmiştir.

Özellikle Covid-19 süreci ile birlikte Uluslararası Af Örgütü, yayınladığı raporlarda Çin'in internet üzerinde uyguladığı sansüre yönelik sert eleştiriler yapmaktadır.[69] Benzer şekilde Freedom House'ın "China: Freedom on the Net 2020 Country Report" isimli raporunda Çin'deki internet kullanıcıları için koşulların günden güne daha da kötüleştiğini ifade edilmiş; ülkenin üst üste altıncı yıldır internet özgürlüğü konusunda dünya sıralamasında en aşağıda olduğu teyit edilmiştir.[70]

Egemenlikçi modelin savunucuları, mevcut statükodan memnuniyetsizliklerini bütün platformlarda dile getirmektedir. Bu modelin savunucuları, siber uzay üzerinde devlet kontrolünü artırmayı ve interneti devletlerin iç meselesi olarak görerek burada "müdahale etmeme" ilkesini geçerli kılmayı hedeflemektedir (Chuanying, 2016). Yukarıda sayılan devletler bağlamında bir değerlendirme yapılacaksa, uluslararası alanda ITU gibi BM kuruluşları aracılığıyla, bölgesel alanda ise ŞİÖ gibi kuruluşlar aracılığıyla bu hedefe ulaşmaya çalışmaktadırlar.

4.1.4.2.ITU'nun Rolü

İki model arasındaki en büyük çatışma alanı, DNS sorumluluğunun ICANN'den ITU'ya devredilmesidir. ITU'nun DNS'yi ICANN'den daha demokratik bir şekilde yönetebileceği iddia edilmektedir (Hoxtell & Nonhof, 2019, s. 12). Bu modelin savunucuları için ITU, kendi internet yönetişim hedeflerine ulaşmaları için en iyi araçtır. Model, çok paydaşlı, merkezi olmayan mekanizmayı reddederek daha "gelenekselci" bir anlayışla hareket etmektedir. Burada amaç, yönetişim için gerekli hamle ve tedbirlerin ulusal araçlarla alınması ve bu sayede ulusal çıkarların dengelenmesidir (Huston, 2004). Onlara göre kamu iletişimi, bir kamu sektörü faaliyetidir. Bu nedenle denetimi, ulusal ve uluslararası düzenleyici rejimler tarafından yürütülmelidir. Bu bağlamda ITU, tarihsel olarak telekomünikasyon sektörüyle bağlantılı hükümetlerarası bir kuruluş olarak en uygun mekanizmadır. Aynı zamanda ITU'yu, uluslararası telekomünikasyon sektörü üzerinde tekel oluşturan ABD'nin konumunu değiştirebilecek en uygun oluşum olarak görmektedirler.

---

[69] Rapor için bkz: Amnesty International. (2021). *Amnesty International Report 2020/21: The State of the World's Human Rights*. https://reliefweb.int/sites/reliefweb.int/files/resources/pol1032022021englısh.pdf (20.04.2021).

[70] Freedom House. (2020). *China Overview*. Freedom House. https://freedomhouse.org/country/china/freedom-net/2020 (20.04.2021).

ITU, 1990'ların sonunda WSIS fikrini başlatarak Minnesota'daki 1998 tarihli Tam Yetkili Temsilciler Toplantısı'nda (*Plenipotentiary Meeting*) 73. Kararı kabul etti. Karar, ITU'yu BM bünyesinde telekomünikasyon ve internet konularının tartışılacağı uluslararası bir zirve düzenlemeye yönlendirdi. ITU'nun böyle bir karar almasının gerekçesi, küresel olarak telekomünikasyon yapılarının büyümesi ve telekomünikasyonun siyasi, ekonomik, sosyal ve kültürel düzeylerde giderek daha belirleyici bir rol oynamasıdır. Kararda ITU kendisini "telekomünikasyon sektörünün gelişimini sağlamak için en uygun yolları arayan kuruluş" olarak tanımlamıştır (Hubbard & Bygrave, 2009, s. 214).

ITU'nun attığı ilk adımlardan biri, Dubai'de düzenlenen WCIT-12'de Uluslararası Telekomünikasyon Yönetmelikleri'ni (International Telecommunication Regulations – ITR's) 549 değiştirmeye çalışmasıdır (Orji, 2018, s. 109). Böylece ITU, internet yönetişiminin geleceği ile uluslararası angajman sürecini başlatmıştır. En son 1988'de Melbourne'da müzakere edilen ITR's, uluslararası telekomünikasyonun sağlanması ve işletilmesi için genel ilkeleri tanımlamaktadır. Dubai Konferansı sırasında uluslararası mobil dolaşım, numaralandırma, adlandırma, dolandırıcılığın ele alınması ve internet gibi konularda önerilen birkaç değişiklik tartışıldı. ITR'lerin revize edilmiş versiyonu tamamlandı, ancak katılan 151 eyaletten yalnızca 89'u tarafından imzalandı. Bu devletler grubu, çoğunlukla Rusya, Çin, Brezilya ve Arap Devletlerinin önderlik ettiği gelişmekte olan ülkelerden oluşuyordu (WCIT, 2012). ABD, Japonya, Avustralya, Birleşik Krallık ve Avrupa ülkelerinin çoğu önerilen değişiklikleri reddetti. Dubai Konferansı öncesinde çok paydaşlı modelin destekçileri, ITU ve bazı üyelerinin Konferansı "inovasyon, ticaret, kalkınma, demokrasi ve insan hakları için korkunç sonuçlar doğuracak şekilde internet yönetimini devlet ve hükümetlerarası mekanizmalar aracılığıyla denetim altına almak" için düzenlediğini ifade etmişlerdir (Fidler, 2013a).

WCIT-12, sonraki toplantılarda uluslararası toplum arasındaki sürtüşmeleri gün yüzüne çıkarmış ve internet yönetişimi konusundaki anlaşmazlıkları ve bölünmeleri derinleştirmiştir (Coşkunoğlu, 2014). Özellikle Mayıs 2013'te ITU Dünya Telekomünikasyon Politikası Forumu ve 2014'te Güney Kore'de düzenlenen ITU Tam Yetkili Temsilciler Konferansı'nda (Busan Konferansı olarak da bilinir) bunun olumsuz etkileri açıkça hissedilmiştir. Busan Konferansı'nda internetin teknik protokollerinin tasarımı ve işletilmesinde ITU'nun yetkilerinin genişletilmesi girişimi başarısız

olmuştur. Çok sayıda ülke internet organizasyonu ile ilgili değişiklikler önerirken; bu değişikliklerin hiçbiri, Batılı devletlerin ağ uzmanlarının "ılımlı baskısı" nedeniyle gerçekleştirilemedi (McCarthy, 2014). Bütün girişimlerine rağmen ITU, 19. yüzyılın sonlarından beri telekomünikasyonda olduğu gibi, kendisini internetin birincil düzenleyicisi olarak konumlandıramamıştır (Take, 2012, s. 506).

WCIT-12, küresel internetin çeşitli gruplar tarafından yönetilmeye devam edeceğini açıkça göstermiştir. Bunun yanında, devletlerin kendi bölgelerindeki ağ altyapısına karar vermede öncü bir role sahip olduğunu, ancak devletlerin yalnızca karar alma sürecinin bir parçası olduklarında internetin en iyi şekilde yönetilebileceğini vurgulamıştır (McCarthy, 2014). Bu aşamada ITU'nun gelecekte internetin gelişimi ve yönetişiminde oynayabileceği rolü tahmin etmek zordur. Esasında bu durum, 2016'da ABD hükümetinin DNS üzerindeki kontrolü tamamıyla ICANN'e devretmesiyle daha da zorlaşmıştır. Zira egemenlikçi modelin savunucuları, artık ABD'nin ICANN üzerinde sağladığı kontrolü bir "koz" olarak kullanamamışlardır.

Sonuç olarak baskıcı rejimler, internet üzerinde küresel kontrol sağlanması ve ITU'nun katılımı için büyük bir baskı yapmaktadır. Post (2014) gibi eleştirmenlere göre, birçoğu hala "devlet tekel telefon ağına" bağlı olan devletlerin mevcut interneti kopyalaması veya yönetmesi mümkün değildir. Ona göre bu devletlerin interneti çoğunluk oyuyla BM tarzı herhangi bir organ aracılığıyla yönetebilmesi de ihtimal dahilinde değildir. Bu görüşlere rağmen, internet yönetişiminde devletlerin ve hükümetlerarası kuruluşların rolüne ilişkin tartışmaların devam edeceği söylenebilir. Bu bağlamda küresel yönetişim ve hukukun entegrasyonu, özellikle siber alanın hızla genişlemesiyle, BM gibi kurumların önemi ve rollerinin yeniden değerlendirilmesini gerektirmektedir. Bu noktada BM, küresel internet yönetişimi konularında bir "köprü kurucu" olarak hareket etse de, nihai olarak görevi çok paydaşlı modeli esas kalan kurumlara ve platformlara devretmelidir.

4.1.5. Alternatif Yaklaşımlar: Rejim Kompleksi Modeli

Joseph Nye (2014) tarafından kaleme alınan "The Regime Complexes for Managing Global Cyber Activities" başlıklı makale, siber yönetişim için bir çerçeve önermektedir. Nye, rejim kompleksi teorisi adını verdiği bu çerçeveyi önerirken, hem uzmanı olduğu liberal kuramsalcılık teorisini hem de Keohane ile birlikte geliştirdiği karmaşık karşılıklı bağımlılık teorisini esas almaktadır (Akyeşilmen, 2018a, s. 273). İnterneti ve

siber faaliyetleri küresel olarak yöneten çok yönlü ve birbirine bağlı bir çerçevenin ana hatlarını çizdiği çalışmasında, siber alanın yönetişimi ve düzenlenmesine toplu olarak katkıda bulunan çeşitli aktörleri, anlaşmaları ve kurumları kategorize etmektedir. Siber uzayın müdahale olayları, kolluk kuvvetleri, uluslararası standartlar, uluslararası hukuk gibi her biri kendi kuralları ve aktörleri bulunan bir dizi alt rejim içerdiğini ve bu durumun bir "rejim kompleksi" oluşturduğunu belirtir (2014, s. 8).

Bu rejim kompleksi, Nye'a göre, gevşek bir şekilde birleştirilmiş rejimler dizisidir ve küresel siber faaliyetlerin yönetişiminin merkezi olmaktan ziyade çok çeşitli aktör ve kurumlara dağılmış olduğunu ifade eder. Bu merkezi olmayan yapı, siber yönetişimin karmaşıklığını ele almak için çeşitli paydaşlar arasında işbirliği, diyalog ve fikir birliği oluşturma gerekliliğine işaret etmektedir (2014, s. 7). Raymond ve DeNardis, Joseph S. Nye'ın öncülük ettiği düşünceleri temel alarak, uluslararası siber alanın yönetişimi üzerine derinlemesine bir inceleme sunar. Nye, sınırlı internet yönetişiminden çok daha geniş bir siber rejim kompleksine doğru analitik bir geçiş yapılmasını önermiştir. Bu kompleks, tanımladığı dört aktör sınıfını kapsayarak, çok paydaşlı yönetişimin bir örneği olarak öne çıkar. Raymond ve DeNardis, Nye'ın bu çerçevesini genişleterek, bir rejim kompleksinin, örtüşen üyeliklere ve konulara sahip, birden fazla konuya özgü rejimlerin yanı sıra, bireysel rejimler arasındaki "sorunlu etkileşimleri" de içermesi gerektiğini vurgular (2015, s. 579).

Özellikle dar bir İnternet yönetişim rejiminin daha geniş bir siber rejim kompleksine gömülü olarak ele alınmasının daha faydalı olacağını savunan Nye, farklı konu alanlarındaki rejimler arasındaki etkileşimlerin ve bağlantıların önemine dikkat çeker. Raymond, Nye'ın bu yaklaşımının, uluslararası rejimler arasındaki karmaşık ilişkileri ve bu rejimlerin üstesinden gelinmesi gereken çatışmaları anlamada bir adım ileri olduğunu belirtir. Ancak, siber rejim kompleksinin henüz oluşum aşamasında olduğunu ve bu nedenle farklı sorun alanlarında yerleşik kurallar ve kurumlar arasındaki etkileşimlerin nasıl yönetileceğinin hala bir soru işareti olduğunu da vurgular. Bu bağlamda, Raymond, Nye'ın teorisinin uluslararası rejimler arasındaki etkileşimleri ve çatışmaları çözme çabalarına katkıda bulunabilecek önemli bir çerçeve sunduğunu, ancak bu sürecin karmaşıklığı ve belirsizliği nedeniyle karşılaşılan zorluklara da işaret eder (2016b, s. 83).

Radu, Nye'ın rejim kompleksi modeline yönelik önemli eleştiriler getirir. Nye'ın analizi ve rejim kompleksi çerçevesi, internet yönetişimine uygulanırken örgütsel altyapıyı ve rejim komplekslerini oluşturan ağlardaki önemli 'düğümleri' tanımlama konusunda yetersiz kalmaktadır. Bu, Nye'ın teorisinin, internet yönetişimi alanındaki spesifik yapıları ve aktörleri yeterince dikkate almadan, genel bir çerçeve sunma eğiliminde olduğunu işaret eder. Ayrıca, rejim değişikliklerinin nasıl gerçekleştiğini açıklama konusunda da Nye'ın teorisinin zorluklar yaşadığını belirtir. Radu, rejim değişiminin politika alanlarının genişletilmesi yoluyla gerçekleştiğini öne süren Helfer'e (2009) atıfta bulunarak, bu sürecin internet yönetişimi alt alanlarında nasıl işlediğine dair bir belirsizlik olduğunu vurgular. Bu eleştiriler, Nye'ın rejim kompleksi teorisinin uygulanabilirliği ve detaylı analiz kapasitesi konusunda önemli soru işaretleri ortaya koymaktadır (2019, s. 20).

Nye, rejim kompleksini "gevşek bir şekilde birleştirilmiş rejimler dizisi" olarak ifade ederken, bu kavram tek bir hukuki araçla yönetilen yapılarla, parçalı düzenlemelere dayalı yapılar arasında, orta düzeyde bir konumlandırma sunar (2014, s. 7). Siber uzayın yönetişimi bağlamında, rejim kompleksi; tek bir rejimin olmaması, birleşik bir kurumun veya tanımlanabilir bir çekirdeğin eksikliği ve hiyerarşik kurallar yerine çeşitli uygulamalar ve kurumlar arasında gevşek bağlantılarla düzenlenen oldukça parçalanmış bir norm ve kurumlar dizisi olarak karakterize edilir. Bu tanım, siber uzayın karmaşık doğasını ve yönetişimindeki çoklu aktörler ve çıkarlar arasındaki etkileşimi yansıtır (Demir, 2018, s. 35). Bu ifade, siber uzayın yönetişiminin hem ulusal hem de çok taraflı yaklaşımları içeren bir yapıda olduğunu ve bu yapıların birbiriyle nasıl etkileşimde bulunduğunu anlamak için kullanışlı bir çerçeve sunuyor gibi görünebilir; ancak, bu yaklaşım, siber uzay yönetişimiyle ilgili güç dinamiklerini ve eşitsizlikleri yeterince ele almadığı için eleştiriye maruz kalabilir.

Nye, ulusal ve çok taraflı yaklaşımlar arasındaki basit ikiliği eleştirirken, siber yönetişimin farklı aktörlerin etkileşimiyle şekillenen karmaşık bir rejim olduğunu savunur. Fakat Nye, farklı paydaşlar arasındaki güç dinamiklerini ve eşitsizlikleri yeterince ele almadığı için eleştirilebilir. Ayrıca, teknolojik değişimlerin düzenleyici çerçeveleri nasıl aştığına dair derinlemesine bir analiz sunmaktan da kaçınır. Dijital teknolojilerin sürekli bir dönüşüm sürecinde olması ve yönetişim yapılarının bu dönüşüme uyum sağlayamaması düzenleyici bir boşluğa sebebiyet vermektedir. Bu durum, güvenlik, gizlilik ve dijital eşitsizlik gibi konularda mevcut sorunları

derinleştirebilir ve yönetişim modellerinin bu çağdaş zorlukları nasıl ele aldığına dair şüpheler uyandırabilir. Sonuç olarak, Nye'ın çalışması, siber yönetişimde güç dinamikleri, teknolojik değişimlerin getirdiği zorluklar ve siber uzay yönetişiminde adalet ve eşitlik meseleleri üzerine daha kritik bir incelemeden faydalanabilir. Bu bağlamda Nye'ın teknolojik değişimler üzerine analizi, teknolojinin hızla değiştiği ve düzenleyici çerçevelerin bu değişime ayak uyduramadığı durumları göz önünde bulundurmadığı için kritik eleştirilere maruz kalabilir. Keza Nye'ın kendisinin de bu durumun farkında olduğu ve çalışmasında bu eksikliği vurguladığı belirtilmiştir (Akyeşilmen, 2018a, s. 273).

4.2.Önerilen Model: IGF Modeli

4.2.1. İnternet Yönetişimi Forumu

Telekomünikasyon ve internet alanında faaliyet gösteren uluslararası örgütler ve kuruluşlar, internet yönetişiminde önemli roller üstlenmektedir. Bu bağlamda BM ve Avrupa Konseyi özellikle dikkat çekicidir. Avrupa Konseyi, Budapeşte Siber Suç Sözleşmesi'nin oluşturulmasıyla bu alanda öne çıkmıştır. 21. yüzyılın başlarında, internetin toplumsal, ekonomik ve politik yaşama derin etkileri giderek daha fazla fark edilmeye başlandıkça, BM, internet yönetişimi konusunda liderlik yapma çabası içine girmiştir. Bu saikle, BM'nin uzmanlık kuruluşu olan ITU, "Bilgi Toplumu" konulu bir dünya zirvesi olan WSIS'i düzenlemekle görevlendirilmiştir. Bu kapsamda ITU, 2003 yılında Cenevre'de ve 2005 yılında Tunus'ta gerçekleştirilen iki aşamalı WSIS'i düzenlemiştir. Cenevre'deki ilk zirve sonrasında, dönemin BM Genel Sekreteri Kofi Annan, internet yönetişimiyle ilgili temel sorunları tanımlamak, bunları açıklığa kavuşturmak ve olası çözüm yolları önermek üzere WGIG'i görevlendirmiştir. Bu grup tarafından elde edilen bulgular, Tunus'taki zirvenin ikinci bölümünde tartışılmış ve bu tartışmalar, internet yönetişimi konusundaki diyalogları resmi bir zemine taşımayı ve bu alanda sürekliliği sağlamayı amaçlayan IGF'nin kurulmasına öncülük etmiştir.

IGF, BM tarafından desteklenen ve 2006'dan bu yana faaliyet gösteren, internet yönetişimine ilişkin konuların tartışıldığı bir platformdur. IGF'nin temel amacı, internetin yönetişimi konusunda tüm paydaşların bir araya gelerek bilgi alışverişinde bulunmalarını ve en iyi uygulamaları paylaşmalarını sağlamaktır. IGF, bağlayıcı karar alma yetkisine sahip olmamasına rağmen, küresel internet politikalarının şekillendirilmesinde önemli bir etkiye sahiptir.

4.2.1.1. Yapısı

IGF'nin yapısı, kapsayıcı ve çok paydaşlı bir yaklaşıma dayanır. Forumun faaliyetleri yıl boyunca sürer ve katılımcıların deneyimlerini paylaştığı, güncel konular üzerine tartıştığı ve politika önerilerini sunduğu yıllık bir toplantı ile sonuçlanır. Bu toplantıdan elde edilen çıktılar, daha sonra hem küresel hem de ulusal düzeyde karar alma mekanizmalarına sunulur. Her IGF toplantısı, BM Genel Sekreteri tarafından düzenlenir ve her yıl farklı bir ülkenin ev sahipliğinde gerçekleştirilir. Bu süreç, BM Ekonomik ve Sosyal İşler İdaresi (UNDESA) tarafından yönetilen ve gönüllü katkılarla desteklenen bir güven fonu aracılığıyla finanse edilir. Ev sahibi ülkeler yıllık IGF toplantısının düzenlenmesiyle ilgili maliyetlerin çoğunu üstlenirken, IGF Sekreteryasının faaliyetleri UNDESA tarafından yönetilen çok bağışçılı bir Güven Fonu'na ödenen bütçe dışı katkılarla finanse edilir.

Tablo 3. IGF'nin Yapısı

Bileşen	Rol ve Aktiviteler	Yapı	Katkılar
IGF Liderlik Paneli	- IGF'nin stratejik ve operasyonel rehberliğini sağlar. - Forumun genel temalarını ve önceliklerini şekillendirir. -IGF'nin görünürlüğünü ve etkisini artırır.	- Hükümet, özel sektör, sivil toplum ve teknik topluluklardan seçilmiş üyeler içerir. - Paydaş çeşitliliğini temsil eden atanan üyelerden oluşur.	- IGF'nin stratejik yönünü yönlendirerek forumun İnternet yönetişimi zorluklarına yanıt vermesini sağlar.
Çok Paydaşlı Danışma Grubu(MAG)	- Yıllık IGF toplantısının planlanmasından sorumludur. - Programın ilgili, çeşitli ve kapsayıcı olmasını sağlar.	- Geniş coğrafi ve paydaş çeşitliliğini yansıtan açık bir aday gösterme süreci aracılığıyla seçilir. - Çeşitli paydaş gruplarından temsilciler içerir.	- IGF'nin yıllık toplantısının, en acil İnternet yönetişimi konularını ele almasını ve tüm paydaş gruplarının perspektiflerini içermesini sağlar.
Dinamik Koalisyonlar(DCs)	- Belirli İnternet yönetişimi konularında çalışır. - Diyalogu kolaylaştırır ve çıktılar üretir.	- Tüm ilgilenen paydaşlara açık. - Aşağıdan yukarıya bir yaklaşımla çalışır.	- Geniş IGF tartışmalarını ve politika oluşturmalarını bilgilendiren derinlemesine içgörüler ve öneriler sağlar.
En İyi Uygulama Forumları(BPFs)	- Deneyimlerin ve en iyi uygulamaların paylaşımını sağlar. - Yıllık olarak değişen konular üzerinde çalışır.	- Koordinatörler tarafından yönetilir. - IGF Sekretaryası tarafından desteklenir. - Tüm ilgilenen tarafların katılımına açıktır.	- Paydaşların kendi bağlamlarında uygulayabileceği kılavuzlar, ilkeler ve politika önerileri gibi kaynaklar üretir.

Politika Ağları	- Tematik İnternet yönetişimi alanlarında odaklanır. - Araştırma yapar ve tartışmaları teşvik eder.	- Çok paydaşlı doğada olup ilgilenen katılımcıların işbirlikçi çabaları aracılığıyla çalışır.	- Karmaşık İnternet yönetişimi zorluklarını ele alan kapsamlı içgörüler ve politika önerileriyle sonuçlanır.
Kapasite Geliştirme	- Anlayış, beceri ve katılımı artırmayı amaçlar. - Özellikle temsil edilmeyen gruplar ve gelişmekte olan ülkelerden olan paydaşlar için.	- Çeşitli paydaşlarla işbirliği içinde geliştirilen ve sunulan eğitim programları, atölye çalışmaları ve kaynakları içerir.	- İnternet yönetişimi süreçlerine katılımın çeşitliliğini ve kalitesini artırır, paydaşların etkili bir şekilde katkıda bulunmalarını sağlar.
Ulusal ve Bölgesel IGF Girişimleri(NRIs)	- Yerel bağlamlara uygun İnternet yönetişimi konularını ele alır. -Tartışmaları kolaylaştırır ve farkındalık yaratır.	- Bağımsızdır ancak küresel IGF'nin prensipleriyle uyumlu çalışır. - Yerel ve bölgesel paydaşlar tarafından organize edilir ve çok paydaşlı modeli yansıtır.	- Yerel perspektifleri ve çözümleri küresel sahneye taşıyarak, İnternet yönetişimine daha kapsayıcı ve kapsamlı bir yaklaşım benimsemeyi teşvik eder.

Kaynak: Tablo, yazar tarafından (IGF, t.y.a) kaynağından elde edilen bilgilerle oluşturulmuştur.

Yukarıdaki tablodan da görüleceği üzere IGF, her biri işleyişinde ve yönetişiminde önemli rol oynayan birkaç temel bileşenden oluşmaktadır. IGF'nin yapısı, stratejik ve operasyonel rehberlik sağlayan IGF Liderlik Paneli, yıllık toplantıların planlanmasından sorumlu Çok Taraflı Danışma Grubu (MAG), belirli konularda çalışan Dinamik Koalisyonlar, en iyi uygulamaların paylaşımını teşvik eden En İyi Uygulama Forumları (BPF'ler), tematik alanlarda odaklanan Politika Ağları, kapasite geliştirme faaliyetleri ve yerel bağlamlara odaklanan Ulusal ve Bölgesel IGF Girişimleri (NRI'lar) dahil olmak üzere çeşitli ana bileşenlerden oluşur. Bu bileşenlerin her biri, internet yönetişimi süreçlerine katılımın çeşitliliğini ve kalitesini artırmak, yerel perspektifleri küresel sahneye taşımak ve açık, güvenli ve herkes için erişilebilir bir interneti destekleyen politikaların ve uygulamaların geliştirilmesine katkıda bulunmak için bir araya gelir.

NRI'lar internet yönetişiminde kilit bir rol oynamaktadır. Bunlar, küresel IGF'nin ana ilkelerine uygun olarak hareket ederken, internet yönetişimiyle ilgili konuları kendi

topluluklarının bakış açısından tartışan organik ve bağımsız oluşumlardır (APC, 2016). 2023 itibariyle, BM'nin beş bölgesinin tamamında yer alan ve dünyanın dört bir yanına yayılmış 155'ten fazla girişim bulunmaktadır.[71] Örneğin Avrupa'da, EuroDIG (İnternet Yönetişiminde Avrupa Diyaloğu) ve SEEDIG (İnternet Yönetişiminde Güney Doğu Avrupa Diyaloğu) gibi platformlar, Avrupa ve Güney Doğu Avrupa'nın internet yönetişimiyle ilgili konularını tartışmak için bir araya gelmektedir.

IGF, BM Genel Sekreteri'ne doğrudan bağlı olmasına rağmen, BM'nin katı kurallarına tam olarak uymak zorunda değildir. Bu, IGF'nin nasıl çalışacağını kendisinin belirleyebilmesine ve kendi kurallarını oluşturabilmesine olanak tanımaktadır. Bu kurallar, BM sistemi içinde ve devlet temsilcilerinin katıldığı organizasyonlarda bugüne kadar uygulanan "en açık" kurallardır (de la Chapelle, 2007, s. 24). Bu yönüyle IGF, küresel internet yönetişiminde eşsiz bir deneyimdir. Önceden tanımlanmış bir üyeliği olmayan, devletlere, sivil topluma, özel sektöre ve internet teknolojisi topluluğuna açık bir platformdur. Esasen katılımcılara "olduğun gibi gel ama sunacak bir şeyle gel" mesajı verilir. IGF, karar alma organı değil, farklı görüşlerin dile getirildiği, diyalog ve tartışmanın teşvik edildiği bir alandır (Doria & Kleinwächter, 2008, s. 4).

4.2.1.2.İşlevleri

Internet Yönetişimi, WSIS sürecinde iki yıl boyunca yapılan tartışmaların ardından, internetin ve kullanımının yol açtığı çeşitli sorunları ele alacak şekilde iki ana boyutta ele alınması gerektiği konusunda bir fikir birliğine varılmıştır. İlk boyut, internetin kendisinin yönetişimini ifade eder ve internetin teknik altyapısını, işleyişini yönetmeyi içerir. Bu, DNS, IP adresleri ve internetin omurgasını oluşturan ağ altyapısı gibi teknik unsurları kapsar. İkinci boyut ise ağ üzerinde yürütülen faaliyetlerin yönetimine odaklanır ve telif hakkı, siber suç, nefret söylemi ve internetin etik kullanımı gibi konuları içerir (de la Chapelle, 2007, ss. 21-22). Bu iki boyutun ayrımı, internetin karmaşıklığını ve çeşitliliğini anlamamızı kolaylaştırır ve her iki alanın da etkin yönetimi, internetin adil, kapsayıcı ve güvenli bir şekilde gelişimini sağlamak için hayati öneme sahiptir.

[71] Girişimlerin haritasına ulaşmak için bkz: Internet Governance Forum. (t.y.). *National and Regional IGF Initiatives*. https://www.intgovforum.org/en/content/national-and-regional-igf-initiatives (02.02.2024).

Bu görevlerin, internet yönetişimi alanında uluslararası işbirliği ve politika geliştirme çabalarını koordine etmek amacıyla kurulan IGF'ye de atfedildiği görülmüştür. Tunus Gündemi'nin (2005) 72. Paragrafında IGF'nin görevleri şunlardır:

> a. İnternetin sürdürülebilirliğini, sağlamlığını, güvenliğini, istikrarını ve gelişimini teşvik etmek amacıyla internet yönetişiminin temel unsurlarıyla ilgili kamu politikası konularını tartışmak;
> b. İnternetle ilgili farklı kesişen uluslararası kamu politikalarıyla ilgilenen organlar arasında söylemi kolaylaştırmak ve mevcut herhangi bir organın kapsamına girmeyen konuları tartışmak;
> c. uygun hükümetlerarası kuruluşlar ve diğer kuruluşlarla arayüz oluşturmak kendi yetki alanlarına giren konularda kurumlar;
> d. bilgi ve en iyi uygulamaların değişimini kolaylaştırmak ve bu çerçevede akademik, bilimsel ve idari personelin uzmanlığından tam olarak yararlanmayı teknik topluluklar;
> e. tüm paydaşlara, teknik toplulukları hızlandırmak için yollar ve araçlar önerme konusunda tavsiyelerde bulunmak Gelişmekte olan dünyada internetin kullanılabilirliği ve uygunluğu;
> f. paydaşların mevcut projelere katılımını güçlendirmek ve geliştirmek ve/veya gelecekteki internet yönetişim mekanizmaları, özellikle de gelişmekte olan ülkeler;
> g. ortaya çıkan sorunları tespit etmek, bunları ilgili organların ve kamuoyunun dikkatine sunmak ve uygun olduğu durumlarda tavsiyelerde bulunmak;
> h. yerel bilgi ve uzmanlık kaynaklarından tam olarak yararlanarak, gelişmekte olan ülkelerde internet yönetişimi için kapasite oluşturulmasına katkıda bulunmak;
> i. İnternet yönetişimi süreçlerinde WSIS ilkelerinin uygulanmasını sürekli olarak teşvik etmek ve değerlendirmek;
> j. diğerlerinin yanı sıra, kritik internet kaynaklarıyla ilgili konuları tartışmak;
> k. İnternetin kullanımı ve kötüye kullanımından kaynaklanan ve özellikle günlük kullanıcıları ilgilendiren sorunlara çözüm bulunmasına yardımcı olmak;

l. Bildirilerini yayınlamak (Tunus Gündemi, 2005, Par. 72).

IGF, çeşitli kamu politikası meselelerini ele almak için tasarlanmış bir platformdur. Amacı, farklı sektörlerden gelen katılımcıların bir araya gelip, internet yönetişimi ile ilgili konuları tartışabilmeleri için bir alan sağlamaktır. IGF'nin temelinde yatan güç, özel sektör ve sivil toplumdan gelen işbirliği ve desteğin yanı sıra, tüm katılımcıların eşit olarak görüldüğü ve birlikte konsensüse dayalı, bağlayıcı olmayan çözümler üretebildiği bir ortamın oluşturulmasıdır. Bu forum, teknik detayların ve geniş çaplı danışmanlığın ön planda olduğu bir hazırlık mekanizması görevi görerek, internet yönetişimi üzerine yapılan tartışmalara değer katmaktadır. IGF'de varılan uzlaşılar, diğer forumlarda ve tartışmalarda –özellikle bağlayıcı olanlarda– çözüm yollarının nasıl şekillendirilebileceği konusunda bir referans noktası oluşturmaktadır (Mueller & Mathiason, 2006). Bu kapsamlı yaklaşım, IGF'nin küresel internet yönetişimi konularında kritik bir rol oynamasını sağlamakta ve çeşitli paydaşların etkileşimini teşvik etmektedir.

IGF'nin temel amacı, internetin yönetişimi konusunda çeşitli paydaşların görüşlerini bir araya getirmek ve internetin herkes için açık, güvenli ve erişilebilir olmasını sağlamak üzerine kuruludur. IGF, bu amaca ulaşmak için her yıl düzenlenen toplantılar, çalışma grupları ve çeşitli tematik ve bölgesel girişimler aracılığıyla internet politikaları, güvenlik, insan hakları, dijital bölünme ve teknolojinin etik kullanımı gibi konularda tartışmalar ve politika önerileri geliştirmeye yönelik bir platform sunar.

IGF'nin işlevleri arasında, tematik çalışmalar, en iyi uygulama forumları, dinamik koalisyonlar, politika ağları, kapasite geliştirme atölye çalışmaları ve gençlik girişimleri gibi çeşitli ara dönem çalışmaları yer alır. Bu çalışmalar, internet yönetişimi ile ilgili mevcut ve ortaya çıkan konularda derinlemesine uzman görüşleri ve iyi uygulamaları paylaşmayı amaçlar. IGF ayrıca, yüksek düzeyli liderler izleği ve parlamento oturumları gibi yüksek düzeyli oturumlar da dahil olmak üzere farklı oturum formatları sunar, burada devletler, özel sektör, sivil toplum ve teknik topluluklardan gelen liderler dijital teknolojilerin ve kamu dijital politikalarının önemli yönlerini ele alır.

Her yıl, IGF toplantıları sonucunda elde edilen çıktılar, oturum raporları, transkriptler, video kayıtları ve özet raporlar gibi çeşitli formatlarda sunulur. Bu çıktılar, IGF'nin internet yönetişimi konularındaki tartışmaları ve önerileri geniş bir kitleye ulaştırma çabasının bir parçasıdır.

4.2.1.3.Katkıları

Yasal, düzenleyici ve politik çerçevelerin farklılığına rağmen, internetin küresel düzeyde sorunsuz çalışmasını garanti altına almak için ülkeler arasında koordinasyon elzemdir. Bu koordinasyon, politika ve gelişmelerin potansiyel etkilerini öngörerek ve bu trendlerin yaratabileceği olası sonuçlara karşı hazırlık yaparak işlev görebilir. İnterneti etkileyebilecek kararların istenmeyen etkilerini değerlendirme, inceleme ve izleme konusunda çok paydaşlı yaklaşım, tercih edilen en iyi model olarak kabul edilmektedir (IGF Summary Report, 2023). Bu bağlamda IGF'nin çok paydaşlı katılım konusunda internet yönetişimiyle ilgili diğer kuruluş ve platformlarından çoğundan daha başarılı olduğu ifade edilmektedir (Creech vd., 2009, s. 2). IGF, farklı paydaşları bir araya getirerek ve internetin yönetişimiyle ilgili önemli konularda diyalog ve işbirliği sağlayarak birçok başarıya imza atmıştır. Tek tek kuruluşların veya tek bir sektörün başaramayacağı sonuçlara ulaşmıştır (Cogburn, 2017, s. 216).

IGF'nin ilk olarak 2005 yılında Tunus Gündemi'nde belirlenen görev süresi, 16 Aralık 2015 tarihinde BM Genel Kurulu'nun 70/125 sayılı kararıyla on yıl daha uzatılmıştır. Bu uzatma, IGF'nin gelişen internet yönetişimi ortamındaki rolünün önemini vurgulamaktadır (IGF, t.y.). Zira IGF modeli, tüm paydaşların sesinin duyulmasını sağlayabilen tek modeldir. Bu model, uluslararası karar alma süreçleri ve mevzuat oluşturma faaliyetlerinde aşağıdan yukarıya doğru bir yaklaşım sunarak, her bir katılımcının görüşlerini ve çıkarlarını dikkate alır. Çok paydaşlı mekanizmalar, devletler tarafından yukarıdan aşağıya uygulanan, çok taraflı normlar ve düzenlemelere kıyasla internetin gerçek çıkar ağlarına hizmet edebilme potansiyeline sahiptir. Bu geniş katılımcı tabanı sayesinde, farklı bakış açılarından gelen zengin görüş ve önerilerin tartışma sürecine dahil edilmesi sağlanır (Lahmann vd., 2017, s. 37). Bu bağlamda IGF'nin katkıları şu şekilde sıralanmıştır:

- Bu forum, uluslararası internet kamu politikaları ve bunların etkileri konusunda anlayışı ve uzlaşmayı kolaylaştırmıştır.
- İnternet yönetişimi ve yeni teknolojiler üzerine anlayış ve uzlaşmayı geliştirmiştir.
- Farklı internet yönetişimi ve teknoloji konularında faaliyet gösteren önemli kuruluşlar ve paydaşlar arasında işbirliğini ve koordinasyonu artırmıştır.

- İnternetin sürdürülebilirliği, güvenliği, istikrarı ve gelişimini teşvik eden fırsatları genişletmiştir.
- Özellikle gelişmekte olan ülkelerin ve onların paydaşlarının internet yönetişimine etkin bir şekilde katılım kapasitelerini güçlendirmiştir.
- İnternette çok dillilik ve çok kültürlülüğü teşvik etmiştir.
- İnternetle ilgili kamu politikaları konularında çok paydaşlı ve çok taraflı girişimleri belirlemiştir (UN Society, t.y., s. 6).

İlk bakışta IGF, basit bir diyalog alanı gibi görünebilir. Karar alma yetkisi olmadan, mütevazı bir yapıya sahip gibi durmaktadır. Fakat bu mütevazı görünümün ardında IGF, uluslararası düzeyde önemli bir rol oynamaktadır. IGF, ilk defa uluslararası alanda, ifade özgürlüğü ve mahremiyet gibi çeşitli ve potansiyel olarak tartışmalı kamu politikası konularını tartışmak üzere devlet temsilcilerini ve ilgili vatandaşları bir araya getiren resmi bir tematik müzakere alanı oluşturmuştur (de la Chapelle, 2007, s. 25). Bu, internet yönetişiminde önemli bir dönüm noktasını temsil eder.

IGF'nin katkısı sadece diyalog alanı sağlamakla sınırlı değildir. Ağın yönetimi ve kullanımına ilişkin iyi uygulama standartlarının belirlenmesine yardımcı olmak için de önemli bir rol oynamıştır. Bunu, iyi ve başarılı çalışmalarla ve bilgi ve deneyim paylaşımına yönelik yeni ortaklıklar kurarak gerçekleştirmiştir. Ayrıca ilgili alanlarda dinamik koalisyonlar oluşturarak ortak eylemler ve pratik sonuçlar doğurmuştur (Doria & Kleinwächter, 2008, s. 6). Diğer yandan, bölgesel ve ulusal IGF girişimleri, çok paydaşlı modelin farklı kültürel, siyasi ve ekonomik bağlamlarda nasıl uygulandığını göstermektedir. Bu forumlar, çok paydaşlılığın gerçekleştirilme biçimlerini, örgütsel yapıları, prosedürleri, finansman mekanizmalarını, gündemleri ve formatlarını keşfetmek için benzersiz fırsatlar sunar. Katılımcı çeşitliliği ve bu etkinliklerin ulusal, bölgesel veya küresel internet yönetişimi tartışmaları üzerindeki potansiyel etkileri, bu girişimlerin değerini ve önemini artırmaktadır (Epstein & Nonnecke, 2016, s. 143).

IGF, bilgi paylaşımı ve tartışma forumu olmanın ötesine geçerek, internet yönetişimiyle ilgili önemli kararların müzakere edildiği daha sağlam bir platforma dönüşmüştür. IGF'nin başarısı, küresel forumu ulusal türevleriyle entegre etme çabalarından kaynaklanmaktadır. Bu çabalar, ulusal ve uluslararası düzeylerde çok sayıda paydaşı bir araya getirerek, küresel ve ulusal internet yönetişim sistemlerinde üzerinde bir denetim ve denge mekanizması oluşturmuştur. IGF, ulusal ağları kullanarak

uluslararası, çok paydaşlı danışma süreçlerini güçlendirerek faaliyetlerini paydaşlarından girdi toplama ve bu girdiyi faaliyetlerine dahil etme konusunda önemli bir rol oynamıştır. Bu süreçler, dünya genelinde vatandaşlara internet sahipliği hissiyatı kazandırmanın yanı sıra, tüm kritik kararların ortak iyilik gözetilerek alınmasını sağlama konusunda da yardımcı olmuştur (Hoxtell & Nonhof, 2019, ss. 15-16).

Patrick, IGF'nin benzersiz yapısına ithafen şöyle bir çıkarımda bulunmuştur: "Başka hiçbir yönetişim modeli, internetin kıskançlıkla korunan, ulusal telekomünikasyon tarafından işletilen kalelere bölünmesini, YouTube gibi sosyal ağlara, hatta internetin kendisine bile erişimin anında engellenebilmesini engelleyemez." Bu sözleriyle Patrick, IGF'nin önemini ve internetin küresel ve açık bir platform olarak korunmasındaki rolünü vurgulamaktadır. Zira IGF, farklı paydaş gruplarını bir araya getirerek ve internetin geleceği hakkında diyalog teşvik ederek, internetin bölünmesini ve ulusal düzeyde kontrol edilmesini engellemektedir (Masters, 2014). Bu bağlamda Çin'in 2010 yılında BM'ye yaptığı açıklamada, IGF'den "Kritik İnternet Kaynaklarının tek taraflı kontrolü sorununu çözmelerini" istemesi dikkat çekicidir. 2016 yılında NTIA, ICANN'in çok paydaşlı platforma geçiş kararını deklare ettiği belgede bunu açıkça belirtti:

> BM'nin 2005 yılında İnternet Yönetişim Forumu'nu (IGF) kurmasından bu yana IGF toplantıları giderek daha verimli hale geldi, ancak bazı devletler hala BM'nin ICANN ve IANA tarafından yürütülen DNS görevlerini denetlemesini istiyor. Çin hükümeti Temmuz-2010'da BM'ye yaptığı açıklamada, BM ve IGF'den "Kritik İnternet Kaynaklarının tek taraflı kontrolü sorununu çözmelerini" istedi (U.S. Government Publishing Office, 2016).

Bu ifade, devletlerin –özelde büyük güçlerin– IGF'nin internet yönetişimindeki rolüne ne kadar önem verdiklerini açıkça göstermektedir. Bu noktada IGF'nin, internet yönetişim kurumlarının uluslararasılaştırılmasına yönelik yaşanan gerginlikleri hafifletmede doğrudan bir rol oynadığı söylenebilir. IGF'nin değer katabileceği en önemli yollardan biri, daha yerleşik internet yönetişimi forumlarında (ICANN, IETF, W3C gibi) alınan kararları etkileyebilmesidir. Bu doğrultuda alınan kararlar için bir "ön tartışma alanı" olarak hareket edebilir. Ancak, IGF'deki tartışmaların bu forumlarda alınan herhangi bir kararı doğrudan etkileyip etkilemediğini kesin olarak söylemek

zordur. Bununla birlikte, bazı kararların IGF'deki tartışmalardan ve kilit aktörlerin katılımından etkilenmiş olması da mümkündür. Bunun kesin olarak bilinmesi, karar alımı sırasında IGF'deki tartışmalara atıfta bulunulmasıyla mümkün olabilir (Creech vd., 2009, s. 4).

IGF, bağlayıcı karar alma yetkisine sahip olmasa da, kilit konuları belirleme gücüne sahiptir. İleriye dönük politikalara rehberlik edebilecek ilke, norm ve değerlerin yaratılmasında siyasi etkileri vardır. Bu yönüyle IGF, gelişmiş ve gelişmekte olan ülkeler arasındaki bütün paydaş kategorileri arasında dinamik, anlamlı ve eşitlikçi katılımı teşvik etmektedir (Pushyamitra, 2022, s. 638). Bu anlamda IGF, uluslararası "yumuşak hukuk" araçlarını benimseme fırsatı sunmakta ve küresel internet yönetişimi düzenlemelerinin tüm katılımcı kategorilerinin çıkarlarını dikkate alarak iyileştirilmesine yönelik rehberlik sağlamayı amaçlamaktadır. Bunun bir örneği, İnsan Hakları Dinamik Koalisyonu tarafından geliştirilen İnternet Hak ve İlkeleri Taslağı ve IGF'nin ilkeleridir. Bu durum, insan hakları belgelerinin internete getirilmesi ihtiyacına etkili bir yanıt olarak kabul edilmektedir (Shcherbovich, 2017, s. 7). İnternet Hakları ve İlkeleri Koalisyonu tarafından hazırlanan İnternet'teki İnsan Hakları ve İlkeler Sözleşmesi, evrensel bir aracın en parlak örneğidir. Bu sözleşme, İnsan Hakları Evrensel Beyannamesi'nin online eşdeğeri olma potansiyeline sahiptir (Shcherbovich, 2017, s. 12).

Malcolm, IGF'nin potansiyelini tam anlamıyla gerçekleştirebilmesi halinde, internet yönetişim rejiminde önemli bir etki yaratacağını ve ICANN, ITU gibi diğer internet yönetişim forumlarının da benzer çok paydaşlı yaklaşımı benimsemelerine öncülük edebileceğini ileri sürmektedir. Malcolm'a göre IGF örneği, internet yönetişimiyle sınırlı kalmayıp, çevre, fikri mülkiyet, ticaret, barışı koruma ve insan hakları gibi çok çeşitli uluslararası kamu politikası alanlarında çok paydaşlı yönetişim modelinin uygulanabilirliğini göstermektedir. Bu, IGF'nin sadece internet yönetişimi alanında değil, aynı zamanda Westphalia sonrası uluslararası ilişkiler çağında "yeni bir paradigma" olarak öncü rol oynayabileceğini işaret etmektedir (2008, s. 521). Bu görüş, IGF'nin potansiyelinin gerçekleşmesi halinde, uluslararası politik ve sosyal meselelerin ele alınış biçiminde köklü değişikliklere yol açabileceğine dair güçlü bir beklenti yaratmaktadır.

4.2.1.4.Toplantıları

IGF, 2006'dan bu yana her yıl önemli toplantılar düzenlemekte ve bu toplantılarda ele alınan konuları kapsayan raporlar yayımlamaktadır. Her yılın toplantısı, internet yönetişimiyle ilgili çeşitli temalar altında düzenlenir ve bu toplantıların sonuçları, "IGF Mesajları" olarak bilinen tematik mesajlar içeren raporlarda özetlenir.

IGF'nin ilk iki toplantısı, internet yönetişimi alanında eşitlik, özgürlük, yönetişim ve katılım gibi temel ilkeleri ve önemli konuları şekillendirmede kritik bir role sahipti. Özellikle eşitlik konusunda, gelişmekte olan ülkelerde ve İngilizce bilmeyen kullanıcılar için internet erişimi ve kullanımındaki eşitsizlikler büyük bir endişe kaynağı olarak görülürken, tartışmalar bu alandaki eşitliği nasıl teşvik edebileceğimize dair stratejiler üzerine odaklandı. Bu, herkes için adil ve eşit internet erişiminin sağlanması hedefini ön plana çıkardı. Özgürlük boyutunda ise ifade özgürlüğünün korunması, siber suçlar ve spam ile mücadele, çocukların korunması gibi konular ele alınırken, ifade özgürlüğü ile mahremiyet arasındaki denge de önemli bir tartışma konusu oldu. Bu, internetin özgür bir alan olarak kalmasını sağlarken, kullanıcıların güvenliği ve mahremiyetinin de korunmasının önemini vurguladı (Doria & Kleinwächter, 2008, s. 4-5).

Milton Mueller'in IGF'nin 2006 tarihli ilk toplantısındaki konuşması, kritik internet kaynaklarının küresel yönetişimine dair temel bir perspektif sunar. Konuşmada, alan adları, kök sunucular ve internet protokol adresleri gibi sanal kaynakların, elektrik enerjisi ve telekomünikasyon altyapısı gibi diğer kritik kaynaklardan farklı olarak, küresel koordinasyon ve yönetişim gerektirdiği vurgulanmaktadır. Bu kaynakların küresel doğası, onların yönetişiminin ulusal veya bölgesel düzeyde değil, küresel bir düzeyde ele alınması gerektiğini gösterir. İnternet adreslerinin tükenmesi, yeni IPv6 protokolünün eski protokollerle uyumsuzluğu ve bu geçişin ekonomik ve teknik zorlukları, konuşmanın önemli noktaları arasındadır. Ayrıca, DNS'nin güvenliğinin artırılması ve kök bölge dosyasının şifrelenmesi, küresel internet için güvenlik dayanağı oluşturacak yeni süreçlerin tanımlanmasını gerektirir. Yeni üst düzey alan adlarının yaratılması, çok dilli olmaları ve bunun küresel içerik düzenlemesi, ulusal internet sorunları ve pazar hakimiyeti ile ilgili yeni sorunlar doğurabileceği belirtilir. Mueller, devletler, özel sektör ve sivil toplum dahil olmak üzere çeşitli paydaşların katılımıyla çoğulcu ve ağ bağlantılı bir yönetişim biçimini savunurken, bu konuların geniş bir paydaş grubu tarafından tartışılmasının önemini vurgular. Bu, sadece teknik

sonuçlara değil, aynı zamanda kamu politikası sonuçlarına da odaklanılması gerektiğini gösterir. Kritik internet kaynakları, gerçek anlamda küresel yönetişim sorunlarıdır ve bu konuda farkındalık yaratmak ve etkili kamu politikası ilkeleri geliştirmek için geniş çaplı işbirliği ve diyalog gerektirir (IGF, 2006, ss. 262-263).

Aşağıdaki tablo, IGF'nin yıllara göre belirlediği alt temaları göstermektedir. IGF elbette tabloda belirtilen her konuya her yıl değinmekte, fakat alt tema olarak belirlediği konular değişkenlik göstermektedir. Bu nedenle tabloda "x" ile işaretlenen kısımların tartışılmadığı kanısına varılmaması önemli bir husustur. Aynı zamanda yıllar içinde -özellikle 2019 itibariyle- çok farklı temalara değinilmiş fakat tabloda genel olarak değinilen temalar kategorize edilmiştir.

Aşağıdaki tablodan da görüleceği üzere başlangıç yıllarında IGF'de açıklık, güvenlik, çeşitlilik, erişim ve kalkınma gibi temel konulara odaklanılırken, zamanla güvenlik, siber güvenlik ve insan hakları gibi konular daha fazla önem kazanmıştır. Bu değişiklik, internetin sosyal ve ekonomik alanda oynadığı rolün artması ve teknolojik gelişmelerin yarattığı yeni zorluklarla uyumlu bir şekilde, IGF'nin gündeminin genişlediğini ve derinleştiğini göstermektedir. 2013 yılından itibaren insan haklarının önemli bir tema olarak kabul edilmesi, internetin ifade özgürlüğü, gizlilik ve diğer temel haklar üzerindeki etkilerinin giderek daha fazla tanınmasıyla ilgilidir. Bu durum, internet yönetişiminde insan haklarına verilen önemin artan uluslararası endişelerle paralel ilerlediğini gösterir.

Tablo 4. Yıllara Göre IGF Toplantılarının Alt Temaları

Alt Temalar	2006	2007	2008	2009	2010	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020	2021	2022	2023
Açıklık	✓	✓	✗	✓	✓	✗	✓	✓	✗	✗	✗	✓	✗	✗	✓	✗	✗	✗
Güvenlik	✓	✓	✓	✓	✓	✗	✓	✓	✗	✓	✗	✗	✗	✓	✗	✓	✓	✗
Çeşitlilik	✓	✓	✗	✓	✓	✗	✓	✓	✗	✓	✓	✓	✗	✓	✗	✗	✗	✗
Erişim	✓	✓	✗	✗	✓	✗	✓	✓	✓	✗	✓	✓	✓	✓	✗	✓	✗	✗
Kalkınma	✓	✓	✗	✗	✓	✓	✓	✗	✓	✗	✗	✓	✓	✗	✗	✗	✗	✗
Kritik İnternet Kaynakları	✗	✓	✓	✓	✓	✗	✓	✗	✓	✓	✓	✓	✗	✗	✗	✗	✗	✗
Yükselen Konular	✓	✗	✓	✓	✓	✓	✓	✗	✓	✓	✓	✓	✓	✓	✗	✓	✓	✗
Gelişmiş İşbirliği	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗	✓	✗	✓
Çok Paydaşlı İşbirliği İlkeleri	✗	✗	✗	✗	✗	✗	✗	✓	✗	✓	✓	✓	✗	✓	✗	✗	✗	✗
İnsan Hakları	✗	✗	✗	✗	✗	✗	✗	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Siber Güvenlik	✗	✗	✓	✗	✗	✗	✗	✗	✗	✓	✓	✓	✓	✓	✗	✗	✗	✓
İnternet Ekonomisi	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✓	✗	✗	✓	✗	✗	✗	✗
Sürdürülebilir Kalkınma	✗	✗	✗	✗	✓	✗	✗	✗	✗	✗	✓	✓	✗	✓	✓	✗	✓	✓

Kaynak: Tablo, yazar tarafından IGF toplantılarından derlenen bilgilerle oluşturulmuştur.

Özellikle 2013'ten itibaren insan haklarına verilen önem artarken, sürdürülebilir kalkınma ve çeşitli işbirliği modelleri gibi temalar da dikkat çekmektedir. Bu durum, IGF'nin internetin toplumsal etkilerini daha kapsamlı bir şekilde ele aldığını, aynı zamanda internet yönetişiminde daha kapsayıcı ve işbirlikçi yaklaşımları teşvik ettiğini göstermektedir. Güvenlik ve siber güvenlik temasının sürekliliği, bu alanın yarattığı tehdit unsurlarıyla paralel ilerlemiştir. Nitekim güvenlik, internetin başından beri sürekli bir endişe kaynağı olmuştur. Siber güvenliğin özellikle 2008'den sonra daha fazla önem kazanması, siber saldırıların artmasıyla internetin güvenliğinin sağlanmasının zorlaştığını göstermektedir. 2023 yılında siber güvenliğin tekrar ön plana çıkması, siber tehditlerin devam eden evrimini ve bu konudaki sürekli ihtiyaçları yansıtmaktadır.

Benzer şekilde sürdürülebilir kalkınma teması da, özellikle 2015'ten sonra önem kazanmıştır. Bu temanın seçilmesi, BM'nin Sürdürülebilir Kalkınma Hedefleri'nin (SDGs) kabul edilmesiyle uyumlu olarak, internetin kalkınma üzerindeki olumlu etkilerine ve teknolojinin sürdürülebilir kalkınma hedeflerine nasıl katkıda bulunabileceğine dair artan bir farkındalığı yansıtmaktadır. Bununla bağlantılı olarak çevre ve iklim değişikliği konuları da 2020'den itibaren önem kazanmıştır. Çevresel sürdürülebilirlik ve iklim değişikliği gibi konuların son yıllarda gündeme gelmesi, teknoloji ve internetin çevre üzerindeki etkilerine dair artan farkındalığı ve sürdürülebilir çözümlere olan ihtiyacı yansıtmaktadır. Bu, küresel düzeyde çevresel sorunlara karşı mücadelede internetin rolünün giderek arttığını gösterir.

Erişim ve dijital kapsayıcılık temalarının belli aralıklarla gündeme alınması, internetin evrenselliğinin ve herkes için eşit erişimin sağlanmasının sürekli gündemde olan bir mesele olduğunu gösterir. Bu, özellikle gelişmekte olan ülkelerde internet erişiminin artırılması ve dijital uçurumun azaltılması çabalarıyla bağlantılıdır. Çok paydaşlı işbirliği temalarının da dönemsel olarak öne çıkması, çeşitli paydaşların katılımının gerekliliğinin altını çizme ihtiyacından doğmuştur. Özellikle 2013 ve sonrasında bu temalara verilen önem, internet yönetişiminde daha kapsayıcı ve işbirlikçi yaklaşımların benimsendiğini göstermektedir.

Sonuç olarak IGF'nin yıllık toplantılarında ele alınan temaların analizi, internet yönetişiminin dinamik ve sürekli gelişen bir alan olduğunu ve IGF'nin bu değişen teknolojilere uyum sağlayabilecek esnekliğe ve adaptasyona sahip olduğunu göstermektedir. Yıllar içinde değişen teknolojik ve sosyal koşullar, forumun gündemini şekillendirmiş ve yeni zorluklara yanıt olarak farklı temalara odaklanılmasını sağlamıştır. Güvenlik, insan hakları ve sürdürülebilir kalkınma gibi temaların ön plana çıkması, internetin toplum üzerindeki derin etkileri ve bu etkileri yönetme ihtiyacını yansıtır. IGF'nin temalarındaki bu değişiklikler, internetin evrensel bir kaynak olarak öneminin altını çizdiğini ve internet yönetişiminin çok yönlü ve dinamik doğasına ayak uydurabildiğini gösterir.

2023 IGF toplantısının genel teması olan "İstediğimiz İnternet – Tüm İnsanları Güçlendirmek" idi. Bu tema, IGF'nin "kimseyi geride bırakmayan kapsayıcı bir interneti gerçekleştirme ve insanlığın sürdürülebilir geleceğine giden yolu hızlandırma kararlılığının güçlü bir ifadesi" olarak belirtilmiştir (IGF Report, 2023). IGF 2023

toplantısında sürdürülebilirlik ve çevre, insan hakları ve özgürlükler, küresel internet yönetişimi ve işbirliği, dijital ayrımlar ve dahil etme, veri yönetişimi ve güven, siber güvenlik, siber suç ve online güvenlik, internetin parçalanmasını önleme, yapay zekâ ve gelişen teknolojiler öne çıkan temalar arasında yer almıştır.

19. IGF toplantısı, 2024 yılının son çeyreğinde Suudi Arabistan Krallığı Hükümeti'nin ev sahipliğinde Riyad şehrinde düzenlenecek. Ayrıca, IGF 2024 için Çok Taraflı Danışma Grubu (MAG) ataması yapıldı ve yeni Başkan, Bahamalar Hükümeti'nden Carol Roach olarak belirlendi (IGF, t.y.).

4.2.2. İnternet Yönetişimi Forumu'nun Sorun Alanları

4.2.2.1. Yapısal Sorunlar

IGF'de ele alınan konular ve tartışmalar, çeşitli eleştirilere konu olmuştur. Özellikle, kritik kaynakların kontrolü, gelişmiş işbirliği ve küresel fikri mülkiyet gibi önemli konuların yeterince kapsamlı bir şekilde ele alınmaması eleştiri odaklarından biridir. Bu tür kritik konuların tartışılması girişimlerinde somut adımlar atılmak istense de, çeşitli bahanelerle bu konuların sıklıkla göz ardı edildiği belirtilmektedir. Bu durum, forumun asıl amacına ulaşmasında engeller yaratmakta ve kritik meselelerin çözümüne yönelik ilerleme kaydedilmesini zorlaştırmaktadır (Josukutty, 2020, s. 66).

Bunun yanı sıra, aşağıdaki tablodan da görüleceği üzere Kuzey-Güney ekseninde anlayış farklılıkları da IGF'deki önemli bir tartışma konusudur. Kuzey ülkeleri (ABD, AB, Avustralya) arasında genelde ortak bir anlayışın hâkim olduğu görülürken, gelişmekte olan ülkeler farklı perspektiflere ve görüşlere sahip. Örneğin, Avustralya'dan Chris Disspain'in mali desteği geri çekme tehdidi gibi durumlar, forum içindeki çözüme yönelik çabaları olumsuz etkileyebilmektedir. Temsil ve seçim konusunda farklı görüşler de mevcut; sivil toplum doğrudan seçim ve öz yönetim modelini savunurken, gelişmekte olan ülkeler daha geleneksel hükümet modellerini tercih etmekte. Ayrıca, özel sektörün, özellikle ABD Ticaret Bakanlığı'nın desteğiyle ICANN'den gelen kişilerin IGF'nin çeşitli organlarında siyasi temsili domine etmesi, forumun dengesini bozabilecek bir başka eleştiri konusudur. G-77 ülkeleri[72] ve Çin gibi gruplar, egemen devletlerin ön plana çıkarıldığı daha geleneksel bir modelin benimsenmesi yönünde önerilerde bulunmuşlardır (Josukutty, 2020, s. 66).

[72] Ayrıntılı bilgi için bkz: https://www.g77.org/.

Tablo 5. Paydaşların Rolüne İlişkin Kuzey-Güney kutuplaşması

Açıklama	Güney'in Görüşü	Kuzey'in Görüşü
Egemen devletlerin rolü	Maksimum	Minimum
Özel sektörün rolü	Minimum	Maksimum
Sivil toplumun rolü	Minimum	Maksimum

Kaynak: Tablo, yazar tarafından Josukutty'den (2020) alınan bilgilerle oluşturulmuştur.

IGF, internetin yönetişiminde önemli bir rol oynamakla birlikte, bazı önemli eleştirilere de maruz kalmaktadır. En önemli eleştirilerden biri, çok paydaşlı bir yapıya sahip olmasına rağmen yeterince kapsayıcı olmamasıdır. Kapsayıcılık bağlamında yapılan eleştiriler genellikle aşağıdaki gibi özetlenebilir (Creech vd., 2009, s. 9):

- *Devletlerin Katılımı:* Birçok devlet, IGF'ye aktif olarak katılmamaktadır. Bu durum, internetin yönetişiminde devletlerin önemli bir rol oynadığı göz önüne alındığında önemli bir eksiklik olarak değerlendirilmektedir.
- *Sivil Toplumun Katılımı:* Sivil toplumun geniş bir yelpazesini temsil eden kuruluşların IGF'ye katılımı sınırlıdır. Bazı önemli sivil toplum alanları yeterince temsil edilmemektedir.
- *Özel Sektörün Katılımı:* Özel sektörün IGF'ye katılımı, internet hizmetlerinden yararlanan işletmelerden ziyade BİT sektörü üzerinde yoğunlaşmaktadır.
- *İnternet Topluluğunun Katılımı:* İnternet servis sağlayıcıları ve ulusal kayıtlar gibi internet topluluğunun bazı önemli bölümleri IGF'de zayıf bir şekilde temsil edilmektedir.
- *Kullanıcıların Katılımı:* Hem ticari hem de bireysel kullanıcıların ve onları temsil eden kuruluşların IGF'ye katılımı sınırlıdır.

Shcherbovich, IGF'nin çok paydaşlı yaklaşımının da bazı olumsuz yönleri olduğu belirtmektedir. Bu olumsuz yönler şu şekilde sıralanabilir (2017, s. 10):

- *Uluslararası Anlaşmaların Eksikliği:* Çok paydaşlı forumlar, uluslararası anlaşmalar yapma yetkisine sahip değildir. Bu nedenle, bu forumlarda alınan kararlar ve öneriler bağlayıcı değildir.
- *Farklı Yasal Yorumlar:* Farklı ülkeler, uluslararası yasal çerçeveyi farklı şekilde yorumlayabilir ve uygulayabilir. Bu durum, tutarsızlıklara ve eşitsizliğe yol açabilir.

- *Etik ve Yasal Olmayan Temeller:* Çok paydaşlı forumlarda alınan kararlar ve öneriler, her zaman yasal veya etik temellere dayanmayabilir.
- *Katılım Sorunları:* Zaman kısıtlamaları, çıkar çatışmaları ve diğer engeller, tüm paydaşların etkin katılımını engelleyebilir.
- *Karar Alma Zorluğu:* Farklı paydaşlar arasında çıkar çatışmaları olması, önemli kararlar üzerinde fikir birliğine varılmasını zorlaştırabilir.
- *Güç Dengesizliği:* Büyük şirketler ve devletler gibi bazı paydaşlar, diğer paydaşlara göre daha fazla güce ve etkiye sahip olabilir.
- *Meşruiyet Sorunu:* Çok paydaşlı forumların meşruiyeti ve hesap verebilirliği sorgulanabilir.

IGF'nin tartışılmaz başarısına ve önemine rağmen, birçok ulusal ve bölgesel yan kuruluşun oluşumu bir yana, politika oluşturma sürecinin sadece başlangıç aşamalarıyla - yani gündem belirleme ve konuları şekillendirme - sınırlı kaldığı görülmektedir. İyi örneklerin belgelenmesine yönelik önemli adımlar atılmasına rağmen, internet yönetişimi için gerekli uluslararası düzenlemelerin uygulanması ve yürürlüğe konması konusunda, belirli konularda sürekli işbirliği yapılabilmesini sağlayacak etkili araçlar henüz geliştirilmemiştir (de La Chapelle & Fehlinger, 2016, s. 10).

4.2.2.2.Paydaş Sorunları

IGF'de, internet yönetişimine ilişkin politikaları ve düzenlemeleri belirleyen çeşitli paydaş grupları temsil edilmektedir. "Paydaş" teriminin kullanılması, farklı gruplar arasında dolaylı olarak bir tür eşit statü oluşturmuştur. Bu, kuşkusuz 180'den fazla ülkenin kabul ettiği resmî belgelerde bir "ilki" teşkil etmektedir (de la Chapelle, 2007, s. 23). Bu gruplar arasında, ulusal hükümetler, internetin altyapısı ve hizmetleri üzerinde önemli bir etkiye sahip olan internet servis sağlayıcıları, teknoloji firmaları ve diğer ticari kuruluşlar gibi özel sektör temsilcileri bulunmaktadır. Ayrıca, internetin sosyal, etik ve hukuki yönlerine odaklanan hak temelli gruplar, akademisyenler ve teknoloji uzmanlarından oluşan sivil toplum kuruluşları; internetin teknik altyapısını ve standartlarını geliştiren IETF, W3C gibi kuruluşlar ve akademik topluluklar ve internet yönetişimi konusundaki küresel çabaları destekleyip koordine eden BM gibi uluslararası ve bölgesel organizasyonlar yer almaktadır. Bu geniş yelpazedeki aktörler, internet yönetişimindeki çeşitli rolleri ve sorumluluklarıyla, internetin adil, açık ve erişilebilir bir platform olarak kalmasını ve kullanıcı haklarının korunmasını sağlama konusunda kritik öneme sahiptirler.

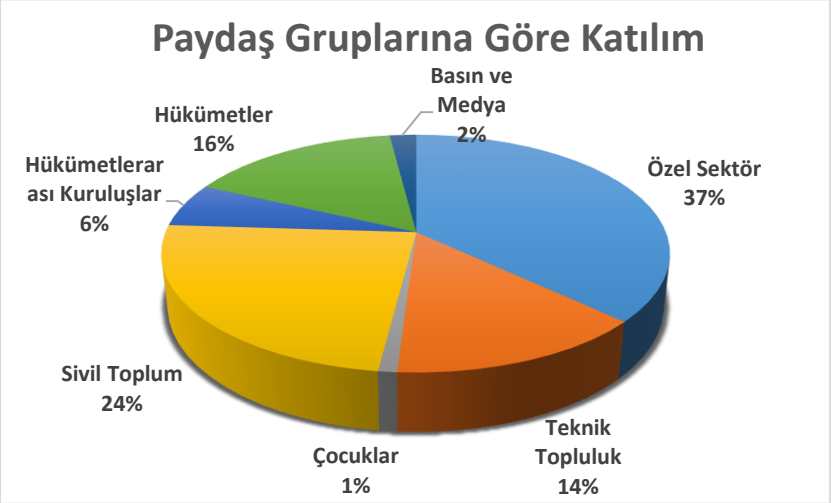
Tablo 6. IGF'nin Paydaş Sorunlarına Yönelik Zorlukların Kategorizasyonu

Zorluk Kategorisi	Açıklama
Temsil	Tüm paydaşların katılımını teşvik etmeyi amaçlasa da, bazı gruplar (özellikle gelişmekte olan ülkelerden ve sivil toplumdan gelen katılımcılar) finansal ve lojistik kısıtlamalar nedeniyle yeterince temsil edilememektedir.
Gündem Belirleme	IGF'nin gündemi, tüm paydaşların görüşlerini yansıtacak şekilde belirlenmesi gerekmesine rağmen, bazı hükümetler ve özel sektör aktörleri gündem üzerinde belirleyici bir rol oynamaya çalışmaktadır. Bu durum, bazı paydaşların seslerinin yeterince duyulamamasına yol açmaktadır.
Güç Politikaları	IGF, eşit katılım ve diyalog ilkelerine dayanmasına rağmen bazı paydaşlar, diğerlerinden daha fazla güce ve etkiye sahiptir. Bu durum bazı paydaşların diğerleri üzerinde baskı kurmasına ve kendi çıkarlarını gözetmesine yol açmaktadır.

Kaynak: Tablo, yazar tarafından oluşturulmuştur.

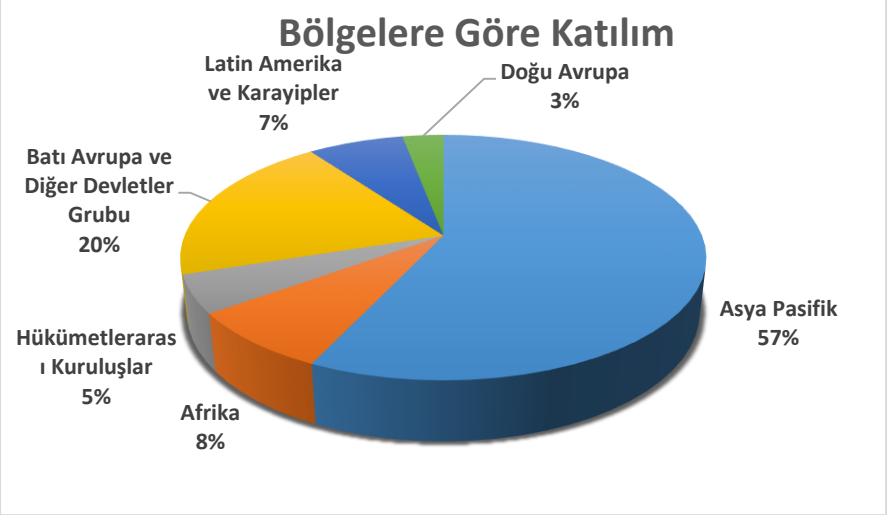
Yukarıdaki tablo, IGF'nin temsil, gündem belirleme ve güç politikalarıyla ilgili temel zorluklarına ve bu zorlukların katılımcıların eşitliği ve etkinliği üzerindeki etkilerine işaret etmektedir. Benzer şekilde aşağıdaki iki grafik, IGF'nin temsil ve katılım sorunlarını yansıtmak açısından önem arz etmektedir. Asya Pasifik bölgesinin yüksek oranda temsil edilmesine karşın, Doğu Avrupa ve Afrika gibi diğer bölgelerin düşük katılım oranları, tüm paydaşların katılımını teşvik etme hedefinin tam olarak gerçekleşmediğini göstermektedir. Bu durum, finansal ve lojistik kısıtlamaların bu bölgelerdeki katılımcıları olumsuz etkilediği savını güçlendirmektedir. Öte yandan özel sektörün gündem belirlemede en yüksek katılım oranına sahip olması, bu aktör grubunun gündem üzerinde belirleyici rol oynama potansiyelini ortaya koymaktadır. Aynı zamanda, bazı hükümetlerin ve özel sektör aktörlerinin gündem üzerindeki ağırlıklarının, diğer paydaşların seslerinin yeterince duyulmamasına yol açabileceği endişeleriyle de örtüşmektedir. Bu durum, IGF'nin eşit katılım ve diyalog ilkeleriyle çelişen bir görünümü yansıtmaktadır.

Grafik 2. IGF 2023 Toplantısı Paydaş Gruplarına Göre Katılım Oranları



Kaynak: (IGF, 2023).

Grafik 3. IGF 2023 Toplantısı Bölgelere Göre Katılım Oranları



Kaynak: (IGF, 2023).

Görünürde IGF'de devletler, şirketler ve sivil toplum arasındaki güç dengesini yansıtan karmaşık bir yapıdadır. Ancak devletler, internet üzerindeki kontrolü sağlamak için düzenleme, erişim engelleme ve polislik gibi araçlara başvururken, bazı şirketler internet içeriğine neyin izin verileceğine dair kurallar koyarak devlete benzer bir otorite sergiler. Zamanla, bu şirketler vatandaşların verileri üzerinde kontrol sağlama, dijital haritalar oluşturma ve hatta resmi iletişim hizmetleri sunma gibi geleneksel olarak devlete ait olan işlevleri üstlenmişlerdir (Pigatto vd., 2021, s. 5).

Kurbalija tarafından önerilen "değişken geometri" yaklaşımı, internet yönetişiminin karmaşık ve çok katmanlı bir süreç olduğunu ve farklı paydaşların farklı düzeylerde katılımını gerektirdiğini savunmaktadır. Ona göre internet yönetişimi, devletler, uluslararası kuruluşlar, sivil toplum kuruluşları, özel sektör ve teknik topluluk gibi çeşitli paydaşların katılımını gerektirir. Her bir paydaşın farklı yetenekleri, uzmanlık alanları ve çıkarları vardır. Bazı paydaşlar, diğerlerinden daha fazla uluslararası yasal güce sahip olabilir (2014, s. 234). Örneğin, devletler, uluslararası antlaşmalar aracılığıyla internet yönetişimini etkileyebilir. Farklı paydaşlar, internet yönetişiminin farklı konularına ilgi duyabilir. Örneğin, sivil toplum kuruluşları, internet özgürlüğü ve ifade özgürlüğü gibi konulara odaklanabilirken, özel sektör, e-ticaret ve fikri mülkiyet hakları gibi konulara daha fazla ilgi gösterebilir. "Değişken geometri" yaklaşımı, her bir paydaşın katılımının, yukarıda bahsedilen faktörlere bağlı olarak değişebileceğini savunmaktadır. Örneğin, bazı konularda tüm paydaşların eşit katılımı sağlanabilirken, diğer konularda belirli paydaşların daha fazla rol oynaması gerekebilir.

Dört yıllık bir süreçte sivil toplum ve özel sektör paydaşları, internet yönetişimiyle ilgili tamamen hükümetlerarası olarak başlayan bir sürece meşru katılımcılar olarak kabul edilmek ve tanınmak için önemli bir mücadele verdi. Bu mücadele, BM zirveleri tarihinde bir ilk olma özelliğini taşıyor ve sonuçları zamanla daha net görülebilecek bir emsal teşkil ediyor (de la Chapelle, 2007, s. 20; Cogburn, 2017, s. 208). Sivil toplum ve özel sektörün internet yönetişiminde meşru katılımcılar olarak tanınması, tartışılmaz yetkinlikleri ve meşruiyetleri sayesinde mümkün olmuştur. Bu aktörler, çoğu devletin dikkatini bile çekmeyen bir dönemde küresel erişim ve başarıya sahip bir ağı kendi başlarına icat edip geliştirmişlerdir. Aynı zamanda, "internet topluluğu" olarak bilinen teknisyenler ve iş dünyasından oluşan grup, internetin doğasının ikinci kez değiştiğini kabul etmek zorunda kalmışlardır (de la Chapelle, 2007, s. 20).

WSIS sürecinde, özellikle gelişmekte olan ülkeler açısından bakıldığında en çok endişe yaratan internet yönetişimi sorunlarından biri sivil toplumun IGF'deki rolünün hala çok açık olmamasıydı (Purcell vd., 2006, s. 15). Üstelik sivil toplumun rolü, meşruiyeti ve temsiliyeti konusundaki tartışmalar halen devam etmektedir. Bu tartışma, WSIS'in ilk yıllarında da açıkça etkisini göstermiştir. Zirveyi kuran BM kararında sivil toplum aktörlerinin tam katılımı açıkça gerekli kılınmasına rağmen, müzakerelerin ilk aşamalarında birçok devlet, bu durumun diğer tartışmalar için bir emsal teşkil

edeceğinden endişe duyarak uygulamanın hükümetlerarası niteliğini korumaya çalışmıştır (de la Chapelle, 2007, ss. 22-23).

Mevcut durumda da toplantılara çok sayıda STK katılmasına rağmen, belirli bir paydaş grubu hakimiyet kurmaktadır. Birçok katılımcı kendilerini sivil toplum olarak tanımlasa da -bireyler ve teknik topluluk üyeleri gibi- aslında farklı paydaş gruplarını temsil ediyor olabilir. Bu durum, IGF'ye kendi paydaş grubunda katılımın sınırlı kalmasına sebebiyet vermektedir. Özellikle çoğu paydaş grubu – akademi ve basın gibi – "diğer" etiketinin altında listelenmiş ve net bir kategorizasyon oluşturulamamıştır (Meyer & Shahin, 2021, s. 3). Bu nedenle sivil toplumun tek bir homojen yapı olarak değil, farklı çıkar grupları ve hedefleri olan bir grup olarak ele alınması gerektiği ifade edilmektedir. Yani sivil toplum için "amaç odaklı bir tipoloji" önerilmektedir (Meyer & Shahin, 2021, s. 14).

Mueller, IGF toplantılarında sivil toplum ve teknik topluluklar arasında yaşanan tartışmalara dikkat çekmiştir. Teknik topluluğun temsilcileri, ICANN ile RIR'lerin kâr amacı gütmeyen kuruluşlar ve dolayısıyla sivil toplumun parçası oldukları konusunda ısrar etmişlerdir. Teknik topluluk, kendini kâr amacı gütmeyen ve gönüllü temelli gruplar olarak görürken; sivil toplum bu grupların aslında mevcut sistemi korumaya çalışan ve IGF'deki bağımsız eleştirilere karşı kendilerini savunma amacı güden organizasyonlar olduğunu ileri sürmektedir. Bu durum, farklı gruplar arasında önemli görüş ayrılıklarına sebebiyet vermiştir. Katılımcılar, özellikle forumun hangi konuları tartışması gerektiği konusunda farklı görüşlere sahip olmuşlardır. Mueller tarafından "forum güvercinleri" olarak adlandırılan teknik topluluk, tartışmalı konulardan kaçınıp daha az çatışma yaratan konulara – erişim ve kritik internet kaynakları gibi – odaklanmak isterken; forumun daha cesur ve etkili olmasını savunan "forum şahinleri" ise tartışmalı konuların – ifade özgürlüğü, sansür, gizlilik gibi – ele alınıp bu konularda ilerleme kaydedilmesini istemiştir (2010, s. 117).

Bu süreçte özellikle bazı teknik topluluk kuruluşları, internet yönetişimi konusundaki tutumlarıyla gündeme gelmiştir. Örneğin ISOC, başlangıçta "internet yönetişimi" kavramını reddederek, sadece "teknik koordinasyon" olduğunu savunmuştur. Bu görüş, internet yönetişimi konusundaki tartışmaların geçersiz olduğu iddiasındayken; zamanla bu iddia IGF'nin gereksiz olduğu yönünde bir görüşe evrilmiştir. Ancak IGF kurulduğunda ve etkili bir platform olarak kabul görmeye başladığında, teknik topluluk

IGF'nin yönetim grubu (MAG) içinde etkin rol almak için yoğun lobi çalışmaları yürütmeye başlamıştır. Bu topluluğun ana hedefi, IGF'nin gündemini gelişmekte olan ülkelerde internet erişimini artırmaya odaklanırken, kritik internet kaynaklarıyla ilgili politika meselelerinden uzak durması yönünde baskı yapmaktı (Mueller, 2010, s. 117).

IGF'nin gündemindeki tartışmalar, forum katılımcılarının forumun tartışmalı konularla ne kadar ilgilenmesi gerektiği konusundaki farklı isteklerinden kaynaklanmaktadır. "Forum güvercinleri" adı verilen bir grup, tartışmalı konuları gündemden çıkararak daha az tehditkâr konulara odaklanmak isterken; daha güçlü bir forum isteyenler, tartışmalı konuları ele alarak bu konularda ilerleme kaydetmek istiyor. Özellikle, WSIS'te çözülemeyen "kritik internet kaynakları" yönetişimi ve "geliştirilmiş işbirliği" çağrıları gibi konular, tartışmanın odağında yer alıyor.

Bu bağlamda sivil toplum aktörleri, küresel yönetişim süreçlerine katılımıyla hem “piyon” hem de “ortak” rolü üstlenmektedirler. NETmundial gibi önemli konferanslardaki rollerine dair eleştiriler, sivil toplumun zengin ve çeşitli katılımının meşruiyet ve etkinlik açısından kritik öneme sahip olduğunu göstermektedir. Bu katılımcılar, sürecin meşruiyetini artırarak önemli ortaklar haline gelirken, aynı zamanda bu platformlarda süreci etkileyebilme potansiyeline de sahiptirler. Buna rağmen, sivil toplumun katılımının zayıf olduğu söylenebilir (Cogburn, 2017, s. 269).

IGF, daha somut sonuçlar üretebilmek için, diğer IGF topluluk faaliyetlerini tamamlamak amacıyla En İyi Uygulama Forumları (BPF'ler) adında bir ara dönem programı geliştirmiştir. 2018 yılı için BPF, siber güvenlikte kültür, normlar ve değerlere odaklanmaktadır. BPF, süreci, siber uzayda IGF paydaş gruplarının rolleri ve sorumlulukları üzerine önceki çalışmalarını temel alarak ve bu gruplara uygulanan normların neler olduğunu araştırarak başlatmaktadır. Tartışılan sorular arasında, "devlet davranışı" veya "özel sektör davranışı" gibi her paydaş grubunun davranışlarına ilişkin sorular bulunmaktadır. Sivil toplumun norm geliştirmedeki rolü, bireysel kullanıcıların güvenli ve emniyetli online davranışlarına dair sosyal normları da içermektedir. Eğer bir normun evrensel bir uygulaması yoksa, normun uygulanmasının istenmeyen sonuçları varsa veya farklı bir bağlamda (örneğin etkili bir hukuk düzenine sahip olanlar ve olmayanlar arasında) farklı etkileri varsa, bu, normların sunduğu korumada "sahip olanlar" ve "sahip olmayanlar" arasında bir grup yaratabilir (Horenbeeck, 2018, s. 3).

Tüm bu paydaş sorunlarına rağmen IGF, devlet ve devlet dışı aktörlerin internet yönetişimi konularında etkileşimde bulunmaları için sistemli bir çözüm sunarak, bu aktörlerin kamu politikasındaki potansiyel değişiklikler veya içerikle ilgili kararlarda daha aktif bir rol almasını kısıtlama amacı güder. İnternet yönetişimindeki bu çeşitlilik, farklı aktörlerin çeşitli rolleri ve sorumlulukları üstlenmelerine olanak tanır (Pigatto et al., 2021, s. 4). Bu durum, internet yönetişiminin çok katmanlı ve çok aktörlü doğasını yansıtır, farklı perspektif ve çıkarların dengelenmesine yardımcı olur.

4.2.3. IGF'ye Hukuki Bağlayıcılık Kazandırılabilir Mi?

4.2.3.1. Hukuki Bağlayıcılık: Bir Sorun Mu?

Uluslararası politika konferansları, resmiyet derecesi, kaynak taahhüdü ve nihai anlaşma türü gibi çeşitli kriterlere göre farklılık gösteren bir spektrumda yer alır. Spektrumun bir ucunda, resmi kuralların, antlaşmaların ve anlaşmaların formüle edildiği ve kabul edildiği resmi uluslararası konferanslar bulunur. Bu tür konferanslar, genellikle devletlerarası antlaşmaların yapıldığı ve uluslararası hukukun şekillendirildiği yerlerdir. Spektrumun biraz daha az resmi bölümünde ise, bağlayıcı olmayan ilkelerin ve değerlerin oluşturulduğu, uluslararası normların teşvik edildiği toplantılar yer alır. Bu tür konferanslar sıklıkla ITU veya WTO gibi resmi hükümetlerarası kuruluşlar tarafından düzenlenmektedir. Bu aktörler, uluslararası politikada önemli roller üstlenerek, konferansların düzenlenmesi ve yönetilmesi sürecinde önemli bir etkiye sahip olmaktadır. Bu durum, uluslararası ilişkilerin ve diplomasinin yalnızca devletler arasında değil, aynı zamanda çok çeşitli aktörler arasında da gerçekleştiğinin altını çizer (Cogburn, 2017, s. 41).

İşte IGF, uluslararası politika konferansları spektrumunun tam ortasında yer alan ve bağlayıcı olmayan kararların alındığı o platformlardan birini oluşturur. Tunus Gündemi'nin 77. maddesinde şu ifade yer almaktadır: "IGF'nin gözetim işlevi olmayacak ve mevcut düzenlemelerin, mekanizmaların, kurumların veya kuruluşların yerini almayacak, ancak onları da dahil edecek ve uzmanlıklarından yararlanacaktır. Tarafsız, ikilik yaratmayan ve bağlayıcı olmayan bir süreç olarak oluşturulacaktır. İnternetin günlük ya da teknik operasyonlarına hiçbir müdahalesi olmayacaktır." (Tunus Gündemi, 2005, Mad. 77).

2006 yılındaki IGF toplantısı, uluslararası internet yönetişimi konusunda diyalog ve işbirliği için önemli bir platform olarak kabul edilmiş olmasına rağmen, somut eylem

planları ve karar alma mekanizmalarının eksikliği nedeniyle forumun etkinliği konusunda soru işaretleri yaratıyor. Katılımcılar, IGF'nin diyalog ve en iyi uygulamaların paylaşımı için kritik bir platform olduğu konusunda hemfikir olmakla birlikte, ulusal ve küresel düzeyler arasında etkili bir köprü kurmanın ve internetin merkezi olmayan doğasını korumanın zorluklarına dikkat çekiyorlar. Phil Bond, forumun gelişmekte olan dünyada inovasyon ve insan odaklı yaklaşımları teşvik ederek mevcut durumdan ileriye doğru bir adım atma potansiyeline sahip olduğunu vurgularken, somut eylemlere geçiş konusundaki belirsizlikleri de dile getiriyor. Lynn St. Amour, IGF'nin karar alma veya öneri sunma yetkisi olmadığını, bunun yerine zengin bir diyalog ortamı sunduğunu belirtirken; yerel düzeye odaklanmanın yanı sıra internetin merkezi olmayan yapısının korunması gerektiğinin de altını çiziyor. Karen Bankalar, ulusal ve küresel düzeyde etkili bağlantı kurmanın zorluklarına işaret ederken, IGF'nin farklı paydaşlar arasında diyalog kurma konusunda önemli bir rol oynayabileceğini ifade ediyor. Jean-Jacques Massima Landji ise, siber güvenlik gibi konularda uluslararası işbirliğinin önemini vurgulayarak, IGF'nin tavsiye verme gücü olmamasına rağmen, ortak zemin bulma çabalarının kritik olduğunu belirtiyor (IGF, 2006, ss. 118-119). Bu çeşitli perspektifler, IGF'nin uluslararası internet yönetişimi konusunda kritik bir platform olduğunu gösterirken, somut eylemlere geçiş ve etkili karar alma mekanizmaları konusunda ilerleme kaydetmenin önemi üzerinde durulmaktadır. Bu bağlamda, IGF'nin bağlayıcı olmayan tavsiyeleri, devletlerin ve uluslararası topluluğun internet yönetişimi konularında bilinçlenmesi ve kapasite geliştirmesi için bir fırsat sunar, ancak nihai politika oluşturma süreci ulusal düzeydeki mevzuata ve uluslararası hukuka tabidir.

IGF'nin kendi kararlar alamamasının birkaç temel sebebi bulunmaktadır: Birincisi; devletler, internet yönetişimi ile ilgili konularda kendi egemenliklerini korumak istemektedir. Bu durum, IGF'nin uluslararası hukukta yer alan bağlayıcı antlaşmalar ve yasalar oluşturamamasının temel nedenidir. Keza internetin kontrolü üzerine yapılan tartışmalar, geleneksel Westphalian devlet egemenliği kavramının, küresel internet yönetişiminde belirleyici bir norm olmaya devam ettiğini göstermektedir. Bu görüşün savunucuları, internetin sınırsız dünyasını tanıyıp kabul etmekle birlikte internet yönetişiminde, tıpkı geçmişteki iletişim sistemlerinde olduğu gibi, devletler ve yasalar tarafından yönlendirilmesi gerektiğini vurguluyorlar. Bu, devletlerin ve uluslararası hukukun, internet yönetişiminin temel taşları olması gerektiğini savunan çok taraflı bir

yaklaşımı ifade eder. Bu yaklaşım, her ne kadar resmi olarak çok paydaşlı yönetişim anlayışına karşı olmasa da, onu farklı bir perspektiften ele alır. İnternet özgürlüğüne dair savunular, politika yapım sürecine kamu, özel sektör ve sivil toplumun eşit katılımını vurgularken; internet egemenliği anlayışı, devlet dışı aktörlerin tartışmalara katılma hakkını kabul eder fakat nihai politika belirleme yetkisini yalnızca devletlere bırakır (Budnitskiy, 2018, s. 102).

Egemenlik meselesini en iyi şekilde özetleyen cümle belki de IGF'nin 2006 tarihli ilk toplantısında salondan yükselen bir sesti: "Küreselleşmiş çok dilli bir İnternet için çalışırken, ulusal egemenlik meselesiyle nasıl başa çıkacağız? […] Teknoloji egemenlik argümanını atlamamıza izin veriyor mu?" (IGF, 2006, s. 174). Esasında bu yaklaşım, devlet merkezli egemenlik anlayışı ile sınır tanımayan dijital alanın çatışmasını vurgular. Diğer bir deyişle IGF'nin bağlayıcı olmayan karar alma yapısı, çok paydaşlığın sınırlarını ortaya koymaktadır. Bu yapı, küresel siber alanın yönetişimi için geniş katılımlı bir diyalog ve işbirliği ortamı sunsa da, somut politika değişiklikleri ve uygulamaları konusunda yeterli yetkiye sahip olmaması, her şeyden önce, egemenliği öne süren bakış açısının bir sonucudur.

İkincisi, farklı devletlerin internet yönetişimi ile ilgili farklı öncelikleri ve yaklaşımları bulunmaktadır. Bu durum, IGF'nin tüm paydaşların kabul edebileceği somut kararlar almasını zorlaştırmaktadır. IGF'nin kapsamının genişletilmesine karşın, ITU gibi bazı platformlarda alınan kritik kararlar, demokratik olmayan veya otoriter rejimlere sahip ülkeler de dahil olmak üzere, internet düzenlemesi konusunda farklı çıkarları olan ülkeler arasında gerçekleşmektedir. BM'nin IGF'yi kurmasındaki motivasyonun önemli bir kısmı bile, ABD merkezli ICANN'e karşı bir denge oluşturmaktı. Ancak ICANN'in aksine IGF'ye bağlayıcı kararlar alma yetkisi dahi verilmemiştir (Lahmann vd., 2017, ss. 34-35).

Üçüncüsü; IGF, çok paydaşlı bir platformdur. Bu platformda devletlerin yanı sıra sivil toplum kuruluşları, özel sektör ve teknik topluluk da yer almaktadır. IGF'nin tüm paydaşların görüşlerini dengelemek zorunda olması, karar alma sürecini karmaşık hale getirmektedir. Özel sektörün genel eğilimi, bağlayıcı kararlara ve aşırı düzenlemeye karşı olmaktır. Özel sektör, katı kurallar ve düzenlemelerin bürokrasiyi artıracağına, yeniliği engelleyeceğine ve yatırımları caydıracağına inanmaktadır. Bu bağlamda, özel sektör, sağlıklı pazar rekabetinin teşvik edilmesi, pazara girişte herhangi bir yasal

engelin bulunmaması ve lisanslama sürecinin kolaylaştırılması gibi unsurları ön plana çıkarır. Ayrıca, son kullanıcı hizmet sağlayıcılarının devletlerin mülkiyetinde olmaması, uluslararası ağ geçitlerine ve kablolarına makul piyasa oranlarında erişim, fiyatlandırma ve hizmet seçeneklerinin şeffaflığı, ön ödemeli ve kademeli fiyatlandırma modellerine izin verilmesi ve ağ ile ulusal sınırların aşılmasının önündeki engellerin kaldırılması gibi politikaları savunmaktadır (WG-IMP Report, 2015, s. 23).

Öte yandan sivil toplum kuruluşları ve teknik topluluk ise IGF'nin daha fazla yetkiye sahip olması gerektiğini savunmaktadır. Bu aktörler, IGF'nin bağlayıcı kararlar alabilmesinin internetin daha adil ve daha demokratik bir şekilde yönetilmesine katkıda bulunacağını düşünmektedir. Bu bağlamda sivil toplumun IGF için yürüttüğü lobi faaliyetleri de internet yönetişiminin geleceğinin şekillendirilmesindeki etkisini ve nüfuzunu göstermektedir (Purcell vd., 2006, s. 24).

IGF'nin 2006 tarihli toplantısında, bağlayıcı olmayan tavsiyelerin potansiyel faydasından da söz edilmektedir (IGF, 2006, s. 404). Bu toplantıda IGF'nin hukuki bağlayıcılığının olmamasını olumlu yönde değerlendirenler uzmanlar olmuştur. Toplantıda Jeanette Hofmann, "Forumun bağlayıcı kararlar alma yetkisinin bulunmaması, bu toplantıya katılan tüm paydaşlar arasında eşitliğin sağlanmasının ön koşuludur" ifadesini kullanmıştır. Zira Hofmann'a göre forumun en büyük yeniliği, bağlayıcı kararlar alınmadan, tüm paydaşların eşit olarak katıldığı, küresel bir "*talk shop*"un oluşturulmasıdır. Burada, hükümet delegasyonları, sivil toplum ve özel sektör temsilcileri aynı seviyede yer alır ve söz almak için aynı sıraya girer. Bu yapı, her türlü coğrafi, kültürel, cinsel ve politik sınırları aşarak yeni iletişim ve fikir birliği oluşturma biçimlerini denemek için bir fırsat sunar (IGF, 2006, s. 221).

Hoffmann'ın IGF 2006 toplantısında bağlayıcılık hakkında söyledikleri, forumun bağlayıcı olmayan doğasını ve bu sayede tüm paydaşlar arasında eşitliği sağlama prensibini yansıtır. Bu durum, uluslararası kurumların sahip oldukları dinamizmi bu yolla kazandığını belirten Young'ın görüşlerini hatırlatır. Young'a göre uluslararası kuruluşların etkinliği, büyük ölçüde maddi hükümlerinde değişiklik yapma yeteneklerine bağlıdır. Bu değişiklikler, kurumların değişen koşullara ayak uydurmasına ve yeni zorluklara karşı koymasına olanak tanır. Kabul edilmiş kuralların katılığı, değişiklik yapma sürecinin ne kadar kolay veya zor olacağını belirler. Katı kurallar, değişiklik yapmayı zorlaştırırken, esnek kurallar daha fazla esneklik sağlar

(1992, s. 180). Bu anlamda IGF'nin aldığı kararların katı bir hukuki zorunluluğu olmaması, ona daha esnek ve dinamik yapı kazandırır. Dolayısıyla bu durum, forumun tartışma ve fikir alışverişi için açık bir alan olmasını sağlar ve tüm katılımcıların eşit bir şekilde katılımını kolaylaştırır.

Netice itibariyle, forum bağlayıcı değildir fakat, yetkisi, önerilerinin ve analizlerinin ikna ediciliğinden gelecektir (Mueller & Mathiason, 2006, s. 2). NETmundial'in yol haritasının 35. paragrafı[73], bu noktada IGF'ye bir rol atfetmiştir. Paragrafta, devletlerin gözetim, dinleme ve kişisel veri toplama faaliyetlerini uluslararası insan hakları hukukuna uygun olarak gerçekleştirmeleri gerektiği üzerinde durulurken, aynı zamanda uluslararası düzeyde daha geniş kapsamlı bir diyaloğa ve tüm ilgili konularda ortak bir anlayışın geliştirilmesine olan ihtiyaç vurgulanmaktadır. Bu amaçla, IGF ve İnsan Hakları Konseyi gibi forumların etkin bir şekilde kullanılması gerektiği belirtilmektedir. Bu paragraftan yola çıkarak, IGF'nin hukuki olarak bağlayıcı kararlar alma yetkisi olmadığı, ancak hukukun uygulanmasını teşvik etmek için bir diyalog ortamı olarak görüldüğü sonucuna varabiliriz. Benzer şekilde IGF'nin 2023 toplantısında "Siber Güvenlik, Siber Suç ve Online Güvenlik" teması altında verilen mesajda kullanılan şu ifade dikkat çekicidir:

> Birleşmiş Milletler, gelişmekte olan teknolojilerin değerlendirilmesine yönelik standart ve yönetmeliklerin geliştirilmesini analiz etmek, bilgi ve en iyi uygulamaları paylaşmak ve gelişmekte olan teknolojiler için ortak ilkelerin nasıl geliştirileceğine dair çok paydaşlı fikir alışverişleri için bir platform sağlamak üzere daha fazlasını yapabilir. Bu, ilkeleri bağlayıcı standartlara ve düzenlemelere dönüştürecek doğru kurumlara sahip olmamızı sağlamaya yardımcı olabilir (IGF Summary Report, 2023).

Verilen mesajda, BM'nin gelişmekte olan teknolojiler için ortak ilkelerin geliştirilmesinde daha fazla rol oynaması gerektiği ifade edilmektedir. Aynı zamanda, bu ilkelerin nihayetinde bağlayıcı hale gelmesi için gerekli zemini hazırlaması gerektiği düşünülmektedir. Buradan hareketle, IGF'nin hükümetlerarası kuruluşlar gibi bağlayıcı antlaşmalar ve yasalar oluşturamasa da, kurumları uluslararası hukuka ve uluslararası

[73] "[...] İletişimin gözetlenmesi, dinlenmesi ve kişisel verilerin toplanması, kitlesel gözetleme, dinleme ve toplama dahil olmak üzere, devletlerin uluslararası insan hakları hukuku kapsamındaki yükümlülüklerine uygun olarak yürütülmelidir. Bu konuda, IGF ve İnsan Hakları Konseyi gibi forumlar kullanılarak uluslararası düzeyde daha fazla diyaloğa ihtiyaç duyulmakta ve ilgili tüm hususlarda ortak bir anlayış geliştirilmesi amaçlanmaktadır." (NETmundial, 2014, Par. 35).

normlara uymaya teşvik eden bir yapısı olduğu söylenebilir. Czempiel yönetişimi, "işlerin yapılmasını emredecek yasal yetki olmaksızın işlerin yapılmasını sağlama kapasitesi" olarak tanımlar (1992, s. 250). Dolayısıyla IGF'den böyle bir kapasiteye sahip olması beklenmektedir.

Peki IGF için biçilen bu "kolaylaştırıcı" rol yeterli mi veya küresel internet yönetişimine büyük bir katkı sağlamasına yetiyor mu? Elbette hayır. IGF, tüm paydaşları bünyesinde barındıran bir platform olarak, daha fazla yetkiyi hak ediyor. Zira bugün, küresel internet yönetişimiyle ilgili kronik sorunlardan biri, yönetişim mekanizmalarının aldığı kararların nasıl hayata geçirileceğiyle ilgilidir. Bu bağlamda, mevcut sistemin güçlü yönlerinden biri, ICANN, IETF ve W3C gibi teknik standardizasyon kuruluşlarının belirlediği teknik standartların gönüllü olarak uygulanmasıdır. Geniş çapta kabul görüp uygulanabilen bir yapı, nispeten başarılı olarak kabul edilebilse de, mevcut sistemdeki en zayıf noktalardan biri, IGF gibi bir yapının bağlayıcılığının olmamasıdır (Cogburn, 2017, s. 276). IGF, ilkeler, normlar ve değerler arasındaki uyumu teşvik ederek önemli bir işlev görse de, bu yönlendirmeleri zorunlu kılmak için yaptırım gücüne sahip değildir. Bu durum, IGF'nin yönetişim alanında yalnızca rehberlik ve kolaylaştırıcı bir rol üstlenmesine neden olmaktadır.

Bağlayıcı olmayan tavsiyeler ve kararlar, katılımcıların önerileri ciddiye alma veya uygulama konusunda herhangi bir yükümlülük altına girmemeleri anlamına gelir. Bu, forumun önerilerinin, özellikle de uluslararası düzeyde etkili olması gereken meselelerde, somut sonuçlar doğurmasını zorlaştırır. Yani, IGF'nin tavsiyeleri, devletler veya diğer ilgili aktörler tarafından göz ardı edilebilir veya yalnızca kısmen uygulanabilir, bu da forumun etkinliğini ve etkisini ciddi şekilde sınırlar. Bunun yanında, "talk shop" olarak işlev gören bir platformun, acil eylem gerektiren küresel sorunlara hızlı ve etkili çözümler üretme kapasitesi sınırlıdır. Bu tür bir yapı, tartışma ve fikir alışverişi için değerli bir alan sağlasa da, karar alma süreçlerinin uzamasına ve zamanında müdahale edilmesi gereken meselelerde gecikmelere yol açabilir. Bu durum, IGF'nin küresel internet yönetişimi konularında proaktif ve etkili bir aktör olma kapasitesini sınırlayan bir faktördür.

Sonuç olarak, küresel internet yönetişimi ve uluslararası siber hukukun geliştirilmesinde IGF gibi platformların rolü, giderek artan önem kazansa da IGF'nin potansiyelini tam olarak gerçekleştirebilmesi için, mevcut yapısal özelliklerinin ve

işleyiş mekanizmalarının ötesine geçmesi gerektiği bir gerçek. IGF'nin sadece bir tartışma forumu olarak kalmayıp, uluslararası siber hukuk düzenlemelerinin geliştirilmesinde daha etkin bir rol oynaması için bağlayıcı yetkilere sahip olması gerektiği yönünde bir argüman sunmak, bu bağlamda önemli bir değerlendirme sunar. Böylesi bir argümanın güçlendirilmesi, hukuki olasılıkları göz önünde bulundurmayı ve ardından normatif çözüm önerileri sunmayı gerektirir.

4.2.3.2.Hukuki Olasılıklar

Geçmişte uluslararası hukuk, egemen devletler arasındaki ilişkilere odaklanırdı. Bu sistemde devletler, uluslararası hukukun tek yaratıcıları ve uygulayıcıları olarak kabul edilirdi. Otorite, devlet tarafından tanımlanır ve uygulanırdı (Cutler, 2003, s. 2). Bu yaklaşımın bir çıktısı olarak devlet, uluslararası hukukun tek öznesi/süjesi olarak kabul edilir. Geleneksel olarak uluslararası hukukçular bu kabulü, uluslararası arenadaki diğer aktörlerin faaliyetlerini "hukuki" statüden ziyade "siyasi" statüye indirgemek için öne sürerler (Malcolm, 2008, s. 98). Bununla birlikte, devletler dışındaki aktörlerin faaliyetlerini de kapsayan, konularını daha geniş bir şekilde ele alan, uluslararası hukuku uluslar üstü bir yönetim rejimi, yani belirli durumlarda devlete üstün gelebilecek bir rejim olarak tanıyan uluslararası hukukçular da mevcuttur (Koh, 1997; Diehl & Ku & Zamora, 2003; Peters, 2017; Hildebrandt, 2019; Marelli, 2023).

Geleneksel uluslararası kamu hukukunda devletlerin tek özne kabul edildiği bir bakış açısı hâkim olsa da, günümüzde bu bakış açısı önemli ölçüde değişmiştir. Modern uluslararası hukukta devletlerin yanında uluslararası örgütler, *sui generis*[74] toplumlar, sınırlı yetkili ülkeler, kalıcı olarak tarafsızlaştırılmış devletler ve bireyler de uluslararası hukukun öznesi olarak kabul edilmektedir. Günümüzde uluslararası hukuk, bazı konularda bireylere de hak ve yükümlülükler yüklemektedir. Özellikle insan hakları ve uluslararası ceza hukuku alanlarında bireyler uluslararası hukukun öznesi olarak kabul edilmektedir. Yine de devletler uluslararası hukuki statüye sahip tek varlıklar ve münhasır uluslararası aktörler olmamakla birlikte, uluslararası hukukun birincil özneleridir ve en geniş hak ve yükümlülük yelpazesine sahiptirler. Hak ve yükümlülüklere otomatik olarak sahip olan devletlerin aksine, uluslararası örgütler,

[74]"Sui Generis" Latince bir terim olup, "kendi türünden" anlamına gelir ve uluslararası hukukta benzersiz bir durumu veya sorunu tanımlamak için kullanılır. Bu terim, karşılaştırma yapılacak veya emsal alınacak başka bir durum olmadığını belirterek, bir hukuki durumun ya da sorunun kendi başına bir kategori oluşturduğunu ifade eder. Sui Generis haklarının uluslararası hukuka etkisi, özellikle yerli halkların haklarını değerlendirirken, bu hakların uluslararası hukuk ve düzenlemelerin uygulanması ve yürütülmesinde sui generis olarak kabul edilmesi gerektiğinin anlaşılmasıyla ortaya çıkar (Barton, t.y.).

bireyler ve diğerleri uluslararası hukuktaki hak ve yükümlülüklerini doğrudan belirli belgelerden alırlar. Örneğin bireyler, her ikisi de 1976 yılında yürürlüğe giren Ekonomik, Sosyal ve Kültürel Haklar Uluslararası Sözleşmesi ve Medeni ve Siyasi Haklar Uluslararası Sözleşmesi uyarınca uluslararası hukuk kapsamındaki haklarını ileri sürebilirler (Shaw, t.y.).

Uluslararası sivil toplum kuruluşları, çok uluslu şirketler ve uluslararası örgütler gibi aktörler, uluslararası normların ve kuralların oluşturulmasına ve uygulanmasına katkıda bulunmaktadır. Resmi olmayan normatif yapılar ve "yumuşak hukuk" araçları da uluslararası düzende önemli bir rol oynamaya başlamış; yeni bir ulusötesi hukuk düzeni şekillenirken, geleneksel devlet odaklı ve pozitivist uluslararası hukuk ve "kamu" otorite kavramları değişime uğramıştır. Bu değişimde, devlet dışı hukuk, resmi olmayan normatif yapılar ve "özel" ekonomik güç ve otorite gibi unsurlar önemli bir rol oynamıştır. Bu yeni yasal düzen, hem yerel hem de küresel düzeydeki yönetişimde önemli dönüşümler gerçekleştirmiştir (Cutler, 2003, s. 2).

Devletlerin egemenliği ve uluslararası hukukun temel ilkeleri, küresel düzeydeki düzen ve istikrarın temel taşları olarak önemini halen korumasına rağmen, yeni ulusötesi hukuk düzeninin ortaya çıkışı, bu sabit yapıları test eden yeni zorluklar getirmektedir. Bu yeni dönemde, devlet dışı aktörlerin artan etkisi, meşruiyet ve hesap verebilirlik gibi konuları daha karmaşık hale getirmekte; uluslararası hukukun uygulanmasında ise eşitsizlik riskini artırmaktadır. Bu durum, uluslararası hukukun evrensel ilkelerinin korunması ve herkes için adil bir şekilde uygulanması noktasında önemli sorunları beraberinde getirmekte ve uluslararası toplumun bu yeni zorluklarla başa çıkabilmesi için yenilikçi çözümler geliştirmesi gerekliliğini ortaya koymaktadır.

Bazıları uluslararası hukukun geçirdiği bu dönüşümü “uluslararası hukukun parçalanması” olarak ifade etmektedir (Treves, 2009; Cogan, 2011; Peters, 2017; Chawla, 2021). "Uluslararası hukukun parçalanması" terimi, hem bu hukukun göreceli bir şekilde parçalanmış hale gelmesini anlatan bir süreci hem de bu parçalanmışlığın sonucunu ifade eder. Parçalanma teşhisi, 1989'dan sonra uluslararası hukukun yeni ve uzmanlaşmış alt alanlarının hızlı büyümesine, devletlerin yanı sıra uluslararası örgütler, STK'lar ve işletmeler gibi yeni aktörlerin yükselişine ve kabul edilen kaynakların dışında yeni uluslararası norm türlerinin ortaya çıkmasına atıfta bulunur (Peters, 2017, ss. 672-673).

BM Genel Kurulu'nun 2006 tarihli "Uluslararası Hukukun Parçalanması: Uluslararası Hukukun Çeşitlenmesi ve Genişlemesinden Kaynaklanan Zorluklar" adlı raporunda uluslararası hukukta meydana gelen parçalanmanın nedenleri, bu durumun yol açtığı zorluklar ve olası çözüm yolları detaylı bir şekilde tartışılmaktadır. Rapora göre uluslararası hukukun parçalanması, farklı alanlar ve normlar arasında tutarsızlıklar ve farklılıklar ortaya çıkarmaktadır (UNGA, 2006).

Raporda parçalanmanın nedeni olarak sıralanan iki madde, geleneksel uluslararası hukukun parçalanmışlığına atıfta bulunsa da, siber alanın neden özgün bir hukuka ihtiyaç duyduğunu anlamak açısından da büyük önem taşımaktadır. Zira parçalanmanın ilk nedeni olarak gösterilen "farklı aktörlerin farklı arayışları ve tercihleri" siber alanla uyumludur. İkinci neden olarak gösterilen "sorunlu alanlarla ilgili yaşanan değer ve çıkar çatışması" ise hem alanın mahiyeti hem de yarattığı çatışma ortamı ile uyum sağlamaktadır. Siber alanda faaliyet gösteren farklı aktörlerin farklı çıkarları ve öncelikleri vardır. Devletler, ulusal güvenlik ve egemenliklerini korumaya öncelik verirken, STK'lar insan hakları ve dijital özgürlükleri korumaya odaklanabilir. Özel sektör ise ticari çıkarlarını ve kârlarını maksimize etmeye çalışır. Bu farklı arayışlar ve tercihler, siber alanda uygulanacak hukukun içeriği ve yorumu konusunda anlaşmazlıklara yol açabilir. Dolayısıyla parçalanma olarak nitelendirilen durum, yeni bir düzenin ortaya çıkma isteğidir. Bu denli yeni bir alana eski bir hukuk mekanizmasını dayatmak, hukukun değil, alanın kendisini parçalayacak bir girişim olacaktır.

Buna rağmen uluslararası hukuk – ve elbette onun süjeleri – halen uluslararası hukukun geçirdiği bu dönüşüme uygun hareket etmekten imtina etmektedir. Uluslararası hukukun geçirdiği dönüşümün hem teorik hem de pratik düzeyde kabul edilmesinin zorunluluğu, küreselleşen bir sistemde giderek daha karmaşık hale gelen uluslararası ilişkilerin gerektirdiği bir gerçekliktir. Günümüzde, siber alanın yükselişi, iklim değişikliği, uluslararası terörizm, pandemiler ve çok uluslu şirketlerin faaliyetleri gibi küresel sorunların yarattığı “küresel risk toplumu” uluslararası hukukun sadece devletler arası bir düzenleme mekanizması olarak kalmaması gerektiğini açıkça ortaya koymaktadır. Bu yeni zorluklar, uluslararası hukukun kapsamını genişletmekte ve hukukun uygulanabilirliğini ve etkinliğini artırmak için çeşitlilik ve esneklik talep etmektedir.

Uluslararası hukukun parçalanması, çeşitlenen aktörler ve artan normatif yapılarla birlikte bir zayıflık olarak görülse de, bu durum aynı zamanda uluslararası hukukun evrim geçirerek daha bütüncül ve etkileşimli bir yapıya büründüğünün de bir göstergesidir. Bu yeni yapı, farklı düzeylerde ve alanlarda spesifik normlar aracılığıyla daha geniş bir yelpazede adalet sağlama potansiyeline sahiptir. Örneğin, siber güvenlikle ilgili uluslararası normların geliştirilmesi ve buna yönelik normların inşa edilmesi, uluslararası hukukun çeşitlenen ve genişleyen yapısının önemli faydalarından bazılarıdır.

Bu bağlamda IGF gibi platformların hukuki bağlayıcılık kazanamaması, uluslararası hukukun modern zorluklar karşısında adaptasyon ve yenilikçilik konusunda yetersiz kaldığının bir göstergesidir. Bu durum, uluslararası hukukun devlet dışı aktörlerin artan önemini ve teknolojik ilerlemenin getirdiği yeni sorunları ele almak için gerekli araçlara sahip olmadığını göstermektedir. Dolayısıyla, modern uluslararası hukukun mevcut yapıları ve mekanizmalarının bu yeni zorluklarla başa çıkmak için yeterli olmadığı söylenebilir. Bu eksiklikler, uluslararası hukukun evrensel ilkelerinin korunması ve adil bir şekilde uygulanması noktasında ciddi engeller teşkil etmektedir. Bu nedenle, özellikle internet yönetişimi gibi bir alanda, geleneksel hukukun sınırlarını aşan, internetin gerektirdiği kapsayıcılığı karşılayabilen bir hukuk mekanizmasının inşası zorunlu hale gelmiştir. Bu hukuk mekanizmasının ilk adımı da, halihazırda iyi yönetişim unsurlarını karşılayan ve bunu normatif bir çerçeveye oturtmaya çalışan bir platforma bağlayıcı yetki verilmesi olabilir.

4.2.3.3.Hukuki ve Normatif Çözüm Önerileri

IGF'nin önerilerinin etki kapasitesinin genişletilmesi ve uygulanabilirliğinin artırılması yönündeki taleplere cevaben, birtakım normatif öneriler geliştirilebileceği kanısına varılmıştır. IGF'nin önerilerinin bağlayıcılık kazanması, belirli hukuki süreçler ile yapısal değişiklikler aracılığıyla teorik olarak mümkündür. Böyle bir dönüşüm, uluslararası hukuk ve uluslararası ilişkilerin temel ilkeleri çerçevesinde, dikkatli bir şekilde ele alınmalıdır. Bu sürecin başarısı, farklı paydaşların çıkarlarını dengeli bir şekilde gözeten ve IGF'nin çok paydaşlı yapısını koruyarak, daha etkili ve uygulanabilir politika önerileri geliştirmeyi hedefleyen bir yaklaşım gerektirir. Bu saikle, tüm bu hususlar göz önünde bulundurularak aşağıda birtakım hukuki ve normatif çözüm önerileri sunulmuştur:

Uluslararası Kuruluşların Güçlendirilmesi: IGF, BM çatısı altında faaliyet göstermektedir. Bu nedenle, BM Genel Kurulu gibi organlar aracılığıyla IGF'nin statüsünün ve yetkilerinin güçlendirilmesi mümkün olabilir. Zira BM Genel Kurulu'nun kararları bile, hatta oy birliği ile alınanlar dahi, belirli istisnalar haricinde (BM'nin kendi iç işleyişine ilişkin meseleler veya Güvenlik Konseyi seçimleri gibi BM'nin yetki alanı içindeki konular) bağlayıcı nitelik taşımaz. Bununla birlikte, bu kararlar resmi olarak zorunlu olmasa da, örf ve âdet hukukunun ilan edilmesine veya gelişimine katkıda bulunabilirler. AB gibi kuruluşlarda dahi –hukuk düzeni ve kanun yapma konularını ayrıntılı olarak düzenleyen kurucu anlaşmalarda bile– bağlayıcı olmayan hükümler yer alabilmektedir (Faix, t.y., ss. 78-79).

Halihazırda birincisi 2013, ikincisi 2017 tarihinde yayınlanmış olan Orijinal Tallin El Kitabı ve Tallinn El Kitabı 2.0'a ek olarak, şu anda hazırlanmakta olan Tallinn 3.0 bu noktada önemli bir adım atmayı hedeflemektedir. El Kitabının güncellenmesi ve geliştirilmesi, siber operasyonlar ve devletlerin buna verdiği tepkilerin sürekli değişen doğasını yansıtmayı amaçlamaktadır. Bu çerçevede, mevcut devlet uygulamaları ve devletlerin uluslararası hukuka ilişkin resmi beyanlarına ek olarak, BM ve bölgesel düzeydekiler gibi uluslararası forumların faaliyetleri ve beyanları, akademik çalışmalar ve devletler, özel sektör ve sivil toplumu içeren çok paydaşlı girişimler de dikkate alınacaktır. Tallinn El Kitabı'nın güncellenmesi, siber alandaki mevcut ve gelecekteki zorluklara uyum sağlamak için uluslararası hukukun yeniden ifade edilmesi ve geliştirilmesine katkıda bulunurken, IGF'nin güçlendirilmesi, bu alandaki uluslararası işbirliğini ve koordinasyonu artırarak daha etkili bir uygulama ve takip mekanizması oluşturabilir.

Dolayısıyla BM sistemi içinde IGF'ye bağlayıcı yetkiler atfetmek için bir karar alınması, IGF'nin uluslararası siber hukuk alanında daha etkin bir rol oynamasını sağlayabilir. Abbott, Green ve Keohane (2016) küresel yönetişim yapılarındaki dönüşümün analizini yaptıkları çalışmada, "Özel Ulusötesi Düzenleyici Kuruluşların"[75]

[75] Cogburn (2017), Ulusötesi Savunuculuk Ağlarının (TAN's) kritik rolü ve konferans diplomasisindeki güç dinamikleri için ne anlama geldiğini tartıştığı çalışmasında IGF'yi de bu kategoride değerlendirmiştir. IGF'nin yeni bir uluslararası kurum biçimini temsil ettiğini ve yeni ortaya çıkan küresel yönetişim mekanizmasının temelini oluşturduğunu savunmaktadır. Dolayısıyla Abbott ve diğerlerinin (2016) güçlerini arttırdığını iddia ettikleri kuruluşlar sınıfına IGF'nin de dahil edilebileceği sonucuna varılmıştır.

resmi “Hükümetlerarası Kuruluşlara” kıyasla büyümesine vurgu yapmaktadır.[76] Çalışmada, değişen kurumsal ortamın etkisiyle küresel yönetişim ortamının nasıl evrildiği özetlenmektedir. Yazarlar, hükümetlerarası kuruluşların göreceli durağanlığının aksine özel ulusötesi düzenleyici kuruluşların hızla çoğalması durumunu betimlemek için "örgütsel ekoloji" çerçevesini kullanmakta ve bu kuruluşların esnekliğini, daha düşük maliyetlerini ve yönetişim ekosistemindeki boşlukları doldurma yeteneklerini vurgulamaktadır. Bu kuruluşların geleneksel hükümetlerarası kuruluşların yanında nasıl önemli aktörler haline geldiğini ve karmaşık küresel yönetişim sistemine daha iyi cevap verdiklerini ifade etmektedirler. Bu bağlamda siber uzayın karmaşık yapısı göz önüne alındığında geleneksel hükümetlerarası kuruluşların böyle bir alanda yönetişim mekanizmasını sürdürmesi zordur. Abbott ve diğerlerinin vurguladığı gibi, değişen küresel yönetişim ortamında, IGF gibi kuruluşların güçlendirilmesi, uluslararası toplumun karşı karşıya olduğu siber tehditlerle başa çıkmada daha etkin mekanizmalar oluşturabilir. Bu nedenle IGF gibi kuruluşların güçlendirilmesi ve resmiyet kazandırılması önem arz etmektedir.

Normatif teorinin küresel düzen üzerine geliştirdiği argümanlar bu noktada önem arz etmektedir. Küresel dönüşümlerin dinamikleri, 'düzen' kavramının analitik ve normatif boyutları arasındaki ilişkiyi netleştirirken, normatif kaygıların yoğunlaşmasını da beraberinde getirir (Rosenau, 1992). Bu durum, internet gibi sürekli değişen ve teknolojik gelişmelere bağlı alanlarda da kendini gösterir. Bu bağlamda uluslararası kuruluşların güçlendirilmesi, küresel internet yönetişimi ve diğer küresel sorunlar karşısında uluslararası toplumun sürekli değişen yapısına ve yeni zorluklara etkili bir şekilde yanıt verebilmesi için kritik öneme sahiptir.

IGF'ye Uluslararası Organizasyon Statüsü Kazandırılması: Birçok uluslararası kurum, sadece bir "kolaylaştırıcı forum" olmanın ötesine geçerek küresel hukuk düzeninde özerk bir konuma yükselmiştir. Bu tür durumlarda yasa yapma süreci, devlet dışındaki kurumsal aktörlerin katılımıyla ve iyi tanımlanmış prosedürler aracılığıyla gerçekleşmiştir. AB hukuk sistemi, devletlerin anlaşmalarda önceden kabul ettikleri

[76] 1945'ten sonra BM sistemi altında onlarca uzman kurum, program ve komisyon kurulmuştur. WTO gibi diğer işlevsel hükümetlerarası kuruluşlar ortaya çıkmış ve nüfuz kazanmıştır. Avrupa kurumları da önemli ölçüde genişlemiştir. Çok taraflı anlaşmalar da çoğalmıştır; örneğin çevre anlaşmaları 1990'larda neredeyse %150 oranında artmıştır. Ancak 21. yüzyılın ilk yıllarında uluslararası kuruluş sayısındaki artış belirgin şekilde yavaşlamıştır. Mevcut IGO'lar faaliyetlerini genişletmeye devam etse de, yeni kuruluşların oluşumu yaklaşık %20 oranında azalmıştır. Yeni çevre anlaşmalarının kabulü de daha da keskin bir şekilde yavaşlamıştır (Abbott, Green & Keohane, 2016).

hükümlerin ötesine geçen içtihatlar temelinde büyük ölçüde şekillenmiştir. Bu durum, devletlerin başlangıçta kabul etmiş oldukları metinlerin ötesine geçen yargı kararlarıyla hukukun nasıl evrildiğine dair bir örnektir (Wessel & Blockmans, 2014).

IGF'nin statüsünün, bağlayıcı kararlar alabilen bir uluslararası organizasyona dönüştürülmesi için gerekli hukuki ve yapısal değişiklikler yapılabilir. Bu, BM Genel Kurulu veya başka bir uluslararası kuruluş tarafından resmi bir kararla gerçekleştirilebilir. Bu değişiklik, IGF'ye üye devletler üzerinde bağlayıcı kararlar alma yetkisi verebilir. Esasen IGF, yapısal olarak da bu statüyü kazanabilecek bir platform olarak görülmektedir. BM uzman kuruluşları ve diğer uluslararası hükümetlerarası kuruluşlar, genellikle genel kurul organları, yürütme organları ve sekreteryadan oluşurlar. Bu organlar, prosedür kuralları olarak da bilinen iç tüzüklerle yönetilir. Usul kuralları, oylama, gündem, diller, toplantılar ve organların işleyişi gibi konularda prosedürleri belirler. IGF de, resmi bir karar alma yetkisine sahip olmasa da, benzer bir yapıya sahiptir. Örneğin, doğası gereği çok paydaşlı olan ve resmi karar alma yeteneğine sahip olan bir kuruluş örneğini temsil eden Uluslararası Çalışma Örgütü (ILO), böylesi bir kuruluşun nasıl işletilebileceğini göstermektedir.[77] ILO örneği, BM himayesi altında bulunan ve sadece hükümet delegelerinden oluşmayan uluslararası bir organın ilgili ve etkili karar alma mekanizmasının nasıl işlediğini göstermektedir. IGF de benzer bir prosedür izleyerek resmi karar alma yetkisine sahip bir statü kazanabilir (Shcherbovich, 2017, s. 11).

IGF'nin bağlayıcı kararlar alabilen bir uluslararası organizasyona dönüştürülmesi, normatif teorinin savunduğu demokratik meşruiyet ve etik ilkelerle uyumlu bir adım olacaktır (Hirst vd., 2009, s. 322). Zira IGF gibi küresel yönetişim forumları, meşruiyet kazanabilmek için demokratik süreçlere ihtiyaç duyarlar. Bu nedenle, meşruiyet kazanmak için gelişmekte olan ülkelerin katılımını artırmalı, kâr amacı gütmeyen kuruluşlara erişim sağlamalı ve demokratik hesap verebilirliği sağlamalıdırlar (Baird, 2014, s. 16).

[77] Uluslararası Çalışma Örgütü (ILO), doğası gereği çok paydaşlı olan ve resmi karar alma yeteneğine sahip olan bir kuruluş örneğidir. Uluslararası Çalışma Konferansı, ILO'nun tüm üye ülkelerini temsil eder. Yürütme organı olarak Yönetim Kurulu, ILO'nun politikasını belirler. Sekreterya ise ILO'nun idari işlevlerinden sorumludur. ILO, hükümetlerin, işverenlerin ve çalışanların temsilcilerinden oluşan benzersiz bir "üçlü" yapıya sahiptir. Bu yapı, ILO'nun karar alma sürecinde tüm paydaşların sesini duyurmasını sağlar. ILO Konferansı, hangi delegelerin oy kullanma hakkına sahip olacağına karar verir. Hükümet dışı delegelerin kimlik bilgileri, özel bir komite tarafından incelenir (Shcherbovich, 2017, s. 11).

Böylesi bir dönüşüm, siber uzayın karmaşık yapısına daha etkin bir şekilde müdahale edebilmek için gerekli yapısal değişiklikleri ve hukuki süreçleri içerebilir. Bu bağlamda IGF'nin uluslararası organizasyon statüsü kazanması ve bağlayıcı kararlar alabilmesi, küresel internet yönetişiminde adil bir yapı oluşturma yönünde atılabilecek önemli adımlardandır. Bu, siber adalet kavramıyla uyumlu bir yaklaşımı temsil eder ve siber alanda insan hakları normlarına dayalı iyi yönetişimi teşvik eder (Mihr, 2016, s. 314).

Yumuşak Hukuk İlkelerinin Sert Hukuka Dönüştürülmesi: Yumuşak hukuk, devletler tarafından resmi olarak kabul edilmiş, ancak yasal olarak bağlayıcı olmayan normlar ve ilkelerden oluşur. Yumuşak hukuk yasal olarak bağlayıcı olmasa da ana akım değerleri somutlaştırır ve küresel yönetişimde sert hukukun oluşumunu etkiler (Zhu & Tang, 2023, s. 1). "Yumuşak hukuk" unsurları (örneğin, politika önerileri, ilkeler, standartlar) zamanla "sert hukuk" unsurlarına (bağlayıcı uluslararası anlaşmalar, tüzükler) dönüşebilir (Abbott & Snidal, 2000; Guzman & Meyer, 2010; Gemalmaz, 2022). IGF tarafından geliştirilen ilkeler ve öneriler, zamanla devletlerin gönüllü katılımı ve uluslararası toplumun geniş çapta kabulü ile "sert hukuk" statüsü kazanabilir. Bu, belirli ilkelerin uluslararası antlaşmalara dönüştürülmesi veya uluslararası hukukun genel prensipleri olarak kabul edilmesi yoluyla gerçekleşebilir.

Örneğin BPF 2021 yılında hazırladığı raporda gönüllü, bağlayıcı olmayan siber güvenlik normları da dahil olmak üzere paydaşlar arasında 38 uluslararası anlaşmanın içeriğini incelemiştir. Rapor, çeşitli uluslararası kuruluşlar ve hükümetlerarasındaki siber güvenlik işbirliğini ve anlaşmalarını detaylandıran bir dizi bölümden oluşmaktadır. İncelenen anlaşmalar arasında Afrika Birliği Siber Güvenlik ve Kişisel Veri Koruma Sözleşmesi, APEC Siber Güvenlik ISP Uygulama Kodları için Gönüllü Kılavuzlar, Arap Bilgi Teknolojisi Suçlarıyla Mücadele Sözleşmesi ve daha fazlası yer almaktadır. Raporun siber güvenlik konusunda küresel normların oluşturulması, uygulanması ve bu normların etkinliğinin değerlendirilmesi konularına odaklandığı görülmektedir.[78]

BPF'nin 2021 raporu, gönüllü ve bağlayıcı olmayan siber güvenlik normlarının uluslararası işbirliği ve güven inşasını teşvik etmede oynadığı önemli rolü vurgular. Ancak bu yaklaşımın bazı sınırlılıkları da mevcuttur. Somut yaptırımların yokluğu, bazı

[78] Ayrıca bkz: Internet Governance Forum. (2021, November). *Best Practice Forum Cybersecurity on the use of norms to foster trust and security: Mapping and Analysis of International Cybersecurity Norms Agreements - BPF Workstream 1 Draft Report - References Document*. https://www.intgovforum.org/en/filedepot_download/235/19830

aktörlerin bu normları göz ardı etmesine yol açabilirken; uygunluğun izlenmesi ve doğrulanması, özellikle devlet dışı aktörler söz konusu olduğunda zorlayıcı olabilir. Bunun yanında farklı uygulamalar, tutarsızlığa sebebiyet verecektir. Özellikle gönüllü normların yeterince kapsayıcı olmadığı veya uygulamada yetersiz kaldığı durumlar, internet yönetişimi alanındaki boşlukların derinleşmesine neden olacaktır. Bu nedenle bu normların sert hukuka dönüştürülmesi gerekliliği ortaya çıkmaktadır.

Bu yaklaşım, normatif teorideki "hukukun düzenleyici rolü" ile de uyumludur. Normatif teori, hukukun devletler arası ilişkilerde istikrar ve düzeni sağlamada kritik bir role sahip olduğunu kabul eder (Dyer, 1997; Nardin, 2022). IGF'nin bağlayıcılık kazanması ve uluslararası siber hukuk alanında etkili bir rol oynaması, yasal olarak bağlayıcı olmayan norm ve ilkelerin yani "yumuşak hukukun" zaman içinde sert hukuk haline getirilmesi sürecini içerebilir. Bu, özellikle IGF tarafından geliştirilen ilkelerin ve önerilerin, devletlerin gönüllü katılımıyla uluslararası anlaşmalara dönüştürülmesi veya uluslararası hukukun genel prensipleri olarak kabul edilmesi yoluyla gerçekleşebilir. Bu süreç, normatif teorinin uluslararası ilişkilerde ahlaki bağların güçlendirilmesi ve uluslararası adaletin sağlanması yönündeki vurgularıyla uyum içindedir.

Çok Taraflı Anlaşmalar Aracılığıyla Uygulama: Devletler arasında, IGF'nin belirli önerilerini uygulamayı taahhüt eden çok taraflı anlaşmalar yapılabilir. Bu anlaşmalar, katılımcı devletler için bağlayıcı olacak ve IGF'nin önerilerinin belirli yönlerini uygulama konusunda yasal yükümlülükler oluşturacaktır. Zira anlaşmalar, uluslararası hukukun temel kaynaklarından biridir. Devletler arasında bağlayıcı olan antlaşmalar, çeşitli konularda düzenlemeler içerir ve bu düzenlemelerde uluslararası hukuka atıflar sıklıkla yer alır. Bu şekilde antlaşmaya taraf olan devletlerin, belirli bir konudaki hak ve yükümlülüklerini uluslararası hukuk çerçevesinde netleştirilir (Wilson, 1953, s. 2).

Uluslararası hukukun temel kaynakları, Uluslararası Adalet Divanı Statüsü'nün 38. Maddesinde sıralanmıştır. Madde 38'de sıralanan önemli kaynaklardan biri de uluslararası anlaşmalar olarak kabul edilmiştir.[79] Örneğin Paris İklim Anlaşması, iklim değişikliğiyle mücadele konusunda uluslararası bir işbirliğini teşvik eden çok taraflı bir anlaşmadır. Anlaşma, uluslararası toplumun küresel ısınmayı 2 derecenin altında tutma

[79] Uluslararası Adalet Divanı Statüsü'nün 38. Maddesinin "a" bendinde "İhtilaflı devletler tarafından açıkça tanınan kuralları belirleyen genel veya özel uluslararası sözleşmeler" ibaresi kullanılmıştır. Detaylı bilgi için bkz: UN. (t.y.). *Statute of the International Court of Justice*. https://www.un.org/en/about-us/un-charter/statute-of-the-international-court-of-justice

hedefine ulaşmak için taahhütlerde bulunmasını sağlar. Bu anlaşma, devletlerin uluslararası taahhütlerini yerine getirme konusunda nasıl harekete geçirilebileceğinin bir örneğidir ve IGF'nin siber güvenlik veya veri koruma gibi konularda benzer bir yaklaşımla bağlayıcı taahhütler oluşturabileceğini gösterir.

Devlet dışı aktörler uluslararası hukukta resmi bir kapasiteye sahip olmamasına rağmen, belirli şartlar altında uluslararası hukukun bir kaynağı olarak uluslararası anlaşmalar yapma yetkisine sahip olabilmektedir (Loja, 2018). IGF, hem tüm paydaşların üzerinde uzlaşabileceği bir metin formüle etmek hem de bu formülasyonu uluslararası hukuktaki mevcut standartlara ve bağlayıcı olmayan bildirge ve standartlara bağlamak için çalışmalarını sürdürmektedir. Bu çalışmaların önemli bir çıktısı da IGF'nin 2019 yılındaki toplantısı sırasında başlatılan Web Sözleşmesi'dir.

Redeker (2019), Web Sözleşmesi'nin amaçlarını, içeriğini ve potansiyel etkilerini ele aldığı çalışmasında sözleşmenin dijital anayasacılık[80] kavramıyla nasıl ilişkilendirilebileceğini ve internetin küresel anayasallaşma sürecinde nasıl bir rol oynayabileceğini tartışmaktadır. Web Sözleşmesi, şirketler, sivil toplum ve devletler dahil olmak üzere geniş bir destekçi ağı üzerine kuruludur. Her bir grup, dokuz prensibin üçünü üstlenir. Örneğin, sözleşmeyi imzalayan devletler, internet erişimini insan hakları yasalarıyla uyumlu olmadıkça kesmeme sözü verir. Bireyler, siber alanda herkesin güvende hissetmesini sağlamak için hareket etme taahhüdünde bulunur. Ancak, sözleşme yasal olarak zorunlu değildir ve özellikle şirketlerin (örneğin Facebook'un) taahhütlerini yerine getirip getirmeyeceği tartışmalıdır. Yine de Web Sözleşmesi, internet için küresel bir normatif ve yasal çerçeve oluşturma sürecinin bir parçası olarak kabul edilir.

IGF'nin önerileri, küresel internet yönetişimi için kapsayıcı ve katılımcı bir çerçeve sunarak normların yayılmasına ve uygulanmasına katkıda bulunabilir. Antik Yunan filozoflarının adalet ve iyi toplum üzerine düşüncelerinden, modern düşünürlerin ahlak ve özgürlük üzerine çalışmalarına kadar, tarihsel süreçte normatif teori, küresel düzenin ve uluslararası ilişkilerin şekillendirilmesinde önemli bir yer tutmuştur. IGF'nin siber güvenlik, ifade özgürlüğü ve erişim hakları gibi alanlarda geliştirdiği norm ve ilkeler,

[80] Dijital anayasacılık, internet hakları ve prensipleri üzerine haklar, ilke ve güç sınırlamaları hakkında geniş, karşılıklı ve normatif bir yaklaşımı temsil eder. Bu kavram, sivil toplum ağları tarafından yönlendirilen ve bazen de özel şirketler tarafından yazılan belgelerle ilişkilendirilir. Bu belgeler, internetin küresel anayasallaşma sürecinin bir parçası olarak görülür ve farklı sosyal gruplar ve coğrafi alanlar arasında tartışma yaratır.

bu teorik çerçeveden güç alarak, adil ve güvenli bir siber ortamın oluşturulmasına katkıda bulunabilir.

Ulusal Düzeyde Entegrasyon: Devletler, IGF'nin önerilerini kendi ulusal yasalarına ve politikalarına entegre ederek, bu önerileri kendi yargı alanlarında bağlayıcı hale getirebilir. Bu, ulusal yasama organlarının IGF'nin önerilerini destekleyen yasaları kabul etmesiyle sağlanabilir. Anlaşmaların uluslararası hukukun bir kaynağı olarak kabul edilmesi için gerekli formal, prosedürel ve bazen seremoniye ilişkin onayların yanı sıra, bu süreçlerin devletler tarafından desteklenmesi gerekmektedir. Bu bağlamda, devlet dışı aktörlerin yaptığı anlaşmalar, belirli koşullar altında uluslararası hukukun bir kaynağı olabilir (Loja, 2018).

Sonuç olarak, siber uzayın küresel doğası göz önüne alındığında, uluslararası işbirliğinin derinleştirilmesi ve yargı alanları arası tutarsızlıkların giderilmesi, siber hukukun uygulanmasında karşılaşılan önemli zorluklardan biridir. IGF'nin bağlayıcı yetkilere sahip olması, bu zorlukların üstesinden gelmekte önemli bir adım olabilir. Uluslararası rejim teorisi perspektifinden bakıldığında IGF, bazı konferanslara kıyasla "uluslararası ilişkilerin belirli bir alanındaki beklentilerin yakınlaşmasını" sağlamaya çok daha yatkındır (Cogburn, 2017, s. 268).

IGF'nin bağlayıcı yetkilere sahip olması, siber güvenlik, veri koruma ve siber suçlar gibi konularda uluslararası standartların belirlenmesi ve uygulanmasında kritik bir rol oynayabilir. Bu, üye devletler ve diğer ilgili taraflar arasında daha tutarlı ve etkili bir uluslararası siber hukuk çerçevesinin oluşturulmasına yardımcı olabilir. Uluslararası düzeyde, norm ve standartların oluşumu sadece resmi uluslararası örgütlerle sınırlı değildir; aynı zamanda farklı uluslararası organları da içerir. Devlet temsilcileri ve karar alma süreçlerinin incelenmesi, pek çok normun başka uluslararası organlardan kaynaklandığını veya çok daha geniş bir uluslararası tartışmanın parçası olduğunu gösterir. Bu geniş spektrum, resmi olmayan hükümetlerarası işbirliği yapılarından (örneğin, G20, Kara Para Aklama Mali Eylem Görev Gücü, Basel Bankacılık Denetim Komitesi gibi), kamu malının özel düzenlemelerine (örneğin, ISO, ICANN ve IETF gibi) kadar çeşitlilik gösterir. Bu, uluslararası hukukun ve normların gelişiminde çok sayıda aktörün ve forumun etkili olduğunu gösteren karmaşık bir tabloyu ortaya koymaktadır (Wessel & Blockmans, 2014).

Değerlendirme

Dördüncü bölüm, internet yönetişiminin evrimi ve çeşitli yönetişim modellerinin uygulanabilirliği üzerine bir değerlendirme sunmaktadır. İnternet yönetişimi modelleri üzerine yapılan detaylı inceleme, internetin yönetişim biçimlerinin evrimini ve bu evrime öncülük eden çeşitli fikir akımlarını ele almaktadır. Öz-yönetim modeline dair analiz, 1980'lerden 1990'ların ortalarına kadar olan dönemde internetin yönetişimine yönelik geleneksel hukukun uygulanmasına karşı çıkan bir yaklaşımı ortaya koymakta iken; internetin yaygınlaşması ve çeşitli sosyal, ekonomik ve politik etkileri ile birlikte, internet yönetişimi modellerinin daha kapsayıcı ve çok boyutlu yaklaşımları içermesi gerektiği anlaşılmıştır.

Ulusal (Domestic) Model, devletlerin siber alanı nasıl yönetme eğiliminde olduklarını ve bu eğilimin uluslararası ve bölgesel örgütler aracılığıyla nasıl bir egemenlikçi modele dönüşmeye çalıştığını ele alır. Otoriter devletlerin, interneti diğer devletlerin iç işlerine müdahale aracı olarak gördükleri iddiası, siber uzayı “fiziksel devlet sınırlarına” karşılık gelen “sanal sınırlar” ile çevrili bir bölge olarak algılamalarına yol açmaktadır. Bu perspektif, özellikle otoriter devletlerin siber uzayı kontrol altına alma ve uluslararası hukuku bu alana genişletme arzusu için bir temel oluşturur.

Çok paydaşlılık modeli, ABD'nin özgürlükçü modeli ve ICANN'in rolü gibi alt başlıklar aracılığıyla, internet yönetişimi modellerindeki çeşitlilik ve bu modellerin avantajları ile sınırlılıkları incelenmiş; ABD'nin internete yönelik "laissez faire" anlayışının yanı sıra, ICANN'in rekabeti teşvik etmek ve küresel internet kuruluşlarının çıkarlarını temsil etme rolü değerlendirilmiştir. Ayrıca, çok paydaşlı modelin karşılaştığı sorun alanlarına da değinilmiş, bu sorunların modelin meşruiyetini nasıl etkileyebileceği ve internetin evrimiyle birlikte bu modelin karşı karşıya kaldığı zorluklar tartışılmıştır. Bu bağlamda, çok paydaşlılık modeli, internet yönetişiminde önemli bir ilerleme olarak değerlendirilirken, aynı zamanda modelin işleyişini zorlaştırabilecek güç dengesizlikleri, karar alma süreçlerindeki karmaşıklıklar ve modelin meşruiyeti ile ilgili endişeler de gündeme gelmiştir.

Diğer yandan çok taraflılık modeli, devletlerin ve hükümetlerarası kuruluşların internet yönetişiminde daha baskın bir rol alması gerektiğini öne sürerken, Amerikan siber hegemonyasına karşı bir alternatif sunmaktadır. Egemenlikçi model altında siber uzaydaki devlet egemenliği ve siber-westphalian çağının başlangıcı gibi kavramlar

irdelenmiştir. ITU'nun rolüne dair bölümde, DNS sorumluluğunun ICANN'den ITU'ya devredilmesi gibi çatışma alanları ve ITU'nun uluslararası telekomünikasyon sektöründe oynadığı rol tartışılmıştır. Çok taraflılık modeli, devletlerin internet üzerinde daha fazla kontrol sahibi olmasını savunduğu için, bu durum siber özgürlükleri ve ifade özgürlüğünü sınırlayabilir veya devletlerin interneti daha sıkı bir şekilde düzenlemesi, sansür ve gözetim gibi uygulamaların artmasına yol açabilir. Bunun yanında, büyük ve güçlü devletlerin küçük ve zayıf devletler üzerinde aşırı bir etkiye sahip olmasına yol açabileceğinden güç dağılımı noktasında da sorunlar yaratabilir.

Alternatif Yaklaşımlar kapsamında ise Joseph Nye tarafından önerilen Rejim Kompleksi Modeli ele alınmıştır. Nye'ın siber yönetişim için önerdiği bu çerçeve, interneti ve siber faaliyetleri küresel olarak yöneten çok yönlü ve birbirine bağlı bir çerçevenin varlığını savunmaktadır. Ancak bu model, güç dinamikleri, teknolojik değişimler ve siber uzay yönetişiminde adalet ve eşitlik meseleleri üzerine daha derinlemesine bir inceleme gerektirmektedir.

Son olarak incelenen ve nihai olarak önerilen model olan IGF'nin ise, tüm faktörlerden önce, yapısal olarak küresel internet yönetişimi tartışmalarında benzersiz bir yapı sunduğu görülmüştür. IGF'nin esnek yapısı ve çok paydaşlı katılımı, internetin evrensel bir kaynak olarak rolünü ve internet yönetişiminin çok yönlü ve dinamik doğasına nasıl uyum sağlayabildiğini vurgulamaktadır. Bu durum, IGF'nin internet yönetişimi konusundaki küresel tartışmalarda önemli bir katkı sağladığını ve farklı paydaşların bir araya gelerek internetin geleceği hakkında ortak bir anlayış geliştirebilmesine olanak tanıdığını gösterir.

Yapılan incelemede, IGF'nin tüm katkılarının yanında çeşitli sorunlar da barındırdığı gözlenmiştir. Özellikle, Kuzey-Güney eksenindeki anlayış farklılıkları, forum içinde önemli bir tartışma konusu oluşturmakta ve forumun küresel bir platform olarak kapsayıcılığını zedelemektedir. Özellikle gelişmiş ülkeler ile gelişmekte olan ülkeler arasındaki görüş ayrılıkları, forumun etkin bir işbirliği platformu olmasını engellemektedir.

Özellikle, IGF'nin kararların bağlayıcılığı ve hukuki zorunluluk yaratma konusundaki kapasitesi, bu platformun etkinliği üzerinde önemli bir tartışma konusu olmuştur. Uluslararası politika konferansları spektrumunun tam ortasında yer alan IGF, bağlayıcı

olmayan kararlar alınan bir platform olarak tanımlanır. Tunus Gündemi'nin vurguladığı gibi, IGF'nin amacı, tarafsız, ikilik yaratmayan ve bağlayıcı olmayan bir süreç olarak internetin yönetişimine katkıda bulunmaktır. Ancak, bu "kolaylaştırıcı" rol, günümüzün karmaşık ve hızla gelişen siber dünyasında yeterli görünmemektedir. IGF'nin aldığı kararların bağlayıcı olmaması, uluslararası düzeyde somut sonuçlar doğurmasını zorlaştırmakta ve özellikle acil eylem gerektiren küresel sorunlara hızlı ve etkili çözümler üretme kapasitesini sınırlamaktadır. IGF gibi yapıların, yönlendirmeleri zorunlu kılmak için yaptırım gücüne sahip olmaması, bu platformun rehberlik ve kolaylaştırıcı rolünü önemli ölçüde sınırlandırmaktadır.

Bu bağlamda, IGF'nin küresel internet yönetişimi ve uluslararası siber hukukun geliştirilmesinde daha etkin bir rol oynaması için bağlayıcı yetkilere sahip olması yönünde bir tartışma ön plana çıkmaktadır. IGF'nin sadece tartışma ve fikir alışverişi için bir alan olmaktan öte, karar alma süreçlerine somut katkılar sunması ve uluslararası düzeyde etkili olması gerektiği vurgulanmaktadır. Bu, IGF'nin mevcut yapısal özelliklerinin ve işleyiş mekanizmalarının ötesine geçmesini ve uluslararası siber hukuk düzenlemelerinin geliştirilmesinde daha etkin bir rol üstlenmesini gerektirir. Böylece, IGF'nin potansiyelini tam olarak gerçekleştirebilmesi ve küresel internet yönetişimi alanında proaktif ve etkili bir aktör olabilmesi için, yapısal ve işlevsel değişikliklerin ve hukuki bağlayıcılığın sağlanması önem taşımaktadır. Bu durum, hem normatif çözüm önerileri sunmayı hem de hukuki olasılıkları göz önünde bulundurmayı gerektirir, böylelikle IGF, uluslararası siber düzenin şekillendirilmesinde merkezi bir role sahip olabilir.

Bir sorun olarak kabul edilen IGF'nin bağlayıcı kararlar alamaması durumu, hukuki sınırlılıklar göz önünde bulundurularak giderilmeye çalışılmıştır. IGF'nin hukuki bağlayıcılığa sahip olabilmesi için öncelikle, uluslararası hukukun mevcut sınırlılıklarının ve bu alandaki dönüşümün incelenmesi gerekmektedir. Günümüzde uluslararası hukuk, devletlerin yanı sıra uluslararası örgütler, sivil toplum kuruluşları, çok uluslu şirketler ve bireyler gibi çeşitli aktörleri kapsayan geniş bir spektruma yayılmış durumdadır. Bu genişlemiş aktör yelpazesi, uluslararası hukukun geleneksel devlet-merkezli yapısının ötesine geçerek daha kapsayıcı ve etkileşimli bir yapıya doğru evrilmesine neden olmuştur. Ancak, bu dönüşüm, uluslararası hukukun uygulanabilirliği ve etkinliği açısından yeni zorluklar ve sorunlar da getirmektedir.

Bu yeni zorluklara yanıt olarak, uluslararası hukukun çeşitlenmesi, hukukun daha bütüncül ve etkileşimli bir yapıya bürünmesinin yanı sıra, uluslararası norm ve kuralların oluşturulması ve uygulanmasında farklı aktörlerin artan etkisinin bir göstergesi olarak değerlendirilmektedir. Bu durumun, siber güvenlik, insan hakları ve dijital özgürlükler gibi alanlarda uluslararası normların geliştirilmesi ve bunlara yönelik spesifik normların inşa edilmesi gibi önemli faydalar sunduğu gözlemlenmiştir.

SONUÇ

Bilgi ve iletişim teknolojilerinin yarattığı "küresel" devrim; siyaset, ekonomi ve sosyal yapıların tümü üzerinde büyük değişimler yaratırken; siber uzay ve onun en önemli bileşeni olan internet de bilgi ve iletişim teknolojilerinin bir ürünü olarak ortaya çıktı. 1990'lardan bu yana internet, ulusal ve bölgesel sınırların ötesine geçerek tüm dünyayı birbirine bağlayan sanal bir alan yarattı. Bir yandan, devlet ve devlet dışı aktörler internetin sağladığı kolaylıklardan yararlanmak için harekete geçerken; diğer yandan internetin değiştirdiği dinamiklere ayak uydurmaya çalışmaktadır. Bugün dünya nüfusunun %66'sını birbirine bağlayan internet; günümüzün ekonomik, sosyal ve kültürel temelinin en kritik parçalarından biri haline gelmiş ve bilgi toplumunun küresel altyapısı olmuştur (Statista, 2024). Dolayısıyla bu ağın "nasıl yönetileceği" veya "yönetilebilir olup olmadığı" küresel tartışmaların ve bu çalışmanın gündemine oturmuştur. Siber uzay üzerinde barışçıl, güvenli, açık ve işbirliğine dayalı bir yönetişimin nasıl oluşturulacağı, tüm aktörlerin karşı karşıya olduğu temel stratejik bir "sorun" haline gelmiş ve çalışmada bu sorun alanı kapsamlı bir şekilde analiz edilmiştir.

Bu hassas ve önemli "sorun" alanında küresel düzeyde birtakım adımlar atılması gerektiği fikri, özellikle siber tehditlerin artmaya başlamasıyla gündeme gelmiştir. Bu nedenle, 1980'lerin sonu ile 1990'ların başındaki ilk büyük siber saldırılar, internet yönetişimine duyulan ihtiyacı da artırmaya başlamıştır. Özellikle 1990'ların başında yaşanan teknolojik gelişmeler, internetin ticarileştirilmesi ve bu gelişmelerin getirdiği tehditler, bu alanın yönetişimine dair tartışmaları gündeme getirmiştir. Bu dönemde siber suç ve siber saldırılar gibi zararlı faaliyetlerin çoğalması, uluslararası toplumun işbirliğine ihtiyaç olduğunu göstermiştir. Siber uzayın yönetişimine dair tartışmaların başlaması da, ilk teknolojik gelişmelerin yaşandığı 1990'larda başlamıştır. İnternetin herhangi bir düzenlemeye tabi olup olmaması gerektiği konusu tartışmaların zeminini oluşturmuştur. İnternetin ilk mimarları, internetin yönetilebileceği, hatta yönetişim gerektirdiği fikrini dahi reddetmişlerdir. Bunun yerine, IETF ve IANA'da da görüldüğü üzere aşağıdan yukarıya, işbirliğine dayalı, büyük ölçüde gönüllü bir şekilde koordine edilen bir standart geliştirmişlerdir. Ancak, 1992'de World Wide Web'in icadı, internetin geniş kitleler için erişilebilir hale gelmesinin önünü açarak internetin ticari değerini artırmış ve onu tüm ülkeler için önemli bir konuma getirmiştir. İnternetin

güvenliğine yönelik tehditlerin ortaya çıkması, yeni sorunları gündeme getirmiş ve bütün aktörleri internetin nasıl yönetilmesi gerektiği konusunda uluslararası bir tartışmanın içine çekmiştir.

İlk zamanlar yalnızca bir güç mücadelesi gibi görünen internet, özellikle devletlerin üzerinde söz sahibi olmak istedikleri bir ağ olarak algılanmıştır. Nitekim 2000'li yılların başlarında internetin hangi aktörler tarafından ne şekilde yönetilmesi gerektiğine dair tartışmalar birtakım bölünmeleri ortaya çıkarmıştır. 2010'lardan sonra ise bu tartışmalar derinleşmiş ve genişlemiştir. Özellikle Çin, Rusya, Hindistan ve Brezilya gibi yükselen güçler, Batı'nın internet yönetişimi ve altyapısı üzerinde kurmuş olduğu küresel politik-ekonomik hegemonyadan rahatsız olmuş ve buna meydan okumaya başlamışlardır.

Zaman içerisinde derinleşen tartışma, küresel dijital yönetişimin ilgilendiği sorunlar üzerinde yoğunlaşmaya başlamıştır. Zira bu sorunlar, küresel bir mahiyet kazanarak küresel çözümler gerektiren sorunlar haline gelmiştir. Günümüz itibariyle bu konular/sorunlar, oldukça geniş bir alanı kapsamaktadır. Teknik standartların oluşturulması, siber güvenlik sorunları, gizlilik gibi insan hakları düzenlemeleri ve telif haklarının korunması gibi çeşitli konularda sorunlar meydana gelmektedir. Bunlar, internetin ilk yaygınlaşmaya başladığı zamanlardan bu yana devamlılığını sürdüren konular olarak adlandırılabilir. İnternet kullanımının küresel anlamda yaygınlaşmasıyla birlikte yönetişim konuları da genişlemeye başlamış ve hala genişlemeye devam etmektedir.

Bu bağlamda siber uzayla ilgili konularda etkili bir uluslararası işbirliği için bir çerçeve oluşturma ihtiyacı olduğu küresel platformlarda gündeme getirilmeye başlanmıştır. BM gibi uluslararası örgütler tarafından düzenlenen çalışmalar bu gerçeği yansıtmaktadır. 2004 yılında BM, hükümetlerarası bir yapı üzerine inşa edilen paradigmanın değişmesi gerektiğine dikkat çekmiştir. Bu yapının sivil toplum gibi devlet dışı grupları da içerecek şekilde küresel sistemde var olması gerektiğini vurgulamıştır. Bu doğrultuda BM, "küresel sorunlarla ilgili tüm seçmenleri bir araya getirmek ve etkili sonuçlar için uygun ağları harekete geçirmek" şeklinde bir tavsiye sunmuştur.

Bu dönemde siber uzay, BM'nin önerdiği küresel çizginin uzağında konumlandırılmıştır. Zira siber uzay, dar bir bakış açısıyla değerlendirilerek yalnızca "teknik" bir alan gibi muamele görmüştür. Nitekim 1990'lar boyunca, geleneksel

düzenleyici yaklaşımlar, siber uzayın düzenlenmesi için uygun görülmemiştir. Bunun yerine, internet yönetişiminin teknik topluluk ve özel sektör tarafından ademi merkeziyetçi, kapsayıcı ve aşağıdan yukarıya bir politika ile yönetilmesi gerektiği savunulmuştur. Bu bağlamda oluşturulan IANA ve ICANN gibi kuruluşlar, bu formülasyonun birer çıktısı olarak karşımıza çıkmaktadır.

Nihayetinde, bu tür bir yönetişimin tek başına etkili olacağını savunan tarafların beklentileri karşılıksız kalmıştır. Zira bu alanda uluslararası kuruluşlar aracılığıyla etkin olan devletler, internet yönetişimi konusunda önemli bir rol üstlenmeye başlamıştır. Bu aşamadaki ilk adım, Uluslararası ITU önerisi ile oluşturulan WSIS olmuştur. İki aşamada gerçekleştirilen Zirve, internet yönetişiminin "teknik" düzeyden "politik" düzeye taşınmasında önemli bir rol üstlenmiştir.

WSIS'in internet yönetişimine kazandırdığı politik boyutun etkisiyle, internet yönetişim yapısına çeşitli aktörler dahil edilmiştir. Bugün, devletler, hükümetlerarası kuruluşlar, özel sektör ve sivil toplum gibi pek çok grup, bu sürecin içerisinde yer almaktadır. Bu yeni aktörlerin çoğu, ilk nesil internet yöneticilerinden farklı olarak internet yönetişiminde birincil role sahip değildir. Bazılarının internet yönetişimi ile uzun bir geçmişi olsa da, genellikle sahip oldukları rol nispeten az olmuştur. Birçoğu, halen internet yönetişiminde söz sahibi olamamanın endişesini taşımakta ve bu alanda etkili olmaya yönelik adımlar atmaktadır. Bunu yaparken, politika gündemlerine internet yönetişimine dair söylemleri dahil etmekte ve bu doğrultuda stratejiler geliştirmektedir. Özellikle 21. yüzyılın başlarında siber tehditlerin önü alınamaz boyutlara ulaşması, bu alandaki teknik bakış açısını politik düzeye taşımış ve güvenli bir siber uzay oluşturmak yalnızca teknik topluluğun değil, tüm paydaşların önemli bir meselesi haline gelmiştir. Bu bağlamda aktörler, küresel ve bölgesel yönetişim kurumları oluşturarak bu alana ayak uydurmaya çalışmaktadır. Ancak bugün, siber uzay üzerinde uzlaşmaya varılacak bir yönetişim mekanizmasının oluşturulmasında güçlük çekilmektedir. Esasında yönetişimin kendisi bile halen tartışmalı bir kavram olarak karşımıza çıkmaktadır.

Bu denli komplike ve ayrıntılı sorunu kapsayan bu ağın yönetişiminin küresel işbirliği gerektirdiği bu çalışmanın odak noktasını oluşturmuştur. Zira bu ağ, toplumların gelişimi için büyük bir fırsat olarak görülmektedir. Ancak son yıllarda politika yapıcılar, internetin potansiyelini baltalamaktadır. Özellikle devletler ve özel sektör,

bilgiye erişimi ve ifade özgürlüğünü kısıtlayarak “parçalanmış ve küresel olmayan” bir ağ yaratmaktadırlar. Bu nedenle açık, özgür ve küresel bir internetin sağlanabilmesi zorlaşmaktadır. Her ne kadar iki taraflı, bölgesel veya çok taraflı anlaşmaların sayısı artsa da, küresel mekanizmaların yetersizliği gizlilik, online korsanlık ve güvenlik politikaları üzerindeki tehlikeyi devam ettirmektedir. Dolayısıyla güvenli bir siber alanın anahtarı olan iyi yönetişim ilkeleri zarar görmektedir.

Bu çalışma, çeşitli aktörlerin el birliğiyle değil, ayrı ayrı, işbirliği mekanizmalarını görmezden gelerek gerçekleştirdikleri faaliyetlerle zarar verdikleri bu iyi yönetişim ilkelerini koruma, hatırlatma ve potansiyel etkilerini ortaya koyma motivasyonuyla yola çıkmıştı. İlk motivasyon, şu soruya cevap bulmaktı: Küresel internet yönetişimi neden bir sorun? Bu soru, diğer bütün araştırma sorularının çıkış noktasını oluşturmaktadır.

Küresel internet yönetişimi, çok çeşitli nedenlerden dolayı önemli ve karmaşık bir sorun haline gelmiştir. Bunun temelinde yatan nedenler arasında teknolojinin hızlı gelişimi, ulusal sınırları aşan internetin doğası ve çeşitli aktörlerin (devletler, uluslararası kuruluşlar, özel sektör ve sivil toplum) bu alandaki farklı ve bazen çatışan çıkarları yer almaktadır. Tez boyunca, internet yönetişiminin çok katmanlı ve karmaşık bir yapıya sahip olduğu ve bu yapı içerisinde farklı aktörlerin önemli roller oynadığı analiz edilmiştir. Devletler, özel sektör, sivil toplum ve teknik topluluk arasındaki etkileşimlerin, güç dengelerini sürekli olarak değiştiren ittifaklar kurarak internet yönetişimindeki etkilerini artırmaya çalıştığı gözlemlenmiştir. Bununla birlikte, aktörlerin rol ve sorumluluklarına rehberlik edecek herhangi bir parametre üzerinde henüz uzlaşmaya varılamamıştır. Bu durum yönetişim sorununu derinleştirmekte ve çok paydaşlı süreçlerdeki esneklik ile paydaşlara atfedilen rol ve yetkilerin genişliği, internet üzerindeki etki alanıyla uyumlu olarak kabul görmemiştir. "Siber karşılıklı bağımlılık çağı"nda işbirliği ve çok paydaşlı diyaloglar, siber uzayın yönetişimi için en etkili yol olarak öne çıkmaktadır. Sürdürülebilir ve kapsayıcı bir dijital gelecek inşa etmek, bu tür bir işbirliğine bağlıdır. Bu karmaşık yönetişim manzarası, çeşitli paydaşların siber uzayı yöneten normları, kuralları ve standartları şekillendirmede kritik bir rol oynadığını göstermektedir.

Teknik, politik ve sosyo-politik boyutlarda ortaya çıkan sorunlar, internetin yönetişimiyle ilgili küresel çözümler bulunmasını zorunlu kılmaktadır. Bu çalışmanın

odaklandığı temel sorunlar, TCP/IP, DNS, Kök Bölge, World Wide Web ve Blok Zinciri gibi temel internet teknolojilerinin yanı sıra siber güvenlik, insan hakları ve kalkınma gibi konuları içermektedir. Her bir teknoloji ve konu, kendi içinde özel yönetişim zorluklarına sahiptir. Örneğin, TCP/IP ve DNS gibi internetin temelini oluşturan teknolojiler, küresel erişim ve bağlantı sağlamak için uluslararası işbirliğine ihtiyaç duyar. Öte yandan, kök bölge yönetimi ve World Wide Web'in evrimi, merkeziyetçi olmayan yönetişim modellerinin önemini vurgular. Blok zinciri teknolojisi, veri güvenliği ve gizlilik konularında yeni fırsatlar sunarken, aynı zamanda düzenleyici meydan okumaları da beraberinde getirir.

Politik sorun alanlarına gelince, siber güvenlik yönetişimi ve siber suçlar, ulusal ve uluslararası düzeyde koordinasyon ve işbirliğini gerektiren kritik konulardır. İnsan hakları sorunları, özellikle veri koruma, gizlilik ve online özgürlükler, internetin açık ve özgür kalmasını sağlama ihtiyacını vurgular. Kalkınma ve erişimle ilgili sosyo-politik sorunlar, internetin tüm insanlar için adil ve eşit fırsatlar sunmasını sağlamak amacıyla ele alınmalıdır.

Bu çeşitlilik, küresel internet yönetişiminin neden karmaşık ve çok katmanlı bir sorun olduğunu göstermektedir. Küresel işbirliği gerektiren bu sorun alanlarının belirlenmesi, sorunların üstesinden gelmek ve internetin potansiyelini en üst düzeye çıkarmak için gerekli ilk adımdır. Ancak bu, aktörlerin mevcut sorunları ve potansiyel çözümleri anlamalarını ve kabul etmelerini gerektirir. Küresel internet yönetişimi üzerine yapılan bu çalışma, sorunların sadece belirlenmesiyle kalmayıp, aynı zamanda bu sorunlara yönelik etkili stratejiler geliştirilmesi için bir temel teşkil etmektedir. Bu bağlamda çalışmada, internetin başlangıçtaki merkeziyetçi yapısının, günümüzde karşılaşılan ticaret, güvenlik, ve evrensel haklar gibi karmaşık sorunlar karşısında yeni yönetişim mekanizmaları ve iş birliklerini gerektirdiği tespit edilmiştir. Bu, internet yönetişimi konusundaki tartışmaların sadece teknik meselelerle sınırlı kalmadığını, aynı zamanda geniş bir paydaş yelpazesinin katılımıyla şekillenen siyasi ve sosyal bir alan olduğunu vurgulamaktadır.

Çalışmanın ortaya çıkmasındaki ikinci motivasyon, bu birbirinden ayrı, ve fakat bir o kadar da birbiriyle bağlantılı olan bu sorunların yönetilip yönetilemeyeceğine dair bir argüman oluşturmaktı. Bu çalışma, internetin “yönetilebilir” ve “düzenlenebilir” potansiyeline dikkat çekmeyi tercih etti. Üstelik bu yapılırken, normatif bir vurgu ile

yola çıkıldı. Bu yaklaşımın korunması ve sürdürülmesi, kriminalize edilmiş ve güvenlikleştirilmiş bir alan için zordu, fakat gerekliydi. İnternetin yönetilebilir ve düzenlenebilir potansiyelinin altını çizen bu çalışma, özellikle uluslararası normatif teoriyi seçmiştir çünkü bu alanın geleneksel güvenlik odaklı değil; sürdürülebilir ve esnek yaklaşımlara ihtiyacı vardır. Ancak, bu alana yönelik teorik katkılarda bulunmaya çalışan teorisyenler, çeşitli engellerle karşılaşmaktadırlar. Bu engellerden biri, uluslararası ilişkilerde ahlaki yargıların uygunsuz olduğunu genel kabul gören fikirdir. Beitz'in vurguladığı üzere, bu, yaygın ancak yeterince sorgulanmamış bir inanç olup, normatif uluslararası teorinin imkânsız olduğu düşüncesini daima beslemektedir (1999, s. 5).

Normatif teorinin önündeki bu engeller, internetin yönetişimi ve düzenlenmesi konusunda normatif bir yaklaşımın gerekliliğini daha da önemli kılmaktadır. Zira internet, sınır ötesi bir yapıya sahip olduğu için, uluslararası normların ve standartların belirlenmesi, bu dijital ortamın daha adil, güvenli ve yönetilebilir hale gelmesini sağlayabilmektedir. Bu bağlamda, normatif teorinin internetin yönetişimiyle ilgili sorunlara çözüm bulmada önemli bir rol oynayabileceği bu çalışmanın başat argümanlarından birini oluşturmuş ve bundan edinilmiş bakış açısıyla siber uzayın yönetilebilir potansiyelini ortaya çıkaracak iyi yönetişim ilkeleri benimsenmiştir.

Bu yapılırken, internetin "düzenlenebilir" potansiyelinin önündeki engeller de göz ardı edilmemiştir. Siber uzayın doğası, aktör çeşitliliği, teknik bakış açısı ve işbirliği ile çıkar ikilemi gibi unsurlar, internetin yönetişimini ve düzenlenmesini zorlaştıran temel faktörler olarak tanımlanmıştır. Bu faktörlerin her biri, siber uzayın karmaşık yapısını ve yönetişimine yönelik çözümlerin bulunmasında karşılaşılan zorlukları vurgular. Siber uzayın doğası, onun sürekli gelişen ve değişen bir yapıda olmasından kaynaklanmaktadır. Aktör çeşitliliği, farklı hedefleri ve öncelikleri olan devletler, uluslararası kuruluşlar, özel sektör ve sivil toplum gibi çok sayıda paydaşın varlığıyla ilgilidir. Teknik bakış açısı, internetin teknik yönlerinin ve altyapısının karmaşıklığına işaret ederken, işbirliği ve çıkar ikilemi, paydaşların ortak hedeflere ulaşma konusunda işbirliği yapma kapasitesiyle ilgili zorluklara dikkat çeker.

Bu engellere rağmen, siber iyi yönetişimin mümkün olduğu argümanı, çalışmanın odaklandığı diğer bir önemli noktadır. Siber uzay, genellikle yönetilmeyen bir alan olarak görülse de, aslında çeşitli düzenleyici çerçevelerle desteklenen sınırlara sahiptir.

Ancak, siber uzaydaki faaliyetleri küresel ölçekte koruyacak ve teşvik edecek ortak bir "yargı" sisteminin eksikliği, yönetişim zorluklarını artırmaktadır. Uluslararası insan hakları normları ve standartları, siber uzaydaki yönetişim sistemlerini oluşturmak için temel ve rehber olarak kullanılabilir. Bu bağlamda iyi yönetişim, insan haklarını teşvik etmeli ve teknolojilerin insan haklarına saygılı bir şekilde geliştirilmesini ve kullanılmasını sağlamalıdır.

Bu faktörlerin etkin bir şekilde sağlanabilmesi, bahsi geçen iyi yönetişim ilkelerinin normatif bir çerçevede benimsenmesiyle mümkündür. Kısaca, çalışmada, etkin bir yönetişim mekanizmasının uygulanabilir olduğu; fakat bunun, ilgili tarafların söz konusu ilkeleri uygulamaya yönelik bir arzuya sahip olmaları koşuluna bağlı olduğu sonucuna varılmıştır. Zira siber alanın doğasından kaynaklanan zorlukların üstesinden gelinebileceği, başarılı uygulamalardan açıkça anlaşılmaktadır. Bu bağlamda, kilit faktör, işbirliği faktörlerini güçlendirerek çok paydaşlı bir yapıyı desteklemektir.

Çalışmanın sorun alanları ve bu alanlara yönelik çözüm önerileri geliştirilirken, düzenleyici bir hukuk mekanizmasının olmayışının alandaki en büyük sorunu teşkil ettiği sonucuna varılmıştır. Bu bağlamda bu çalışma açısından hukuk, hem olmayışı nedeniyle bir sorunu, hem de olması halinde en büyük çözümü teşkil etmektedir. Bu bağlamda sorunların çözümünde çeşitli yaklaşımlar ve alternatif çözüm önerileri gündeme getirilmiştir.

Başlangıçta, internetin düzenlenmesi alanı liberal bir perspektif tarafından domine edilirken, bu bakış açısı kısa süre içinde yerini internetin uluslararası düzenlenmesinin hem uygulanabilir hem de meşru olduğunu savunan görüşlere bırakmıştır. Bu iddia sonrasında uluslararası hukuk uzmanları tarafından desteklenmiştir. 21. yüzyıla gelindiğinde, uluslararası hukukun bu alandaki özel rolü daha detaylı bir şekilde incelenmiş ve internet yönetişiminin önemli bir kavram olarak ele alınması bu alana önemli katkılar sunmuştur. 2010 yılına gelindiğinde, internet hukukunun temel ilkelerine odaklanan yasal bir çerçeve ortaya konmuştur. Özellikle 2010 sonrası dönemde, bu alana yönelik ilginin arttığı literatürden anlaşılmaktadır. Yapılan çalışmalar genellikle geleneksel uluslararası hukuk yaklaşımını temsil ederek, yasal meselelere odaklanmaktadır. Uluslararası hukukun genel ilkeleri, siber terörizm, siber suçlar ve siber casusluk gibi sorunların ele alınmasında vurgulanmıştır. İnternet yönetişimine uluslararası hukukun uygulanması gerektiğini savunan görüşlerin yanı

sıra, internet düzenlemesinde daha geniş bir yasal çerçeve sunan çok merkezli bir yönetişim yaklaşımı da önerilmiştir. Bu yaklaşım, internet yönetişiminin çok paydaşlı modeline işaret ederek, mevcut düzenleyici ilkelere devlet dışı aktörleri de yasal olarak dahil etmeye yönelik daha kapsayıcı bir çerçeve önermiştir.

Farklı yaklaşımların geliştirilmesi her zaman yararlıdır. Ama netice olarak bugün bu seçeneklerin uygulanabilmesi için gerekli olan evrensel norm ve kurumlar mevcut değildir. Elbette birtakım özel ve bölgesel girişim söz konusudur. Ancak bu sorunun çözümü, ulusal ve bölgesel sınırlardan bağımsız küresel bir formül inşa etmektir. Sorun şu ki, uluslararası hukuk, fiziksel alanda dahi işlevini yerine getirememektedir. Zira bugün uluslararası hukuk, devletler arasındaki anlaşmazlıkları çözmekten çok bir yüzleşme aracı olarak kullanılmaktadır. Bu durum sorunu daha da derinleştirmektedir. Siber alandaki zararlı faaliyetler giderek daha tehlikeli hale gelmekte ve geçerli uluslararası yasal normların yeterliliğini sorgulatmaktadır. Bazı durumlarda internetin pasifleştirilmesi ve siber şiddetin uluslararası hukuk sözleşmeleri aracılığıyla çözülmesi gibi seçenekler önerilmektedir. Bu gerçekleşmediği takdirde, siber risklerin sadece uluslararası tüzel kişilere ve uluslararası topluma değil, uluslararası hukuka da zarar vereceği düşünülmektedir.

Bu doğrultuda çalışma, diğer bir motivasyonu oluşturan "olası bir siber hukuk mekanizması" üzerinde düşünmeye teşvik etmektedir. Siber uzayın hem fırsatlar sunan hem de riskler barındıran bir alan olarak kabul edilmesi, daha fazla düzenlemeye ihtiyaç duyulduğu konusunda artan bir konsensüs olduğunu göstermektedir. Ancak tartışma konusu, düzenlemenin gerekliliği değil, nasıl ve ne şekilde yapılacağıdır. Bu bağlamda, işbirliğini ve iyi vatandaşlığı desteklemek amacıyla ortak değerler, ilkeler ve davranış normlarına dayalı bir düzenleyici çerçeve oluşturulması gerektiği vurgulanmaktadır.

Mevcut uluslararası hukuk mekanizmalarının siber uzayın yönetişimi konusunda yetersiz kaldığı, siber uzaya geleneksel uluslararası hukukun uygulanmasının devletler arasındaki konularda bir nebze etkili olabileceği ancak bireyler, özel sektör ve kuruluşların bu noktada eksik kalacağı tespit edilmiştir. Bu, mevcut yasal çerçevenin kullanımının pek çok durumda zorlaştığını göstermektedir. Siber alanın potansiyel risk ve tehditleri bünyesinde barındıran kriminal bir alan olması, uluslararası siber hukuk mekanizmasının oluşturulmasını zorunlu hale getirmektedir. Etkili bir uluslararası siber

hukuk mekanizmasının oluşturulmasında birtakım zorluklar olsa da, bu çok paydaşlı işbirliği, esnek ve dinamik yaklaşım, geliştirilmiş diyalog kültürü, siber/dijital diplomasi faaliyetleri, teknoloji tarafsızlığı ve uyumluluk, eğitim ve farkındalık ve hesap verebilirlik gibi unsurların hayata geçirilmesiyle mümkündür.

Bu alanın yönetilebilir olduğu ve etkin bir hukuk mekanizmasının oluşturulabileceği fikri, temelde soyut bir argüman gibi gözükse de, somut bir dayanaktan güç almıştır: IGF modeli. Zira bugün IGF, halihazırda normatif argümanların ve iyi yönetişim ilkelerinin uygulandığı bir platform olarak karşımıza çıkmakta ve bu yönüyle bu çalışmanın argümanlarına somut bir mahiyet kazandırmaktadır. Model, geniş bir paydaş yelpazesini kapsayarak sürdürülebilir ve etkili çözümler üretme kapasitesine sahip olduğunu kanıtlamıştır. IGF'nin teknolojik gelişmelere hızla uyum sağlayabilecek esnekliğe sahip olduğu, bu gelişmelere bağlı olarak ortaya çıkan yeni sorunlara çözüm üretebilecek kapasitede olduğu tespit edilmiştir. Ayrıca, IGF modelinin siber hukuk alanında –en azından yumuşak hukuk bağlamında– normatif çözümler ve standartlar geliştirme konusunda kritik bir platform sağladığı gözlemlenmiştir.

Öte yandan, IGF'nin bağlayıcı olmayan karar alma yapısının, çok paydaşlığın sınırlarını ortaya koyduğu, bu yapının küresel siber alanın yönetişimi için geniş katılımlı bir diyalog ve işbirliği ortamı sunduğu ancak somut politika değişiklikleri ve uygulamaları konusunda yeterli yetkiye sahip olmadığı gözlemlenmiştir. Bu durum, özellikle uluslararası düzeyde etkili olması gereken meselelerde IGF'nin önerilerinin somut sonuçlar doğurmasını zorlaştırmaktadır. Ancak, geleneksel uluslararası hukukun zaman içinde devlet dışı aktörlere de alan açmaya başlaması, IGF gibi platformların hukuki bağlayıcılık kazanması noktasında önemli bir gelişme olarak değerlendirilmiştir.

Ancak IGF'nin mevcut yapısı, bağlayıcı olmayan kararları nedeniyle kritik bir zayıflık taşımaktadır. Bu yapı, önerilerin ciddiye alınmasını ve uygulanmasını zorunlu kılmadığından, özellikle uluslararası düzeyde etkili olması gereken meselelerde forumun önerilerinin somut sonuçlar doğurmasını zorlaştırmaktadır. Bu nedenle, IGF'nin önerilerinin bağlayıcılık kazanması, belirli hukuki süreçler ve yapısal değişiklikler aracılığıyla, teorik olarak mümkündür. Bu bağlamda, IGF'nin etkisini artırmak ve küresel internet yönetişiminde daha somut değişiklikler yapabilmek için, forumun yapısında ve işleyişinde önemli değişikliklere ihtiyaç duyduğu sonucuna varılmıştır.

IGF'nin çok paydaşlı modelinin, küresel internet yönetişimi sorunlarına çözüm bulma konusunda önemli bir potansiyel taşıdığı ancak bu potansiyelin tam olarak gerçekleşebilmesi için forumun bağlayıcılık kazanması gerektiği vurgulanmıştır. IGF'nin bağlayıcılığını artırmak ve küresel internet yönetişiminde daha etkili bir rol oynamak için hukuki süreçler ve yapısal değişikliklerin gerekliliği ortaya konmuştur. Bu değişiklikler, IGF'nin önerilerinin uluslararası düzeyde daha etkili olmasını sağlayacak ve küresel internet yönetişimi sorunlarına karşı daha somut çözümler üretmesine olanak tanıyacaktır. Bu bağlamda, siber uzayın karmaşık ve dinamik doğasını dikkate alarak, çok paydaşlı işbirliği, esnek yaklaşımlar ve sürdürülebilir diyalog kültürünün önemi bir kez daha vurgulanmaktadır. Dolayısıyla, IGF'nin mevcut ve gelecekteki zorluklara etkili çözümler üretebilmesi için, bağlayıcılığı artırma ve yapısında gerekli değişiklikleri yapma yolunda adımlar atılması zorunludur.

Sonuç olarak, bu tez, internetin yönetişimi konusunda iyi yönetişim ilkelerini esas alan bir model önerisi sunmaktadır. Bu model, çok paydaşlı işbirliği, esnek ve dinamik yaklaşımlar ve geliştirilmiş diyalog kültürünü içermektedir. Bu bağlamda internet yönetişimi, sadece teknik bir mesele olmaktan çıkıp, sosyal adalet, eşitlik ve insan hakları gibi temel değerleri içeren küresel bir konu olarak ele alınmalıdır. İnternetin evrensel ve eşit erişim ilkelerine ters düşen güç merkezleri tarafından domine edilmesi yerine, teknolojik eşitsizliklerin ve paydaşlar arasındaki bölünmelerin üstesinden gelinerek, etkili bir denetim mekanizması kurulmalıdır. Bu, sadece belirli güç merkezleri tarafından değil, geniş bir paydaş yelpazesinin katılımı ve uzlaşısı ile mümkün olacaktır.

KAYNAKÇA

AAG. (2022, Aralık). The Latest 2022 Cyber Crime Statistics. https://aag-it.com/the-latest-2022-cyber-crime-statistics/

Abbate, J. (1999). *Inventing the Internet*. Cambridge, MA: MIT Press.

Abbott, K. W., & Snidal, D. (2000). Hard and Soft Law in International Governance. *International Organization, 54*(3), 421–456.

Abbott, K. W., Green, J. F., & Keohane, R. O. (2016). Organizational Ecology and Institutional Change in Global Governance. *International Organization, 70*(2), 247–277.

Acharya, A. (2004). *Constructing a New World Order: Multipolarity, Globalization, and the United Nations*. Routledge.

Adams, S., Brokx, M., Dalla Corte, L., Galič, M., Kala, K., Koops, B. J., Leenes, R., Schellekens, M., E Silva, K., & Skorvánek, I. (2015). The governance of cybersecurity: A comparative quick scan of approaches in Canada, Estonia, Germany, the Netherlands and the UK. Tilburg University.

Adler, E. & Haas, P. M. (1992). Conclusion: Epistemic Communities, World Order, and the Creation of a Reflective Research Program. *International Organization, 46*(1), 367-390.

Adler, E., & Bernstein, S. (2004). Power in Global Governance: Knowledge in power: the epistemic construction of global governance. İçinde M. Barnett & R. Duvall (Eds.), *Power in Global Governance* (ss. 294-318). Cambridge University Press.

Adomey, M. K. G. (t.y.). *Introduction to Cryptography*. International Telecommunication Union. https://www.itu.int/en/ITU-D/Cybersecurity/Documents/01-Introduction%20to%20Cryptography.pdf (20.02.2023).

African Union. (2014, Haziran 27). African Union Convention on Cyber Security and Personal Data Protection. https://au.int/sites/default/files/treaties/29560-treaty-0048_-_african_union_convention_on_cyber_security_and_personal_data_protection_e.pdf

Äijälä, J., Riikonen, R., Huhtinen, A.-M., & Sederholm, T. (2023, Kasım 16). Adolescents and the dark side of social media – Law enforcement perspectives. *Sec. Media Governance and the Public Sphere.* https://www.frontiersin.org/articles/10.3389/fcomm.2023.1106165/full

Akdeniz, Y. (2004). Çağdaş İnternet Yönetimi. http://www.policy.hu/akdeniz/beyaz_kitap_sura.pdf

Akyeşilmen, N. (2018a). *Disiplinlerarası Bir Yaklaşımla Siber Politika & Siber Güvenlik*. Ankara: Orion Kitabevi.

Akyeşilmen, N. (2018b). Cyber Good Governance: A New Challenge in International Power Politics? *Cyberpolitik Journal, 3*(5&6), 2-21.

ALAC. (t.y.). Community. https://atlarge.icann.org/alac (05.06.2021).

Alvestrand, H. (2004, Şubat). Request for Comments 3710: An IESG charter. IETF. https://tools.ietf.org/html/rfc3710

Amnesty International. (2015, Aralık 15). Tech companies must reject China's repressive internet rules.

Amnesty International. (2021). *Amnesty International Report 2020/21: The State of the World's Human Rights*. https://reliefweb.int/sites/reliefweb.int/files/resources/POL1032022021ENGLISH.PDF

Andjelkovic, M. (2006, Eylül). Internet Governance: In the Footsteps of Global Administrative Law. University of Kent Law School, Brussels. https://www.iisd.org/system/files/publications/infosoc_int_gov_law.pdf

Andrews, E. L. (1993, Eylül 15). Business Technology; Policy Blueprint Ready For Data Superhighway. *The New York Times*. https://www.nytimes.com/1993/09/15/business/business-technology-policy-blueprint-ready-for-data-superhighway.html

APC. (2016, Aralık 15). Spotlight on national and regional initiatives at the global IGF. https://www.apc.org/en/news/spotlight-national-and-regional-initiatives-global

APNIC. (2024, Ocak 17). IP addresses through 2023. https://blog.apnic.net/2024/01/17/ip-addresses-through-2023/

Arner, D. W., Castellano, G., & Selga, E. (2021). The Transnational Data Governance Problem. *Berkeley Technology Law Journal*. University of Hong Kong Faculty of Law Research Paper No. 2021/039.

ASO. (t.y.). Our Purpose. https://aso.icann.org/ (05.06.2021).

Atzori, M. (2017). Blockchain technology and decentralized governance: Is the state still necessary? *Journal of Governance and Regulation, 6*(1), 45-62.

Avant, D. D., Finnemore, M., & Sell, S. K. (2010). *Who Governs the Globe?*. Cambridge University Press.

Avunduk, H., & Aşan, H. (2018). Blok Zinciri (Blockchain) Teknolojisi ve İşletme Uygulamaları: Genel Bir Değerlendirme. *Dokuz Eylül Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi, 33*(1), 369-384.

Aydınlı, E., & Rosenau, J. N. (2005). *Globalization, Security, and the Nation-State: Paradigms in Transition*. State University of New York Press.

Bail, C. A., Argyle, L. P., Brown, T. W., & Volfovsky, A. (2018). Exposure to opposing views on social media can increase political polarization. *PNAS, 115*(37), 9216–9221.

Baird, Z. (2002). Governing the Internet: Engaging Government, Business, and Nonprofits. *Foreign Affairs, 81*(6), 15-20.

Balkin, J. M. (2004). Digital Speech and Democratic Culture: a Theory of Freedom of Expression for the Information Society. *New York University Law Review, 79*(1), 1-55.

Banks, A. M. (2003). The Growing Impact of Non-State Actors on the International and European Legal Systems. *Faculty Publications, 132*, 293-299.

Barlow, J. P. (1996, Şubat 8). A Declaration of the Independence of Cyberspace. Electronic Frontier Foundation. https://www.eff.org/cyberspace-independence

Barnes, I. A. (2018, Aralık). *Implementation of Active Cyber Defense Measures by Private Entities: The Need for an International accord to Address Disputes*. Master Thesis. Naval Postgraduate School Monterey, California.

Barton, E. (n.d.). *What does sui generis mean?* Ed Barton. https://edbarton.com/topics/law/international-law/what-does-sui-generis-mean/#:~:text=Sui%20Generis%20is%20a%20Latin,unique%20status%20within%20the%20law. (02.03.2024).

Bauer, J. M. (2005, Ağustos 31). Internet governance: Theory and first principles. *ResearchGate*. Preliminary Draft.

Bavitz, C. T. (2019). The Right to be Forgotten and Internet Governance: Challenges and Opportunities. *Latin American Law Review, 02*, 1-21.

BBC News. (2015, Aralık 16). China internet: Xi Jinping calls for 'cyber sovereignty'.

Bechtold, S. (2003). Governance in Namespaces. *Loyola of Los Angeles Law Review, 36*, 1239-1320.

Belli, L. (2015). A heterostakeholder cooperation for sustainable internet policymaking. *Internet Policy Review, 4*(2).

Bendiek, A. (2014). Tests of Partnership Transatlantic Cooperation in Cyber Security, Internet Governance, and Data Protection. *SWP Research Paper, RP 5.*

Benedek, W., & Kettemann, M. C. (2013, Aralık). Freedom of Expression and the Internet. Council of Europe Publishing. https://rm.coe.int/prems-167417-gbr-1201-freedom-of-expression-on-internet-web-16x24/1680984eae

Benkler, Y. (2016). Degrees of Freedom, Dimensions of Power. *Dædalus, the Journal of the American Academy of Arts & Sciences, 145*(1), 18-32.

Bıçakcı, S. (2014). NATO'nun Gelişen Tehdit Algısı: 21. Yüzyılda Siber Güvenlik. *Uluslararası İlişkiler, 10*(40), 101-130.

BIS Shrapnel. (2001, Aralık). Telecommunication Infrastructures in Australia 2001: A Research Report. Technology Applications Group. https://www.accc.gov.au/system/files/Telecommunication%20Infrastructures%20in%20Australia%202001.pdf

Biersteker, T. J. (1992). The "Triumph" of Neoclassical Economics in the Developing World: Policy Convergence and Bases of Governance in the International Economic Order. In J. N. Rosenau & E.-O. Czempiel (Eds.), *Governance without Government: Order and Change in World Politics* (ss. 102-131). Cambridge University Press.

Bing, J. (2009). Building Cyberspace: A Brief History of Internet. İçinde L. A Bygrave & J. Bing (Eds.) *Internet Governance: Infrastructure and Institutions* (ss. 8-48). Oxford University Press.

Blumenthal, M. S., & Clark, D. D. (2001). Rethinking the Design of the Internet: The End-to-End Arguments vs. the Brave New World. *ACM Transactions on Internet Technology*, 1(1), 70-109.

BMSCE. (t.y.). Introduction to Big Data Analytics. https://bmsce.ac.in/Content/IS/Big_Data_Analytics_-_Unit_1.pdf (03.03.2024).

Bodeau, D., Boyle, S., Fabius-Greene, J., & Graubart, R. (2010). Cyber Security Governance A Component of MITRE's Cyber Prep Methodology, MITRE Technical Report.

Bonnici, J. P. M. (2008). *Self-Regulation in Cyberspace*. Information Technology and Law Series (ITLS, volume 16).

Bory, P. (2020). *The Internet Myth: From the Internet Imaginary to Network Ideologies*. London: University of Westminster Press.

Börzel, T. A., & Risse, T. (2010). Governance without a state: Can it work?. *Regulation & Governance, 4*, 113–134.

Bradner, S. (1996, Ekim). Request for Comments 2026: The Internet Standards Process – Revision 3. https://www.ietf.org/rfc/rfc2026.txt

Brighenti, A. M. (2019). Antonio Gramsci's Theory of the Civil Society. İçinde Moebius, S., Nungesser, F., & Scherke, K. (Eds.), *Handbuch Kultursoziologie*. Springer Reference Sozialwissenschaften. (ss. 483–489). Wiesbaden: Springer.

Brooks, J. (2012, Aralık 6). Hands off the Internet! *The New York Times*. https://www.nytimes.com/2012/12/07/opinion/hands-off-the-internet.html

Brown, C. (1992). *International Relations Theory: New Normative Approaches*. Harvester-Wheatons.

Brown, I. (2019, Mart 14). Coga TF Workshop. W3C. https://www.w3.org/Consortium/Offices/blog/category/w3c-offices/

Buchan, R., & Navarrete, I. (2020, Eylül 24). Cyber Espionage. Oxford Bibliographies. https://www.oxfordbibliographies.com/display/document/obo-9780199796953/obo-9780199796953-0212.xml

Buchanan, A., & Keohane, R. (2006). The Legitimacy of Global Governance Institutions. *Ethics & International Affairs, 20*, 405-437.

Budnitskiy, S. (2018). *Digital Nationalisms: Identity, Strategic Communication and Global Internet Governance*. Carleton University, Doctor of Philosophy, Ottawa.

Budnitsky, S., & Jia, L. (2018). Branding Internet sovereignty: Digital media and the Chinese–Russian cyberalliance. *European Journal of Cultural Studies, 21*(5), 594-613.

Bush, R., Karrenberg, D., Kosters, M., & Plzak, R. (2000). Root Name Server Operational Requirements. *RFC 2870*. https://www.rfc-editor.org/info/rfc2870

Bussolati, N. (2015). The Rise of Non-State Actors in Cyberwarfare. İçinde J. D. Ohlin, K. Govern, & C. Finkelstein (Eds.), *Cyber War: Law and Ethics for Virtual Conflicts* (ss. 102–126). Oxford.

Buterin, V. (2017). The meaning of decentralization. *Medium*. https://medium.com/@VitalikButerin/the-meaning-of-decentralization-a0c92b76a274

Bygrave, L. A., & Michaelsen, T. (2009). Governors of Internet. İçinde L. A. Bygrave & J. Bing (Eds.), *Internet Governance: Infrastructure and Institutions* (ss. 92-126). New York: Oxford University Press.

Cai, C. (2018). Global Cyber Governance: China's Contribution and Approach. *China Quarterly of International Strategic Studies, 4*(1), 55-76.

Canazza, M. R. (2018). The Internet as a global public good and the role of governments and multilateral organizations in global internet governance. *Journal Of Global Studies, Meridiano 47*(19), 1-18.

Carr, M. (2015). Power Plays in Global Internet Governance. *Millennium, 43*(2), 640-659.

Carr, M. (2016). *US Power and the Internet in International Relations*. London: Palgrave Macmillan.

Carrillo Santarelli, N. (2016, Kasım 21). Nonstate Actors. https://www.oxfordbibliographies.com/display/document/obo-9780199796953/obo-9780199796953-0085.xml

Castells, M. (1996). *The Rise of the Network Society*. Oxford: Blackwell Publishers.

Castells, M. (2001). *The Internet Galaxy: Reflections on the Internet, Business, and Society*. New York: Oxford University Press.

Cavelty, M. D., & Egloff, F. J. (2019). The Politics of Cybersecurity: Balancing Different Roles of the State. *St Antony's International Review, 15*(1), 37-57.

CCDCOE. (t.y.a). NATO Summit Updates Cyber Defence Policy. https://ccdcoe.org/incyder-articles/nato-summit-updates-cyber-defence-policy/ (08.09.2022).

CCDCOE. (t.y.b). The Tallinn Manual. https://ccdcoe.org/research/tallinn-manual/ (09.10.2023).

CCNSO. (t.y.). About. https://ccnso.icann.org/en/about (05.06.2021).

Cerf, V. (Ed.). (1998). "Request for Comments 2468: I Remember IANA". https://www.ietf.org/rfc/rfc2468.txt

Cerf, V. G., Senges, M., & Ryan, P. S. (2014). Internet Governance Is Our Shared Responsibility. *Journal of Law and Policy for the Information Society, 10*(1), 1-42.

CERN. (t.y.). *A short history of the Web*. https://www.home.cern/science/computing/birth-web/short-history-web (17.12.2022).

Cgi.br. (2014). Marco Civil Law of the Internet in Brazil, Law No. 12.965, 23 Nisan 2014. https://www.cgi.br/pagina/marco-civil-law-of-the-internet-in-brazil/180

Chang, L. Y. C., & Grabosky, P. (2017). The governance of cyberspace. İçinde P. Drahos (Ed.), *Regulatory Theory: Foundations and Applications* (ss. 533-551). ANY Press.

Chen, Y., Pereira, I., & Patel, P. C. (2021). Decentralized Governance of Digital Platforms. *Journal of Management, 47*(5), 1305–1337.

Chenou, J.-M. (2014, Şubat). From cyber-libertarianism to neoliberalism: Internet exceptionalism, multi-stakeholderism, and the institutionalisation of Internet governance in the 1990s. *Globalizations, 11*(2), 205-223.

Chenou, J.-M., & Radu, R. (2015). Beyond Turf Wars in Internet Governance: The Relationship between Internet Organizations and IGOs. İçinde M. Rioux & K. Fontaine-Skronski (Eds.), *Global Governance Facing Structural Changes: New Institutional Trajectories for Digital and Transnational Capitalism* (ss. 37-59). Palgrave Macmillan.

Chiarella, M. L. (2023). Digital Markets Act (DMA) and Digital Services Act (DSA): New Rules for the EU Digital Environment. *Athens Journal of Law, 9*(1), 33–58.

Choucri, N. (2014). Co-Evolution of Cyberspace and International Relations: New Challenges for the Social Sciences. *Massachusetts Institute of Technology Political Science Department Research Paper No 29*.

Choucri, N., & Goldsmith, D. (2012). Lost in cyberspace: Harnessing the Internet, international relations, and global security. *Bulletin of the Atomic Scientists, 68*(2), 70-77.

Christou, G., & Simpson, S. (2007). Gaining a Stake in Global Internet Governance: The EU, ICANN and Strategic Norm Manipulation. *European Journal of Communication, 22*(2), 147–164.

Christou, G., & Simpson, S. (2011). The European Union, multilateralism and the global governance of the Internet. *Journal of European Public Policy, 18*(2), 241–257.

Chuanying, L. (2016, Mayıs 24). China's Emerging Cyberspace Strategy. *The Diplomat*. https://thediplomat.com/2016/05/chinas-emerging-cyberspace-strategy/

CIS Legislation. (2009, Haziran 16). The agreement between the governments of state members of the Shanghai Cooperation Organization on cooperation in the field of ensuring the international information security. https://cis-legislation.com/document.fwx?rgn=28340

CISCO. (2016, Temmuz). The Zettabyte Era – Trends and Analysis. *White Paper*.

Cigi & Chatham House. (2016). Global Commission on Internet Governance: One Internet. https://www.cigionline.org/sites/default/files/gcig_final_report_-_with_cover.pdf

Cochran, M. (2004). *Normative Theory in International Relations: A Pragmatic Approach*. Cambridge University Press.

CoE. (2001, Kasım 23). Convention on Cybercrime. https://rm.coe.int/1680081561

CoE. (2003, Ocak 28). *Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems*. European Treaty Series - No. 189. https://rm.coe.int/168008160f

CoE. (2008, Mart 26). Recommendation of the Committee of Ministers to member states on measures to promote the respect for freedom of expression and information with regard to Internet filters. https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=09000016805d3bc4

CoE. (2011, Haziran). Research Division: Internet: Case-law of the European Court of Human Rights. https://www.refworld.org/pdfid/4ee1d5bf1a.pdf

CoE. (2014). The rule of law on the Internet and in the wider digital world. Issue paper published by the Council of Europe Commissioner for Human Rights.

CoE. (2016, Mart 30). Internet Governance – Council of Europe Strategy 2016-2019 Democracy, human rights and the rule of law in the digital world. https://rm.coe.int/16806ad2a8

CoE. (t.y.). The Budapest Convention (ETS No. 185) and its Protocols. https://www.coe.int/en/web/cybercrime/the-budapest-convention (03.01.2022).

Cogburn, D. L. (2017). Transnational Advocacy Networks in the Information Society. İçinde *Information Technology and Global Governance* (ss. 201-216). Springer.

Commission on Science and Technology for Development Eighteenth session. (2015, Mayıs 4-8). *Mapping of international Internet public policy issues*. Geneva.

Copeland, D. C. (2000). The Constructivist Challenge to Structural Realism: A Review Essay. *International Security, 25*(2), 187–212.

Corn, G. P., & Taylor, R. (2017). Sovereignty in the Age of Cyber. *AJIL Unbound, 111*, 207–212.

Cornett, L., & Caporaso, J. A. (1992). "And Still It Moves!" State Interests and Social Forces in the European Community. İçinde J. N. Rosenau & E.-O. Czempiel (Eds.), *Governance without Government: Order and Change in World Politics* (ss. 219-249). Cambridge University Press.

Coşkunoğlu, O. (2014, Temmuz 10). İnternet Yönetişimi (Söyleşi – 1. Bölüm). https://coskunoglu.org/i%CC%87nternet-y%C3%B6neti%C5%9Fimi-s%C3%B6yle%C5%9Fi-1-b%C3%B6l%C3%BCm-2ebe9680c34b

Couldry, N., & Mejias, U. A. (2018). Data Colonialism: Rethinking Big Data's Relation to the Contemporary Subject. *Television & New Media, 20*(4), 1-14.

Council of Europe Commissioner for Human Rights. (2014). *The rule of law on the Internet and in the wider digital world*. https://rm.coe.int/the-rule-of-law-on-the-internet-and-in-the-wider-digital-world-issue-p/16806da51c

Cox, R. W. (1992). Towards A Post-Hegemonic Conceptualizatıon of World Order: Reflections on the Relevancy of Ibn Khaldun. İçinde J. N. Rosenau & E.-O. Czempiel (Eds.), *Governance without Government: Order and Change in World Politics* (ss. 132-159). Cambridge University Press.

Creech, H., Maclean, D., Souter, D., & Vetter, T. (2009, Temmuz). Review of the Mandate of the Internet Governance Forum: A response from the International Institute for Sustainable Development. https://www.iisd.org/system/files/publications/igf_mandate_review.pdf

Crews, C. W., & Thierer, A. D. (2003). *Who Rules the Net?: Internet Governance and Jurisdiction*. Cato Institute.

Crocker, S. (Ed.) (1969). "Request for Comments (RFC) 1: Host Software". http://tools.ietf.org/html/rfc1

Crozier, R. (2019, Temmuz 1). Govt asked to create new ISP-level site blocking Powers. *Itnews*. https://www.itnews.com.au/news/govt-asked-to-create-new-isp-level-site-blocking-powers-527499

CURIA. (2014, Mayıs 13). An internet search engine operator is responsible for the processing that it carries out of personal data which appear on web pages published by third parties. Court of Justice of the European Union PRESS RELEASE No 70/14. https://curia.europa.eu/jcms/upload/docs/application/pdf/2014-05/cp140070en.pdf

Cutler, A. C. (2003). *Private Power and Global Authority: Transnational Merchant Law in the Global Political Economy*. Cambridge University Press.

CYBIL. (t.y.). Forum of Incident Response and Security Teams (FIRST). https://cybilportal.org/actors/forum-of-incident-response-and-security-teams-first/ (15.10.2022).

Czempiel, E.-O. (1992). Governance and Democratization. İçinde J. N. Rosenau & E.-O. Czempiel (Eds.), *Governance without Government: Order and Change in World Politics* (ss. 50-271). Cambridge University Press.

Çınar, Y. (2023). [Review of *Russia after 2020: Looking ahead after Two Decades of Putin*, by J. L. Black]. *Insight Turkey*, *25*(3), 300–302.

D'Incau, F., & Soesanto, S. (2017, Ağustos 15). The UN GGE is dead: Time to fall forward. European Council on Foreign Relations. https://ecfr.eu/article/commentary_time_to_fall_forward_on_cyber_governance/

Daigle, L. (2003). IETF ISOC Board of Trustee Appointment Procedures, Network Working Group: Request for Comments: 3677. December 2003. https://datatracker.ietf.org/doc/rfc3677/

Daigle, L. (2003). IETF ISOC Board of Trustee Appointment Procedures. *Network Working Group: Request for Comments: 3677*. https://datatracker.ietf.org/doc/rfc3677/

Davis, S. (1997). *Big Brother: Britain's Web of Surveillance and the New Technological Order*. Pan Books.

DCAF. (2019). Guide to Good Governance in Cybersecurity. https://www.dcaf.ch/sites/default/files/publications/documents/CyberSecurity_Governance_ENG_Jan2021_0.pdf

DDP. (t.y.). About Digital Defenders Partnership. https://www.digitaldefenders.org/about-ddp/ (10.12.2022).

de Filippi, P. (2019). Blockchain Technology and Decentralized Governance: The Pitfalls of a Trustless Dream. *Decentralized Thriving: Governance and Community on the Web 3.0*. https://hal.archives-ouvertes.fr/hal-02445179/document

de Filippi, P., & Lavayssière, X. (2020). Blockchain Technology: Toward a Decentralized Governance of Digital Platforms? İçinde *The Great Awakening: New Modes of Life amidst Capitalist Ruins* (ss. 185-222). Punctum Books.

de la Chapelle, B. (2007). The Internet Governance Forum: How a United Nations Summit Produced a New Governance Paradigm for the Internet Age. İçinde C. Möller & A. Amouroux (Eds.), *Governing the Internet: Freedom and Regulation in the OSCE Region* (ss. 19-26). OSCE.

de la Chapelle, B., & Fehlinger, P. (2016, Nisan). Jurisdiction on the Internet: From Legal Arms Race to Transnational Cooperation. Centre for International Governance Innovation and Chatham House. https://www.cigionline.org/static/documents/gcig_no28_web.pdf

de Vey Mestdagh, K., & Rijgersberg, R. (2010). Internet Governance and Global Self Regulation: Building Blocks for a General Theory of Self Regulation. *Legisprudence, 4*(3), 385-404.

Deibert, R. J. & Rohozinski, R. (2010). Risking Security: Policies and Paradoxes of Cyberspace Security. *International Political Sociology*, *4*(1), 15-32.

Deibert, R. J. (2002). Circuits of Power: Security in the Internet Environment. İçinde J. N. Rosenau & J. P. Singh (Ed.), *Information technologies and global politics: The changing scope of power and governance* (ss. 115-142). State University of New York Press.

Deibert, R. J. (2008). The geopolitics of internet control: Censorship, sovereignty, and cyberspace. İçinde *Routledge Handbook of Internet Politics* (ss. 339-352). Routledge.

Deibert, R. J., & Crete-Nishihata, M. (2012). Global governance and the spread of cyberspace controls. *Global Governance: A Review of Multilateralism and International Organizations, 18*(3), 339-361.

Deibert, R. J., & Rohozinski, R. (2010). Control and Subversion in Russian Cyberspace. İçinde R. J. Deibert, J. Palfrey, R. Rohozinski, & J. Zittrain

(Eds.), *Access Controlled: The Shaping of Power, Rights, and Rule in Cyberspace* (ss. 15–34). The MIT Press.

Delerue, F. (2020). *Cyber Operations and International Law*. New York: Cambridge University Press.

Demchak, C., & Dombrowski, P. (2013). Cyber Westphalia: Asserting State Prerogatives in Cyberspace. *Georgetown Journal of International Affairs*, 29–38.

Demir, İ. (2018). Cyber Challenge: Diminishing Power of the State in International Relations. Cyberpolitik Journal, 3(5 & 6), 35-46.

Demmers, J., Fernández Jilberto, A. E., & Hogenboom, B. (Eds.). (2004). *Good Governance in the Era of Global Neoliberalism: Conflict and depolitisation in Latin America, Eastern Europe, Asia and Africa*. Routledge. (Routledge studies in the modern world economy; Vol. 47).

DeNardis, L. & Hackl, A.M. (2015). Internet governance by social media platforms. *Telecommunications Policy, 39*(9), 761-770.

DeNardis, L. (2014). *The Global War for Internet Governance*. Yale University Press.

DeNardis, L. (2020). *The Internet in Everything: Freedom and Security in a World with No Off Switch*. Yale University Press.

DeNardis, L., & Raymond, M. (2013). Thinking Clearly About Multistakeholder Internet Governance. *GigaNet: Global Internet Governance Academic Network, Annual Symposium 2013*.

DeNardis, L., & Raymond, M. (2017). The Internet of Things as a Global Policy Frontier. *UC Davis Law Review, 51*(2), 475-497.

Desheng, C. (2019, Ekim 20). China to step up cyberspace cooperation. *China Daily*. http://www.wuzhenwic.org/download/CHN-BRO-Supplement-001.pgl.pdf

Deutsche Welle. (2012, Aralık 3). The global village, segmented? https://www.dw.com/en/uns-wcit-summit-opens-discussing-internet-regulation/a-16424046

Diehl, P. F., Ku, C., & Zamora, D. (2003). The Dynamics of International Law: The Interaction of Normative and Operating Systems. *International Organization, 57*(1), 43–75.

DiploFoundation. (2006, Şubat). Role of Civil Society: Internet Governance and Developing Countries. http://archive1.diplomacy.edu/pool/fileInline.php?IDPool=129

DiploFoundation. (t.y.). Internet governance and digital policy. https://www.diplomacy.edu/ig (08.09.2022).

Dixit, E. (2022). Current International Law for Cyber Crimes: A Need for Next Step. *Vol. II-I*, 83–92.

Doctorow, C. (2013, Mart 12). What I wish Tim Berners-Lee understood about DRM. *The Guardian*. https://www.theguardian.com/technology/blog/2013/mar/12/tim-berners-lee-drm-cory-doctorow

Dominic, E. (2020, Haziran 8). The debate over internet governance and cyber crimes: West vs the rest? The Centre for Internet & Society. https://cis-india.org/internet-governance/blog/the-debate-over-internet-governance-and-cyber-crimes-west-vs-the-rest

Doria, A., & Kleinwächter, W. (2008). Internet Governance Forum (IGF): The First Two Years. United Nations Digital Library. https://www.intgovforum.org/cms/hydera/IGFBook_the_first_two_years.pdf

Doty, N., Cooper, A., & Seltzer, W. (2023, Mart 10). Human rights and technical standard-setting for the Web. Unofficial Draft. https://www.ohchr.org/sites/default/files/documents/issues/digitalage/cfis/tech-standards/subm-standard-setting-digital-space-new-technologies-standard-setting-organizations-w3c-participants-7-input.pdf

Drake, W. J. (2004). Reframing Internet Governance Discourse: Fifteen Baseline Propositions. İçinde D. MacLean (Ed.), *Internet Governance: A Grand Collaboration*. New York: The United Nations Information and Communication Technology Taskforce, ss. 122-161.

Drake, W. J. (2005). Reforming Internet Governance: Perspectives from WGIG. New York: United Nations ICT Task Force.

Drake, W. J. (2015). Introduction: Why the WGIG still matters. İçinde W. J. Drake (Ed.), *The Working Group On Internet Governance: 10th Anniversary Reflections* (ss. 10-33). APC.

Dreyfuss, E. (2018, Ekim 23). Global Internet Access Is Even Worse Than Dire Reports Suggest. *Wired*. https://www.wired.com/story/global-internet-access-dire-reports/

Drezner, D. W. (2004). The Global Governance of the Internet: Bringing the State Back. *Political Science Quarterly, 119*, 477-498.

Drezner, D. W. (2008). *All Politics Is Global: Explaining International Regulatory Regimes*. Princeton University Press.CORDIS. (1994, Haziran 24-25). Bangemann report: Europe and the global information society. https://cordis.europa.eu/article/id/2730-bangemann-report-europe-and-the-global-information-society

Droege, C. (2011, Ağustos 16). No legal vacuum in cyber space. ICRC. https://www.icrc.org/en/doc/resources/documents/interview/2011/cyber-warfare-interview-2011-08-16.htm

Duberry, J. (2019). *Global Environmental Governance in the Information Age: Civil Society Organizations and Digital Media*. New York: Routledge.

Dutta, N., Jadav, N., Tanwar, S., Sarma, H. K. D., & Pricop, E. (2022). Importance of Cyberlaw. İçinde *Cyber Security: Issues and Current Trends*. Studies in Computational Intelligence, vol 995. (ss. 159–174). Singapore: Springer.

Dutton, W. H., & Peltu, M. (2007). The Emerging Internet Governance Mosaic: Connecting the Pieces. *Information Polity, 12*(1–2), 63–81.

Dutton, W. H., Blank, G., & Groselj, D. (2013). *Cultures of the Internet: The Internet in Britain Oxford Internet Survey 2013 Report*. OxIS. https://oxis.oii.ox.ac.uk/wp-content/uploads/sites/16/2014/11/OxIS-2013.pdf

Dyer, H. C. (1997). *Moral Order/World Order: The Role of Normative Theory in the Study of International Relations*. Palgrave Macmillan.

Ebert, H., & Maurer, T. (2013). Contested Cyberspace and Rising Powers. *Third World Quarterly, 34*(6), 1054–1074.

Economy, E. C. (2019, Haziran 29). The great firewall of China: Xi Jinping's internet shutdown. *The Guardian*. https://www.theguardian.com/news/2018/jun/29/the-great-firewall-of-china-xi-jinpings-internet-shutdown

Eggenschwiler, J. (2019). An Incident-Based Conceptualization of Cybersecurity Governance. İçinde R. Ellis & V. Mohan (Eds.), *Rewired: Cybersecurity Governance* (ss. 81-96). John Wiley & Sons.

Eichensehr, K. E. (2015a). The Cyber-Law of Nations. *The Georgetown Law Journal, 103*, 317-380.

Eichensehr, K. E. (2015b, Şubat 2). International Cyber Governance: Engagement Without Agreement? *Just Security*.

https://www.justsecurity.org/19599/international-cyber-governance-engagement-agreement/

Epstein, D. (2013). The Making of Institutions of Information Governance: The Case of the Internet Governance Forum. *Journal of Information Technology, 28*(2), 137-149.

Epstein, D., & Nonnecke, B. M. (2016). Multistakeholderism in Praxis: The Case of the Regional and National Internet Governance Forum (IGF) Initiatives. *Volume 8, Issue 2*, 148-173.

Ermağan, İ. (2022a). *Uluslararası İlişkiler ve Teknoloji İlişkisi: Endüstri 4.0, Siber Uzay ve Uzay Dünyası* (3. baskı). Nobel Akademik Yayıncılık.

Ermağan, İ. (2022b). Uluslararası İlişkiler ve Teknoloji: Girift Bir İlişkinin Sonu Disiplinde Yeni Bir "Alt Dal" Mı?. *Akademik Hassasiyetler*, *9*(18), 49-78.

Euronews. (2021, Haziran 28). BM Genel Sekreteri Guterres: Küresel sorunları çözmek için uluslararası iş birliği gerekli. https://tr.euronews.com/2021/06/28/bm-genel-sekreteri-guterres-kuresel-sorunlar-cozmek-icin-uluslararas-is-birligi-gerekli

EUROPOL. (2013, Ocak). EC3 First Year Report. https://www.europol.europa.eu/sites/default/files/documents/ec3_first_year_report.pdf

EUROPOL. (t.y.). European Cybercrime Centre - EC3: Combating crime in a digital age. https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3 (07.08.2023).

Fang, B. (2018). Positions of States Toward Cyberspace and Cyber-Relating Regulations. İçinde B. Fang (Ed.), *Cyberspace Sovereignty: Reflections on building a community of common future in cyberspace* (ss. 243-320). Springer.

Farrell, H. (2003). Constructing the International Foundations of E-Commerce – The EU-US Safe Harbor Agreement. *International Organization, 57*.2, 277-306.

Fidler, D. P. (2013a). Internet Governance and International Law: The Controversy Concerning Revision of the International Telecommunication Regulations. *American Society of International Law, 17*(6).

Fidler, D. P. (2013b). Final Acts of the World Conference on International Telecommunications. *International Legal Materials, 52*(3), 843–860.

Filgueiras, F., & Almeida, V. (2021). *Governance for the Digital World Neither More State nor More Market*. Palgrave Macmillan.

Fishman, W. (1980). Introduction to Transborder Data Flows. *Standford Journal of International Law, 16*.

Floridi, L. (2018). Soft ethics, the governance of the digital and the General Data Protection Regulation. *Philosophical transactions. Series A, Mathematical, physical, and engineering sciences, 376*(2133).

Ford, B. (2004). Unmanaged Internet Protocol: taming the edge network management crisis. *SIGCOMM Comput. Commun. Rev.*, 34(1), 93–98.

Franzese, P. W. (2009). Sovereignty in Cyberspace: Can It Exist?. *The Air Force Law Review,* Maxwell AFB, *64*, 1-42.

Freedom House. (2020). China Overview. https://freedomhouse.org/country/china/freedom-net/2020

Froomkin, A. M. (2000). Wrong Turn in Cyberspace: Using ICANN to Route Around the APA and the Constitution. *Duke Law Journal, 50*, 17-186.

Froomkin, A. M. (2003). Habermas@discourse.net: Toward a Critical Theory of Cyberspace. *Harvard Law Review, 116*, 749-873.

GAC. (t.y.). Role of the GAC. https://gac.icann.org/ (05.06.2021).

Gazete Duvar. (2016, Ağustos 20). İnternetin kontrolü Amerika'dan çıkıyor.

GDPR. (t.y.). Art. 17 GDPR: Right to erasure (‘right to be forgotten’). https://gdpr-info.eu/art-17-gdpr/ (15.03.2021).

Gemalmaz, M. S. (2022). Transformation From Soft Law to Hard Law of International Environmental Protection: Process, Basic Concepts and Principles – Part 1: “Common Heritage of Mankind”, “Present and Future Generations”, “Inter/Intra-generational Equity” and “Sustainable Development. *Annales De La Faculté De Droit d’Istanbul, 71*, 119-219.

Gill, L., Redeker, D., & Gasser, U. (2015). Towards Digital Constitutionalism? Mapping Attempts to Craft an Internet Bill of Rights. *Berkman Klein Center for Internet & Society Research Publication 2015-15*.

Gleckman, H. (2018). *Multistakeholder Governance and Democracy: A Global Challenge*. Routledge.

Globe. (2020). *Report: Case study of cyber governance*. https://www.globe-project.eu/case-study-of-cyber-governance_11363.pdf

GNSO (t.y.). GNSO Policy Development Process (PDP). https://gnso.icann.org/en/basics/consensus-policy/pdp (05.06.2021).

Goehring, J. S. (2021). Why Isn't Outer Space a Global Commons? *Journal of National Security Law & Policy, 11*, 573-590.

Goldmann, M. (2012). We Need to Cut Off the Head of the King: Past, Present, and Future Approaches to International Soft Law. *Leiden Journal of International Law, 25*, 335-368.

Goldsmith, J. (1998). 'Against Cyberanarchy'. *University of Chicago Law Review, 65*.

Goldsmith, J. (2010, Haziran 14). *A Future Challenges: Cybersecurity Treaties: A Skeptical View*. Hoover Institution. https://www.hoover.org/sites/default/files/research/docs/futurechallenges_goldsmith.pdf

Goldsmith, J., & Wu, T. (2006). *Who Controls the Internet? Illusions of a Borderless World*. Oxford University Press.

Goudal, T., Bechara, A. J., Paoletti, M., & Azari, A. A. (2020). General Assembly First Committee Background Guide 2020. National Model United Nations, New York City, NY, USA 29 Mart- 2 Nisan (Conf. A) / 5-9 Nisan (Conf. B). https://www.nmun.org/assets/documents/conference-archives/new-york/2020/ny20-bgg-ga1.pdf

Government of the Russian Federation. (2015, Nisan 30). Agreement between the Government of the Russian Federation and the Government of the People's Republic of China on cooperation in ensuring international information security. https://cyber-peace.org/wp-content/uploads/2013/05/RUS-CHN_CyberSecurityAgreement201504_InofficialTranslation.pdf

Granjal, J., Monteiro, E., & Sá Silva, J. (2015). Security for the Internet of Things: A Survey of Existing Protocols and Open Research Issues. *IEEE Communications Surveys & Tutorials*, 17(3), 1294-1312.

Greenberg, B. A. (t.y.). Rethinking Technology Neutrality. *Minnesota Law Review*, 100, 1495-1561.

Grewlich, K. W. (2005). Internet Governance: Definition; Governance tools; Global Multi-stakeholder entity. UN ICT Task Force. http://www.wgig.org/docs/Grewlich.pdf

Guan, Y. (2023). The Past, Conundrums, and Future of International Cybersecurity Governance. *International Journal of Frontiers in Sociology, 5*(4), 61–65.

Gueham, F. (2017, Şubat). Digital sovereignty – steps towards a new system of internet governance. Fondapol. https://www.fondapol.org/en/study/digital-sovereignty-steps-towards-a-new-system-of-internet-governance/

Gurjar, L. R. (t.y.). Cyber Crimes. Vardhaman Mahaveer Open University. http://assets.vmou.ac.in/PGDCL04 (06.03.2023).

Haigh, T., Russell, A. L., & Dutton, W. H. (2015). Histories of the Internet: Introducing a special issue of information & culture. *Information & Culture, 50*(2), 143–159.

Haksever, G. (2018). *İnternet ve Çok-Paydaşlı Yönetişimi*. Yayımlanmamış Yüksek Lisans Tezi, İstanbul Bilgi Üniversitesi: İstanbul.

Hambridge, S. (1995, Ekim). Request For Comments 1855: Netiquette Guidelines. IETF. https://www.ietf.org/rfc/rfc1855.txt

Hansen, L., & Nissenbaum, H. (2009). Digital Disaster, Cyber Security, and the Copenhagen School. *International Studies Quarterly, 53*(4), 1155-1175.

Harbath, K., & Fernekes, C. (2022, Eylül 28). A Brief History of Tech and Elections: A 26-Year Journey. Bipartisan Policy Center. https://bipartisanpolicy.org/report/history-tech-elections/

Haristya, S. (2015). Multistakeholderism and the Democratic Deficit. İçinde W. J. Drake (Ed.), *The Working Group On Internet Governance: 10th Anniversary Reflections*. APC, 123-135.

Haristya, S. (2020). The Efficacy of Civil Society in Global Internet Governance. *Internet Histories, 4*(3), 252-270.

Harris, S. (2001). The Tao of IETF - A Novice's Guide to the Internet Engineering Task Force. *Network Working Group: Request for Comments: 3160*. https://www.rfc-editor.org/rfc/rfc3160

Hauben, M., & Hauben, R. (1998). Preface: What is a Netizen? *First Monday, 3*(7).

Held, D. (1995). *Democracy and the Global Order: From the Modern State to Cosmopolitan Governance*. Polity Press.

Hemmati, M. (2002). *Multistakeholder Processes for Governance and Sustainability: Beyond Deadlock and Conflict*. London: Earthscan Publications. https://minuhemmati.net/wpcontent/uploads/Hemmati-2002.pdf

Henderson, C. (2015). The United Nations and the regulation of cyber-security. İçinde N. Tsagourias & R. Buchan (Eds.), *Research Handbook on International Law and Cyberspace* (ss. 465–490).

Hildebrandt, M. (2020). International and Supranational Law. İçinde *Law for Computer Scientists and Other Folk* (ss. 1-18). Oxford Academic.

Hill, J. F., & Noyes, M. (2019). Rethinking Data, Geography, and Jurisdiction: A Common Framework for Harmonizing Global Data Flow Controls. İçinde R. Ellis & V. Mohan (Eds.), *Rewired: Cybersecurity Governance* (ss. 195-229). John Wiley & Sons.

Hirshleifer, J. (1995). Anarchy and its Breakdown. *Journal of Political Economy, 103*(1), 26-52. The University of Chicago Press.

Hirst, P., Thompson, G., & Bromley, S. (2009). *Globalisation in Question*. Polity Press.

Hofmann, J. (2007). Internet Governance: A Regulative Idea in Flux. İçinde R. K. J. Bandamutha (Editor), *Internet Governance: An Introduction*. Icfai University Press.

Hofmann, J., Katzenbach, C., & Gollatz, K. (2017). Between coordination and regulation: Finding the governance in Internet governance. *New Media and Society, 19*(9), 1406–1423.

Holbrook, J. (2000, Fall). Republic.com, by Cass R. Sunstein. *Harvard Journal of Law and Technology, 14*(1), 753-766.

Holsti, K. J. (1992). Governance Without Government: Polyarchy in Nineteenth-Century European International Politics. İçinde J. N. Rosenau & E.-O. Czempiel (Eds.), *Governance without Government: Order and Change in World Politics* (ss. 30-57). Cambridge University Press.

Houser, K., & Voss, W. G. (2018). GDPR: The End of Google and Facebook or a New Paradigm in Data Privacy? *25 Rich. J. L. & Tech. 1*.

Hoxtell, W., & Nonhoff, D. (2019). Internet Governance: Past, Present and Future. Konrad-Adenauer-Stiftung e.V. https://www.kas.de/en/single-title/-/content/internet-governance-past-present-and-future

Hösl, M. (2019). Semantics of the internet: a political history. *Internet Histories, 3*(3-4), 275-292.

Hubbard, A., & Bygrave, L. A. (2009). Internet Governance Goes Global. İçinde L. A. Bygrave & J. Bing (Eds.), *Internet Governance: Infrastructure and Institutions* (ss. 213-236). New York: Oxford University Press.

Hunter, D. (2003). Cyberspace as Place and the Tragedy of the Digital Anticommons. *91 Calif. L. Rev.* 439, 518.

Hurrell, A. (2002). Norms and Ethics in International Relations. İçinde *Handbook of International Relations* (ss. 183-207). SAGE Publications.

Huston, G. (2004, Kasım). ICANN, the ITU and WSIS and Internet Governance – Part II. APNIC. http://www.apnic.net/community/ecosystem/igf/articles/icann-wsis-part-ii

IAB. (t.y.a). About. https://www.iab.org/about/ (11.05.2021).

IAB. (t.y.b). Description. https://www.iab.org/about/description/ (11.05.2021).

IAB. (t.y.c). History. https://www.iab.org/about/history/ (11.05.2021).

IAB. (t.y.d). Overview. https://www.iab.org/about/iab-overview/ (11.05.2021).

IANA. (t.y.a.). Domain Names. https://www.iana.org/domains (19.05.2021).

IANA. (t.y.b.). Protocol Assignments. https://www.iana.org/protocols (19.05.2021).

IANA. (t.y.c.). Number Resources. https://www.iana.org/numbers (19.05.2021).

IANA. (t.y.d.). Number Resources. https://www.iana.org/numbers (08.09.2022).

IBM. (2006, Aralık). TCP/IP Tutorial and Technical Overview. https://www.redbooks.ibm.com/redbooks/pdfs/gg243376.pdf

IBM. (2021, Mart 22). Internet Protocol Version 4 (IPv4). https://www.ibm.com/docs/en/zos/2.2.0?topic=ipv6-internet-protocol-version-4-ipv4

IBM. (t.y.). Blockchain success starts here. https://www.ibm.com/tr-tr/topics/what-is-blockchain (20.10.2021).

ICANN. (1998, Kasım 25). Memorandum of Understanding Between the U.S. Department of Commerce and Internet Corporation for Assigned Names and Numbers. https://www.icann.org/resources/unthemed-pages/icann-mou-1998-11-25-en

ICANN. (2016, Ekim 1). Stewardship of IANA Functions Transitions to Global Internet Community as Contract with U.S. Government Ends. https://www.icann.org/en/announcements/details/stewardship-of-iana-functions-transitions-to-global-internet-community-as-contract-with-us-government-ends-1-10-2016-en

ICANN. (t.y.). ICANN's Historical Relationship with the U.S. Government. https://www.icann.org/en/history/icann-usg (02.08.2022).

ICANN. (t.y.). What the Ombudsman Can Do For You. https://www.icann.org/ombudsman (05.06.2021).

ICANN. (t.y.a). The History of ICANN. https://www.icann.org/history (11.05.2021).

ICANN. (t.y.b). Get Started. https://www.icann.org/get-started (11.05.2021).

ICANN. (t.y.d.). Address Supporting Organization. https://aso.icann.org/ (08.09.2022).

IETF. (t.y.). "Participate in the IETF". https://www.ietf.org/about/participate/ (06.03.2021).

IETF. (t.y.a). About. https://www.ietf.org/about/ (11.05.2021).

IETF. (t.y.b). How We Work. https://www.ietf.org/how/wgs/ (19.05.2021).

IFLA. (t.y.a.). A Guide to the Policies and Processes behind the Internet and their Impact Part 5: Legal, Economic and Security Issues in Internet Governance. *Internet Governance for Libraries*. https://www.ifla.org/wp-content/uploads/2019/05/assets/hq/topics/info-society/documents/ig_guide_chapter_5.pdf (13.09.2022).

IFLA. (t.y.b.). Background: The Right to be Forgotten in National and Regional Contexts. https://www.ifla.org/files/assets/faife/publications/rtbf_background.pdf (09.10.2022).

IGF Report. (2023). IGF 2023 Annual Meeting Summary Report, Eighteenth Meeting of Internet Governance Forum 8–12 Ekim 2023 Kyoto, Japan. https://www.intgovforum.org/en/filedepot_download/300/26575

IGF. (2006; 2007). Rio de Janeiro, Brazil. Internet Governance Forum (IGF) The First Two Years. Edited by Avri Doria and Wolfgang Kleinwächter in cooperation with the IGF Secretariat. https://www.intgovforum.org/en/filedepot_download/3367/5

IGF. (2008). Internet for all Proceedings of the Third Internet Governance Forum, Hyderabad, India, 3-6 December 2008. https://www.intgovforum.org/en/filedepot_download/3367/6

IGF. (2009). Internet governance: Creating opportunities for all The Fourth Internet Governance Forum, Sharm el Sheikh, Egypt, 15-18 November 2009. https://www.intgovforum.org/en/filedepot_download/3367/7

IGF. (2010). Developing the future together The Fifth Meeting of the Internet Governance Forum, Vilnius, Lithuania, 14-17 September 2010. https://www.intgovforum.org/en/filedepot_download/3367/8

IGF. (2011). 'Internet as a catalyst for change: access, development, freedoms, and innovation' The Sixth Meeting of the Internet Governance Forum, Nairobi, Kenya, 27-30 September 2011. https://www.intgovforum.org/en/filedepot_download/3367/9

IGF. (2012). 'Internet Governance for Sustainable Human, Economic and Social Development' The Seventh Meeting of the Internet Governance Forum, Baku, Azerbaijan, 6-9 November 2012. https://www.intgovforum.org/en/filedepot_download/3367/10

IGF. (2013). 'Building Bridges–Enhancing Multistakeholder Cooperation for Growth and Sustainable Development' The Eighth Meeting of the Internet Governance Forum, Bali, Indonesia, 22–25 October 2013. https://www.intgovforum.org/en/filedepot_download/3367/11

IGF. (2014). Connecting continents for enhanced multistakeholder Internet governance The Ninth Meeting of the Internet Governance Forum, Istanbul, Turkey, 2-5 September 2014. https://www.intgovforum.org/en/filedepot_download/3367/12

IGF. (2015). The 10th Internet Governance Forum (IGF): 'Evolution of Internet Governance: Empowering Sustainable Development' 10-13 November 2015, João Pessoa, Brazil Part I: Summary of IGF 2015 – Reports and outputs from the 10th IGF. https://www.intgovforum.org/en/filedepot_download/3367/208

IGF. (2016). The 11th Internet Governance Forum (IGF): 'Enabling Inclusive and Sustainable Growth' 6-9 December 2016, Jalisco, Mexico Summary of IGF 2016 – Abridged report. https://www.intgovforum.org/en/filedepot_download/3367/1048

IGF. (2017). The 12th Internet Governance Forum (IGF): 'Shape Your Digital Future!' Summary of IGF 2017 - Abridged report, 18 - 21 December 2017, Geneva, Switzerland. https://www.intgovforum.org/en/filedepot_download/3367/1544

IGF. (2018). Thirteenth Internet Governance Forum (IGF): 'The Internet of Trust' Chair's summary & IGF messages, 12 - 14 November 2018, Paris, France. https://www.intgovforum.org/en/filedepot_download/6037/1555

IGF. (2019). Chair's summary fourteenth meeting of Internet Governance Forum, Berlin, 25-29 November 2019. https://www.intgovforum.org/en/filedepot_download/9212/2172

IGF. (2020). 15th annual meeting Internet Governance Forum: Internet for human resilience and solidarity. https://www.intgovforum.org/en/filedepot_download/11138/2452

IGF. (2021). Summary sixteenth meeting of Internet Governance Forum, 6–10 December 2021, Katowice, Poland. https://www.intgovforum.org/en/filedepot_download/223/20706

IGF. (2022). Summary seventeenth meeting of Internet Governance Forum, 28 November – 2 December 2022, Addis Ababa, Ethiopia. https://mail.intgovforum.org/IGF2022_summaryreport_final.pdf

IGF. (2023). Summary eighteenth meeting of Internet Governance Forum, 8–12 October 2023, Kyoto, Japan. https://www.intgovforum.org/en/filedepot_download/300/26575

IGF. (t.y.). About IGF: Internet Governance Forum. https://www.intgovforum.org/en/about (05.02.2024).

IGF. (t.y.a). About the IGF. https://www.intgovforum.org/en/about#:~:text=The%20mandate%20was%20extended%20for,Summit%20on%20the%20Information%20Society (09.12.2023).

IGF. (t.y.b). General Guidance – MAG 2024 Renewal. https://www.intgovforum.org/en/content/general-guidance-mag-2024-renewal (05.02.2024).

Ignatov, A. (2022). The BRICS Agenda on Internet Governance. *International Organisations Research Journal*, *17*(2), 86–109.

International Convention concerning the Use of Broadcasting in the Cause of Peace. (1936, Eylül 23). https://docs.pca-cpa.org/2016/01/International-Convention-concerning-the-Use-of-Broadcasting-in-the-Cause-of-Peace-1936.pdf

International Telegraph Convention. (1872, Ocak 14). http://search.itu.int/history/HistoryDigitalCollectionDocLibrary/4.3.43.en.100.pdf

Internet Live Stats. (2021). Internet traffic today. https://www.internetlivestats.com/ (01.05.2021).

Internet Society. (2016, Nisan 26). Internet Governance Why the Multistakeholder Approach Works. https://www.internetsociety.org/wp-content/uploads/2016/04/IG-MultiStakeholderApproach.pdf

Investopedia. (t.y.). Internet Service Provider (ISP): What They Do and Examples. https://www.investopedia.com/terms/i/isp.asp (21.02.2022).

Iran Focus. (2012, Eylül 20). Iran preparing internal version of Internet.

IRTF. (t.y.). Overview. https://irtf.org/ (11.05.2021).

Isaak, J., & Hanna, M. J. (2018). User Data Privacy: Facebook, Cambridge Analytica, and Privacy Protection. *Computer, 51*(8), 56–59.

ISOC. (2016, Nisan 26). Internet Governance: Why the Multistakeholder Approach Works. https://www.internetsociety.org/resources/doc/2016/internet-governance-why-the-multistakeholder-approach-works/

ISOC. (2020). İnternet Yönetişimi: Çok Paydaşlı Yaklaşım Neden İşe Yarıyor?. https://isoc.org.tr/wp-content/uploads/2020/06/IG-MultiStakeholderApproach-TR.pdf

ISOC. (2020, Kasım 30). The Internet Society and IETF Announce New Strategic Agreement to Support Ongoing Work on Open Standards. https://www.internetsociety.org/news/press-releases/2020/the-internet-society-and-ietf-announce-new-strategic-agreement-to-support-ongoing-work-on-open-standards/

ISOC. (2021). Action Plan 2021: Empowering People to Create a Bigger and Stronger Internet. https://www.internetsociety.org/action-plan/2021/

ISOC. (t.y.a.). İnternet Yönetişimi: Çok Paydaşlı Yaklaşım Neden İşe Yarıyor?. https://isoc.org.tr/wp-content/uploads/2020/06/IG-MultiStakeholderApproach-TR.pdf (07.06.2021).

ISOC. (t.y.b.). History of the Internet Society. https://www.internetsociety.org/timeline/history/ (15.05.2021).

ISOC. (t.y.c.). Our Mission. https://www.internetsociety.org/mission/ (15.05.2021).

IT Governance Institute. (2010). Information Security Governance: Guidance for Boards of Directors and Executive Management. https://citadel-information.com/wp-content/uploads/2010/12/isaca-information-security-governance-guidance-for-boards-of-directors-and-executive-management-2001.pdf

ITU. (2003). WSIS The Geneva Declaration of Principles and Plan of Action.

ITU. (2005a, Kasım 16-18). Report of the Tunis phase of the World Summit on the Information Society.

ITU. (2005b, Haziran). *Background Report: The Working Group On Internet Governance*. https://www.itu.int/net/wsis/wgig/docs/wgig-background-report.pdf

ITU. (2012). World Conference on International Telecommunications (WCIT-12). https://www.itu.int/en/wcit-12/Pages/default.aspx

ITU. (2020a). Global Cybersecurity Index 2020: Measuring commitment to cybersecurity. ITU Publications.

ITU. (2020b). *Measuring digital development Facts and figures 2020*. ITU Publications. https://www.itu.int/en/ITU-D/Statistics/Documents/facts/FactsFigures2020.pdf

ITU. (t.y.). Definition of cybersecurity. https://www.itu.int/en/ITU-T/studygroups/com17/Pages/cybersecurity.aspx (10.09.2022).

ITU/UNESCO Broadband Commission for Sustainable Development. (2021, Eylül). *The State of Broadband 2021: People-Centred Approaches for Universal Broadband*. https://www.itu.int/dms_pub/itu-s/opb/pol/S-POL-BROADBAND.23-2021-PDF-E.pdf

ITÜBİDB. (2013, Eylül 6). DNS (Domain Name System – Etki Alanı Ad Sunucusu). https://bidb.itu.edu.tr/seyir-defteri/blog/2013/09/06/dns-(domain-name-system---etki-alan%C4%B1-ad-sunucusu)

Ivanova, K., Stepanov, A., & Nemchinova, E. (2019). Cyberbullying as a Deviation of the Right of Citizens to Freedom of Opinion on the Internet. *Actual Problems of Russian Law*.

Jang, J., McSparren, J., & Rashchupkina, Y. (2016). Global governance: present and future. *Palgrave Communications, Review Article*, Ocak 19. https://www.nature.com/articles/palcomms201545.pdf

Jensen, E. T. (2017). The Tallinn Manual 2.0: Highlights and Insights. *Georgetown Journal of International Law, 48*, 775-778.

Jervis, R. (1978). Cooperation Under the Security Dilemma. *World Politics, 30*(2), 167-214. Cambridge University Press.

Jigsaw Academy. (t.y.). What is Cyber Law? https://www.jigsawacademy.com/blogs/cyber-security/what-is-cyber-law/ (06.03.2023).

Johnson, C. (2019). Big Tech Surveillance Could Damage Democracy. University Author Recognition Bibliography: 2019. https://scholarworks.boisestate.edu/cgi/viewcontent.cgi?article=1007&context=uar_2019

Johnson, D. R., & Post, D. (1996). Law and Borders: The Rise of Law in Cyberspace. *Stanford Law Review, 48*(5), 1367-1402.

Johnson, D. R., & Post, D. (1998). The New 'Civic Virtue' of the Internet. *First Monday, 3*(1). https://firstmonday.org/article/view/569/490

Jorgensen, R. F. (2019). *Human Rights in the Age of Platforms*. Massachusetts Institute of Technology, The MIT Press.

Josukutty, C.A. (2020). Global Internet Governance: Implications for the South. *Indian Journal of Asian Affairs, 33*(1/2), 63–78.

Kalinauskas, M., & Barčys, M. (2013). Interaction between national governments and ICANN while administering the internet. *3*, 432-447.

Keller, B. (2015, Mayıs). Why We Need to Improve Global Cyber Governance. World Economic Forum. https://www.weforum.org/agenda/2015/05/why-we-need-to-improve-global-cyber-governance/

Kelsey, J. (2008). Hacking into International Humanitarian Law: The Principles of Distinction and Neutrality in the Age of Cyber Warfare. *Michigan Law Review, 106*, 1427-1451.

Keohane, R. O., & Nye, J. S. (1974). Transgovernmental Relations and International Organizations. *World Politics, 27*(1), 39–62.

Kesan, J. P., & Shah, R. C. (2005). Shaping Code. *Harvard Journal of Law & Technology, 18*(2), 319-399. http://jolt.law.harvard.edu/articles/pdf/v18/18HarvJLTech319.pdf

Ketenci, S. & Akın, G. (2009). ANYCAST ve IPV6'da ANYCAST Kullanımı. *İTÜ Bilgi İşlem Daire Başkanlığı*. https://web.itu.edu.tr/akingok/diger/anycast_ve_ipv6.pdf

Khanna, P. (2018). State Sovereignty and Self-Defence in Cyberspace. *BRICS Law Journal, 5*(4), 139-154.

Kissinger, H. (2016). *Dünya Düzeni*. (S. S. Gül, Çev.). Boyner Yayınları.

Klabbers, J., & Piiparinen, T. (2013). *Normative Pluralism and International Law: Exploring Global Governance*. Cambridge University Press.

Kleffner, J. K., & Dinniss, H. A. H. (2013). Keeping the Cyber Peace: International Legal Aspects of Cyber Activities in Peace Operations. *International Law Studies, 89*, 512-535.

Kleinwächer, W. (2009). The History of Internet Governance. İçinde C. Möller & A. Amouroux (Eds.), *Governing the Internet: Freedom and Regulation in the OSCE Region* (ss. 41-90). Vienna: Organization for Security and Cooperation in Europe.

Kleinwächter, W. (2013, Ocak 3). Internet Governance Outlook 2013: "Cold Internet War" or "Peaceful Internet Coexistence"? CircleID. https://circleid.com/posts/20130103_internet_governance_outlook_2013/

Kleinwächter, W. (2014). NETmundial: Watershed in Internet Policy Making? İçinde W. J. Drake & M. Price (Eds.), *Beyond NETmundial: The Roadmap for Institutional Improvements to the Global Internet Governance Ecosystem* (ss. 66-89). Internet Policy Observatory.

Kleinwächter, W. (2020, Ocak 7). Internet Governance Outlook 2020: The Next Generation of Players and Problems Is Coming. CircleID. https://circleid.com/posts/20200107_internet_governance_outlook_2020_next_generation_of_players/

Koenig-Archibugi, M. (2011). Global governance. İçinde J. Michie (Ed.), *The Handbook of Globalisation* (ss. 393-406). Edward Elgar Publishing Ltd.

Koh, H. H. (1997). Why Do Nations Obey International Law? [Review of The New Sovereignty: Compliance with International Regulatory Agreements; Fairness in International Law and Institutions, by A. Chayes, A. H. Chayes, & T. M. Franck]. *The Yale Law Journal, 106*(8), 2599–2659.

Koh, H. H. (2012). International Law in Cyberspace. *Harvard International Law Journal Online, 54*, 1-12.

Kolasi, K. (2017). Savaşın Değişen Niteliği ve Jus ad bellum ve Jus in bello'ya Etkisi. *İnsan Hakları Yıllığı, 35*, 1-29.

Komesar, N., Poiares Maduro, M., Wagner, W., Shaffer, G., & Bakardjieva-Engelbrekt, A. (Eds.). (2014). Understanding Global Governance: Institutional Choice and the Dynamics of Participation. *European University Institute*.

Koops, E. J., Lips, A. M. B., Prins, J. E. J., & Schellekens, M. H. M. (Eds.). (2006). *Starting Points for ICT Regulation; Deconstructing Prevalent Policy One-Liners*. (IT & Law; No. 9). TMC Asser Press.

Korhan, S. (2018). Siber Uzayda Aktör - Güç İlişkisi. *Cyberpolitik Journal, 2*(4), 75-104.

Koukiadis, D. (2015). The issue of legitimacy and accountability of non-state rulemaking. İçinde *Reconstituting Internet Normativity: The role of State, private actors, global online community in the production of legal norms* (ss. 71–99). London: Bloomsbury Publishing.

Kowack, G. (1997). Internet governance and the emergence of global civil society. *IEEE Communications Magazine, 35*(5), 52-57.

Koyuncu, A. Ç. (2015). İnsan Hakları. İçinde Ş. Kardaş & A. Balcı (Eds.), *Uluslararası İlişkilere Giriş* (ss. 499-509). İstanbul: Küre Yayınları.

Krol, E., & Hoffman, E. (1993, Mayıs). FYI on "What is the Internet?". Network Working Group, RFC 1462. https://www.rfc-editor.org/rfc/rfc1462

Kulaç, M. H. (2020, Haziran 30). About the global governance of cyberspace and Internet. Akademik Paradigma. https://www.akademikparadigma.com/about-the-global-governance-of-cyberspace-and-internet/

Kulesza, J. (2012). *International Internet Law*. Routledge Research in IT and E-Commerce Law. USA and Canada: Routledge.

Kumar, N., & Mowshowitz, A. (2008). Increasing internet access and freedoms with IGF participation. *IEEE Technology and Society Magazine, 27*(2), 33–36.

Kumar, S. (2012, Eylül 26). An Introduction to the Issues in Internet Governance. The Center for Internet Society. https://cis-india.org/internet-governance/issues-in-internet-governance

Kumari, S., Sharma, A., Khattar, V., Panwar, A., Baghel, S. S., & Khattar, V. (2022). A brief study on Cyber Crime, Laws and Ethics. İçinde *2022 International Conference on Fourth Industrial Revolution Based Technology and Practices (ICFIRTP)* (ss. 210-214). Uttarakhand, India.

Kuner, C. (2010). Data Protection Law and International Jurisdiction on the Internet (Part 1). *International Journal of Law and Information Technology, 18*(2), 176–193.

Kuner, C. (2013). *Transborder Data Flows and Data Privacy Law*. Oxford University Press.

Kurbalija, J. (2015). The WGIG and the taxonomy of Internet governance. İçinde W. J. Drake (Ed.), *The Working Group on Internet Governance: 10th Anniversary Reflections* (ss. 89-108). Roxana Bassi (APC).

Kurbalija, J. (2016). *An Introduction to Internet Governance (7th edition)*. DiploFoundation.

Kurbalija, J. (2017, Temmuz 24). Ten major trends in Internet governance (2017 mid-year review). DiploFoundation. https://www.diplomacy.edu/blog/ten-major-trends-in-internet-governance-2017-mid-year-review/

Kwiatkowska, M. (2016). E-voting: Leading Us towards Democratic Global Governance? İçinde M. Szkarłat & K. Mojska (Eds.), *New Technologies as a Factor of International Relations* (ss. 123-141). United Kingdom: Cambridge Scholars Publishing.

Lahmann, H., Otto, P., Djordjevic, V., & Maire, J. (2017). Who governs the internet? Players and fields of action. Friedrich-Ebert-Stiftung. https://library.fes.de/pdf-files/akademie/13910.pdf

Landau, S. (2013). Making sense from Snowden: What's significant in the NSA surveillance revelations. *IEEE Security & Privacy, 11*(4), 54-63.

Lantis, J., & Bloomberg, D. (2018). Changing the code? Norm contestation and US antipreneurism in cyberspace. *International Relations, 32*, 149-172.

Lardinois, F. (2012, Haziran 5). Is The U.N. Really Trying To Take Over The Internet? Nope. TechCrunch. https://techcrunch.com/2012/06/05/is-the-u-n-really-trying-to-take-over-the-internet-nope/?guccounter=1

Leiner, B. M., Cerf, V. G., Clark, D. D., Kahn, R. E., Kleinrock, L., Lynch, D. C., Postel, J., Roberts, L. G., & Wolff, S. S. (1997). The Past and Future History of the Internet. *Communications of the Association for Computing Machinery, 40*(2), 102-108.

Lessig, L. (1999a). *Code: And Other Laws of Cyberspace, Version 2.0*. New York: Basic Books.

Lessig, L. (1999b). Open Code and Open Societies: Values of Internet Governance. *Chicago-Kent Law Review, 74*, 1405-1422.

Lessig, L. (1999c). The Law of the Horse: What Cyberlaw Might Teach. *Harvard Law Review*. https://cyber.harvard.edu/works/lessig/LNC_Q_D2.PDF

Lessig, L. (2006). *Code: Version 2.0*. Basic Books, New York.

Levinson, N. S., & Marzouki, M. (2015). Internet Governance Institutionalization: Process and Trajectories. İçinde M. Rioux & K. Fontaine-Skronski (Eds.), *Global Governance Facing Structural Changes: New Institutional*

Trajectories for Digital and Transnational Capitalism (ss. 17-37). New York: Palgrave Macmillan.

Levinson, N.S., & Marzouki, M. (2016). International Organizations and Global Internet Governance: Interorganizational Architecture. İçinde F. Musiani, D.L. Cogburn, L. DeNardis, & N.S. Levinson (Eds.), *The Turn to Infrastructure in Internet Governance* (ss. 47–71). Palgrave Macmillan.

Lewis, J. A. (2013, Ekim). Internet Governance: Inevitable Transitions. *The Centre for International Governance Innovation, Internet Governance Papers, Paper No. 4*. https://www.cigionline.org/static/documents/no4.pdf

Lewis, J. A. (2015, Mayıs 11). Sino-Russian Cybersecurity Agreement 2015. Center for Strategic and International Studies. https://www.csis.org/blogs/strategic-technologies-blog/sino-russian-cybersecurity-agreement-2015

Lewis, J. A. (2020, Ekim 26). Digital Sovereignty in a Time of Conflict. *Observer Research Foundation*. https://www.orfonline.org/expert-speak/digital-sovereignty-in-a-time-of-conflict/

Li, C., Chen, J., Zhang, Z., Cheng, Y., Li, Z., & Li, Z. (2023). Evaluating the Quality of Service of the DNS Root Server From the Service Scope. *2023 International Conference on Mobile Internet, Cloud Computing and Information Security (MICCIS)*, Nanjing, China, ss. 173-177.

Li, R., Makhijani, K., & Dong, L. (2020). New IP: A Data Packet Framework to Evolve the Internet: Invited Paper. *2020 IEEE 21st International Conference on High Performance Switching and Routing (HPSR)*, Newark, NJ, USA.

Liaropoulos, A. (2017). Cyberspace Governance and State Sovereignty. İçinde G. C. Bitros & N. C. Kyriazis (Eds.), *Democracy and an Open-Economy World Order* (ss. 25-35). Springer.

Liddicoat, J. (2013, Mayıs). Internet Governance and ICANN: Reflections from Beijing. *Office of the Privacy Commissioner*. https://ourarchive.otago.ac.nz/bitstream/handle/10523/9030.

Lindsay, J. R. (2015). The Impact of China on Cybersecurity: Fiction and Friction. *International Security, 39*(3), 7–47.

Loja, M. (2018). International Agreements Between Nonstate Actors as a Source of International Law. *Proceedings of the ASIL Annual Meeting, 112,* 151–155.

Lopez-Claros, A., Dahl, A. L., & Groff, M. (2020). A History of Global Governance. İçinde *Global Governance and the Emergence of Global Institutions for the 21st Century* (ss. 30–64). Cambridge University Press.

Lucchi, N. (2014). Internet Content Governance and Human Rights. *Vanderbilt Journal of Entertainment and Technology Law, 16*(4), 809-856.

Lukitasari, D. (2013). Freedom of speech in Cyberspace: Human Rights Perspective. *International Journal of Business, Economics and Law, 2*(3), 78-81.

Lytvynenko, V., & Kantur, O. (2023). "Internet Balkanization" As an Instrument of Information Security of Authorıtarian States. *Bulletin of Taras Shevchenko National University of Kyiv. Public Administration, 17*(1), 28-37.

Mačák, K. (2017). From Cyber Norms to Cyber Rules: Re-Engaging States as Law-Makers. (2017) *30 Leiden Journal of International Law* 877.

Macdonald, T., & Macdonald, K. (2019). Towards a 'pluralist' world order: creative agency and legitimacy in global institutions. *European Journal of International Relations, 26*, 518-544.

Maciel, M., & de Souza, C. A. P. (2011, Eylül). Multi-stakeholder participation in internet governance: An analysis from a developing country, civil society perspective. APC 20.

Madakam, S., Ramaswamy, R., & Tripathi, S. (2015). Internet of Things (IoT): A Literature Review. *Journal of Computer and Communications, 3*, 164-173.

Magalhães, J. C. (2015). Critically Imagining Internet Governance: A Content Analysis of the Marco Civil da Internet Public Consultation. *MEDIA@LSE MSc Dissertation Series*.

Mahmood, M. (2017). *Does Digital Transformation of Government Lead to Enhanced Citizens' Trust and Confidence in Government?* Thesis of Doctor of Philosophy, Brunel University: United Kingdom.

Malcolm, J. (2008). *Multi-Stakeholder Governance and the Internet Governance Forum*. Terminus Press.

Mansell, R. (2004). Introduction - human rights and equity in cyberspace. İçinde Murray, A. D. & Klang, M. (Eds.), *Human Rights in the Digital Age* (ss. 1-10). London, UK: Glasshouse Books.

Marelli, M. (2023). The law and practice of international organizations' interactions with personal data protection domestic regulation: At the crossroads between

the international and domestic legal orders. *Computer Law & Security Review, 50*.

Masters, J. (2014, Nisan 23). What Is Internet Governance?. Council on Foreign Relations. https://www.cfr.org/backgrounder/what-internet-governance

Maurer, T. (2018). *Cyber Mercenaries: The State, Hackers, and Power*. Cambridge University Press.

Maurer, T. (2019). *Cyberspace and International Relations: Rising Powers, Proxies, and Norms*. Berlin: Dissertation. https://refubium.fu-berlin.de/bitstream/handle/fub188/26495/Maurer_Dissertation.pdf?isAllowed=y&sequence=3

McCarthy, K. (2014, Kasım 5). UN takeover of internet postponed indefinitely. *The Register*. https://www.theregister.com/2014/11/05/un_takeover_of_internet_postponed_indefinitely/

Melissen, J. (Ed.). (2005). The New Public Diplomacy: Between Theory and Practice. İçinde *The New Public Diplomacy: Soft Power in International Relations* (ss. 3-28). Palgrave Macmillan.

Mihr, A. (2014). Good Cyber Governance: The Human Rights and Multi-Stakeholder Approach. *Georgetown Journal of International Affairs, International Engagement on Cyber IV*, 24–34.

Mihr, A. (2016). Cyber Justice: Cyber Governance Through Human Rights and a Rule of Law in the Internet. *Us-China Law Review, 13*, 314-336.

Mijwil, M., Mohammad Aljanabi, & ChatGPT. (2023). Towards Artificial Intelligence-Based Cybersecurity: The Practices and ChatGPT Generated Ways to Combat Cybercrime. *Iraqi Journal For Computer Science and Mathematics, 4*(1), 65–70.

Milian, M. (2011, Aralık 22). Keepers of the Internet face their greatest challenges ever. *CNN*. http://edition.cnn.com/2011/12/22/tech/web/icann/

Ministry for Europe and Foreign Affairs. (2020, Mart). The challenges of Internet governance. https://www.diplomatie.gouv.fr/en/french-foreign-policy/digital-diplomacy/the-challenges-of-internet-governance/

Miyashita, H. (2016, Aralık). The "Right to be Forgotten" and Search Engine Liability. *Brussels Privacy Hub Working Paper, 2*(8), 1-15.

Mockapetris, P. (Ed.) (1983). "Request for Comments (RFC) 882: Domain Names – Concepts and Facilities". https://tools.ietf.org/pdf/rfc882.pdf

Mockapetris, P. V., & Dunlap, K. J. (1988). "Development of the Domain Name System". *Computer Communication Review, 18*(4), 1-11.

Morgan, S. (2020, Kasım 13). Cybercrime To Cost The World $10.5 Trillion Annually By 2025. Cybersecurity Ventures. https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021/

Mueller, M. (2002). *Ruling the Root: Internet Governance and the Taming of Cyberspace*. Cambridge, Mass.: MIT Press.

Mueller, M. L. (2007, Nisan). The Politics and Issues of Internet Governance. *Institute for Research and Debate on Governance, Coproduction of Public Action*, http://www.institut-gouvernance.org/en/analyse/fiche-analyse-265.html.

Mueller, M. L. (2010). *Networks and States: The Global Politics of Internet Governance*. Cambridge, Massachusetts; London, England: The MIT Press.

Mueller, M. L. (2012). ITU Phobia: Why WCIT was derailed. *Geopolitics of IG*, Aralık 18. https://www.internetgovernance.org/2012/12/18/itu-phobia-why-wcit-was-derailed/

Mueller, M. L. (2017). *Will the Internet Fragment? Sovereignty, Globalization and Cyberspace*. Cambridge: Polity Press.

Mueller, M. L., Mathiason, J., & Klein, H. (2007). The Internet and Global Governance: Principles and Norms for a New Regime. *Global Governance, 13*(2), 237-254.

Mueller, M., & Mathiason, J. (2006, Şubat 2). Building an Internet Governance Forum. Internet Governance Project. https://www.internetgovernance.org/wp-content/uploads/igp-forum.pdf

Mueller, M., Schmidt, A., & Kuerbis, B. (2013). Internet Security and Networked Governance in International Relations. *International Studies Review, 15*(1), 86–104.

Murphy, A. R. (Ed.). (2020). An Essay towards the Present and Future Peace of Europe (1693). İçinde *William Penn: Political Writings* (ss. 344–362). Cambridge University Press.

Murthy, C. S. R. (2014). India and Issues in Global Governance with Reference to Internet Governance. *International Studies, 51*(1-4), 1-15.

Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System. https://www.ussc.gov/sites/default/files/pdf/training/annual-national-training-seminar/2018/Emerging_Tech_Bitcoin_Crypto.pdf

Nanz, P., & Steffek, J. (2004). Global Governance, Participation and the Public Sphere. *Government and Opposition, 39*(2), 314-335.

Nardin, T. (2019). The Global Justice of Global Governance. İçinde S. Caney, P. Jones, & M. J. Smith (Eds.), *Global Justice: Theory and Practice* (2nd ed., ss. 224-239). Oxford University Press.

NATO Act. (2011, Nisan). Assured Access to the Global Commons. https://www.act.nato.int/images/stories/events/2010/gc/aagc_recommendations.pdf

NetChoice. (2014, Mart 16). U.S. giving up control of Internet address, domain name assignment. https://netchoice.org/media-press/dma-news-u-s-giving-control-internet-address-domain-name-assignment/

NETmundial. (2014, Nisan 14). NETmundial draft outcome document. https://document.netmundial.br/net-content/uploads/2014/04/NETmundial-draft-outcome-document_April_14.pdf

Newman, A. L. (2008). Building Transnational Civil Liberties: Transgovernmental Entrepreneurs and the European Data Privacy Directive. *International Organization, 62*.1, 103-130.

Nocetti, J. (2015). Contest and Conquest: Russia and Global Internet Governance. *International Affairs, 91*(1), 111-130.

Nonnecke, B. (2016). The transformative effects of multistakeholderism in Internet governance. *Telecommunications Policy, 40*, 343-352.

NTIA. (1998a). Statement of Policy on the Management of Internet Names and Addresses. United States Department of Commerce.

NTIA. (1998b). Memorandum of Understanding between the U.S. Department of Commerce and Internet Corporation for Assigned Names and Numbers. United States Department of Commerce.

NTIA. (1999). ICANN designated as "NewCo" for certain purposes under the Cooperative Agreement. United States Department of Commerce.

Nye, J. S. (2010, Mayıs). Cyber Power. Belfer Center for Science and International Affairs. https://www.belfercenter.org/sites/default/files/legacy/files/cyber-power.pdf

Nye, J. S. (2014, Mayıs). The Regime Complex for Managing Global Cyber Activities. *Global Commission on Internet Governance, Paper Series: No 1*. https://www.cigionline.org/sites/default/files/g

OECD. (t.y.). OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. https://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm (11.05.2021).

OHCHR. (2023, Mart 10). It May be Time to Reinforce Universal Access to the Internet as a Human Right, Not Just a Privilege, High Commissioner tells Human Rights Council. https://www.ohchr.org/en/news/2023/03/it-may-be-time-reinforce-universal-access-internet-human-right-not-just-privilege-high

Ølnes, S., Ubacht, J., & Janssen, M. (2017). Blockchain in government: Benefits and implications of distributed ledger technology for information sharing. *Government Information Quarterly: an international journal of information technology management, policies, and practices*, *34*(3), 355-364.

Olson, M. (1993). Dictatorship, Democracy, and Development. *American Political Science Review, 87*(3), 567–576.

Opper, M. H. (2011). WikiLeaks: Balancing First Amendment Rights with National Security. *31 Loy. L.A. Ent. L. Rev.*, 237–267.

Orji, U. J. (2018). *International Telecommunications Law and Policy*. Cambridge Scholars Publishing.

OSCE. (2015, Mayıs 4). Joint Declaration on Freedom of Expression and Responses to Conflict Situations. https://www.osce.org/files/f/documents/a/0/154846.pdf

OSCE. (2016, Temmuz 5). UN Human Rights Council resolution on protection of human rights on the Internet a milestone for free speech, says OSCE Representative. https://www.osce.org/fom/250656

Owens, W. A., Dam, K. W., & Lin, H. S. (2009). *Technology, policy, law, and ethics regarding U.S. acquisition and use of cyberattack capabilities*. The National Academies Press, Washington, DC.

Pai-zhang, C. (2010). The analysis of the common attacking methods of TCP/IP protocol. *Journal of Ningde Teachers' College*.

Parlak, B. & Doğan, K. C. (2019). *E-Yönetişim: Kavramsal/Kurumsal Çerçeve, Ülke İncelemeleri ve Türkiye'ye Yansımaları*. Beta Basım Yayın.

Patel, D.A. (2013). Digital Revolution and Good Governance-A New State in Making. *Bharati Law Review, 2*(1), 57-74.

Pawar, S. C., Mente, R. S., & Chendage, B. D. (2021, Ocak-Şubat). Cyber Crime, Cyber Space and Effects of Cyber Crime. *Int. J. Sci. Res. Comput. Sci. Eng. Inf. Technol, 7*(1), 210-214.

Pernice, I. (2018). Global cybersecurity governance: A constitutionalist analysis. *Global Constitutionalism, 7*, 112-141.

Peters, A. (2017). The refinement of international law: From fragmentation to regime interaction and politicization. *International Journal of Constitutional Law, 15*(3), 671–704.

Phys.Org. (2015, Mayıs 21). ICANN chief stepping down in early 2016. https://phys.org/news/2015-05-icann-chief-early.html

Pigatto, J., Datysgeld, M., & Silva, L. (2021). Internet governance is what global stakeholders make of it: a tripolar approach. *Revista Brasileira de Política Internacional, 64*(2), 1-19.

Pijović, N. (2021). The Cyberspace 'Great Game'. The Five Eyes, the Sino-Russian Bloc and the Growing Competition to Shape Global Cyberspace Norms. İçinde *2021 13th International Conference on Cyber Conflict (CyCon)* (ss. 215-231). Tallinn, Estonia.

Pizzaleo, A. G. (2011). Internet Governance: Analysis of technological and regulatory assumptions, of theoretical principles, of historical development and goals. *NEXA Center for Internet & Society*. https://nexa.polito.it/nexafiles/Internet%20Governance.pdf

Pogge, T. (2002). *World Poverty and Human Rights*. Polity Press.

Pogge, T. (2005). World Poverty and Human Rights. *Ethics & International Affairs, 19*(1), 1–7.

Pohle, J., Hösl, M., & Kniep, R. (2016). Analysing internet policy as a field of struggle. *Internet Policy Review, 5*(3), 1-21.

Post, D. (2014, Kasım 7). Stand Down! UN 'takeover of the Internet' postponed indefinitely. *The Washington Post*. https://www.washingtonpost.com/news/volokh-conspiracy/wp/2014/11/07/stand-down-un-takeover-of-the-internet-postponed-indefinitely/

Purcell, F., Vernous, G., Wakunuma, K., Akbar, S., & Finquelievich, S. (2006, Şubat). Role of Civil Society: Internet Governance and Developing Countries. DiploFoundation. https://archive1.diplomacy.edu/pool/fileInline.php?IDPool=129

Pushyamitra, M. (2022). ICANN: A Study of Its Working. *International Journal for Research in Applied Science & Engineering Technology (IJRASET), 10*(VIII).

PWC. (t.y.). What is a Digital Identity? https://www.pwc.com/it/it/publications/assets/docs/blockchain-and-digital-identity.pdf (03.07.2022).

Qian, X., & Zhang, J. (2020). Global Cyber Security Governance in the New Era: Status, Dilemma, and Development. *DEStech Transactions on Engineering and Technology Research*.

Radu, R. (2019). *Negotiating Internet Governance*. Oxford University Press.

Radu, R., Chenou, J.-M., & Weber, R. H. (2016). *The Evolution of Global Internet Governance: Principles and Policies in the Making*. Springer.

Ramirez, R., & Choucri, N. (2016). Improving Interdisciplinary Communication With Standardized Cyber Security Terminology: A Literature Review. *IEEE Access, 4*, 2216–2243.

Rao, S. S. (2005). Bridging digital divide: Efforts in India. *Telematics and Informatics, 22*(4), 361–375.

Rasevic, Z., Simović, M. N., & Simović, V. M. (2020, Aralık). Cyber Warfare and International Cyber Law: Whither? *Journal of Criminology and Criminal Law*, Belgrade.

Rawls, J. (1999). *The Law of Peoples*. Harvard University Press.

Raymond, M. (2012, Ekim 26). The Internet as a Global Commons? Centre for International Governance Innovation (CIGI). https://www.cigionline.org/publications/internet-global-commons/

Raymond, M. (2016a). Managing Decentralized Cyber Governance: The Responsibility to Troubleshoot. *Strategic Studies Quarterly, 10*(4), 123-149.

Raymond, M. (2016b). Engaging Security and Intelligence Practitioners in the Emerging Cyber Regime Complex. *The Cyber Defense Review*, 1(2), 81–94.

Raymond, M., & DeNardis, L. (2015). Multistakeholderism: anatomy of an inchoate global institution. *International Theory*, 7(3), 572–616.

Raymond, M., & Smith, G. (2013, Temmuz). Reimagining the Internet: The Need for a High-level Strategic Vision for Internet Governance. *Internet Governance Papers Paper No. 1*. https://www.cigionline.org/static/documents/no1_7.pdf

Razmetaeva, Y. (2020). The right to Be forgotten in the European perspective. *TalTech Journal of European Studies, 10*(1), 58-76.

Reardon, R., & Choucri, N. (2012). The Role of Cyberspace in International Relations: A View of the Literature. Paper prepared for the 2012 ISA Annual Convention, San Diego, CA.

Redeker, D. (2019, Kasım 29). The Contract for the Web: The newest manifestation of digital constitutionalism? *Völkerrechtsblog*. https://intr2dok.vifa-recht.de/receive/mir_mods_00007917

Rehman, J. (2010). *International Human Rights Law*. Pearson Education Limited.

Reidenberg, J. R. (2000). Resolving Conflicting International Data Privacy Rules in Cyberspace. *Stanford Law Review, 52*(5), 1315–1371.

Reinalda, B. (2009). *Routledge History of International Organizations: From 1815 to the present day*. Routledge.

Resnick, P. (2014, Haziran). On Consensus and Humming in the IETF. Internet Engineering Task Force (IETF), Request for Comments: 7282. https://tools.ietf.org/html/rfc7282

Rezayi, S., Balakrishnan, V., Arabnia, S., & Arabnia, H. (2018). Fake News and Cyberbullying in the Modern Era. *2018 International Conference on Computational Science and Computational Intelligence (CSCI)*, 7-12.

Rioux, M., & Fontaine-Skronski, K. (2015). Conceptualizing Institutional Changes in a World of Great Transformations: From the Old Telecommunications Regime to the New Global Internet Governance. İçinde M. Rioux & K. Fontaine-Skronski (Eds.), *Global Governance Facing Structural Changes: New Institutional Trajectories for Digital and Transnational Capitalism* (ss. 59-79). Palgrave Macmillan.

Roache, M. (2021, Nisan 1). How Russia Is Stepping Up Its Campaign to Control the Internet. *Time*. https://time.com/5951834/russia-control-internet/

Robinson, P. (1987). From TDF to international data services. *Telecommunications Policy, 11*(4), 369-376.

Rodriguez, K. (2023, Aralık 1). Latest Draft of UN Cybercrime Treaty Is A Big Step Backward. Electronic Frontier Foundation.

https://www.eff.org/deeplinks/2023/12/latest-draft-un-cybercrime-treaty-big-step-backward

Rojszczak, M. (2020). Does global scope guarantee effectiveness? Searching for a new legal standard for privacy protection in cyberspace. *Information & Communications Technology Law, 29*(1), 22-44. DOI: 10.1080/13600834.2020.1705033

Rose, G. (1998). Neoclassical Realism and Theories of Foreign Policy. *World Politics, 51*(1), 144-172. Cambridge University Press.

Rosenau, J. N. (1992). Citizenship in a Changing Global Order. İçinde J. N. Rosenau & E.-O. Czempiel (Eds.), *Governance without Government: Order and Change in World Politics* (ss. 272-294). Cambridge University Press.

Rosenau, J. N. (1997). Global Environmental Governance: Delicate Balances, Subtle Nuances, and Multiple Challenges. In M. Rolén, H. Sjöberg, & U. Svedin (Eds.), *International Governance on Environmental Issues* (Environment & Policy, Vol. 9, ss. 19–56). Springer.

Rosenau, J. N. (2000). Governance, Order, and Change in World Politics. İçinde J. N. Rosenau & E. O. Cziempiel (Eds.), *Governance without Government: Order and Change in World Politics* (ss. 1-29). Cambridge: Cambridge University Press.

Rosenau, J. N., & Czempiel, E.-O. (Eds.). (1992). *Governance without Government: Order and Change in World Politics*. Cambridge University Press.

Roy, A. K. (2012). Role of cyber law and its usefulness in Indian IT industry. İçinde *2012 1st International Conference on Recent Advances in Information Technology (RAIT)* (ss. 143-147). Dhanbad, India.

Rundle, M. C. (2005, Aralık 13). Beyond Internet Governance: The Emerging International Framework for Governing the Networked World. *Berkman Center Research Publication No. 2005-16*.

Sadowsky, G., Zambrano, R., & Dandjinou, P. (2004, Mart 15). Internet Governance: A Discussion Document: Prepared for the United Nations ICT Task Force, Global Internet Policy Initiatives. https://www.internetpolicy.net/governance/20040315paper.pdf

Sambuli, N. (2021, Nisan 22). Digital biases: The chimaera of equality and Access. *Observer Research Foundation*. https://www.orfonline.org/expert-speak/digital-biases-chimaera-equality-access/

San Juan, V., & Martin, A. (2019). Cyber Governance and the Financial Services Sector: The Role of Public–Private Partnerships. İçinde R. Ellis & V. Mohan (Eds.), *Rewired: Cybersecurity Governance* (ss. 97-115). John Wiley & Sons, Inc.

Saran, S., & Kaul, M. (2015, Haziran 24). The 'I' in the Internet Must Also Stand for India. *The Wire*. https://thewire.in/diplomacy/the-i-in-the-internet-must-also-stand-for-india

Sarı Ertem, H., & Korhan, S. (2019). Sosyal Medya ve Dış Politika İlişkisine Yakından Bakmak: Türkiye'de Üniversiteli Genç Yetişkinler Örneği. *Ekonomik ve Sosyal Araştırmalar Dergisi*, *15*(2), 215-233.

Schaake, M. (2012, Eylül 16). Stop Balkanizing the Internet. *HuffPost News*. https://www.huffpost.com/entry/stop-balkanizing-the-internet_b_1661164

Schmitt, M. N. (2011). Cyber Operations and the Jus in Bello: Key Issues. *Israel Yearbook on Human Rights, 41*, 113–135.

Schmitt, M. N. (Ed.). (2013). *Tallinn Manual on the International Law Applicable to Cyber Warfare*. Cambridge: Cambridge University Press.

Schofield, I. (2019, Mart). Does neo-realism present a credible account of global governance? *University of Portsmouth*. https://www.researchgate.net/publication/331498848_Does_neo-realism_present_a_credible_account_of_global_governance

Schrepel, T., & Buterin, V. (2020, Mayıs 18). Blockchain Code as Antitrust. *Berkeley Technology Law Journal*.

Schultz, T. (2007). Private Legal Systems: What Cyberspace Might Teach Legal Theorists. *Yale Journal of Law & Technology, 10*, 151-193.

Segura Serrano, A. (2019, Eylül 25). International Regulation of the Internet. Oxford Bibliographies. https://www.oxfordbibliographies.com/view/document/obo-9780199796953/obo-9780199796953-0194.xml

Segura-Serrano, A. (2006). Internet regulation and the role of international law. *Max Planck Yearbook of United Nations Law Online, 10*(1), 191-272.

Senges, M., & Horner, L. (2009, Ağustos). Values, principles and rights in internet governance. Global Partners & Associates. https://www.gp-digital.org/wp-content/uploads/pubs/values_principles_and_rights_internet_governance_senges_horner.pdf

SGI (t.y.). Data Analysis. https://www.sgi-network.org/2022/Data_Analysis (20.10.2023).

Shacklett, M. E., Novotny, A., & Gerwig, K. (2021). Definition: TCP/IP. *TechTarget*. https://www.techtarget.com/searchnetworking/definition/TCP-IP

Shahbaz, A. (2018, Ekim). The Rise of Digital Authoritarianism. *Freedom House, Freedom on the Net 2018*. https://freedomhouse.org/sites/default/files/FOTN_2018_Final.pdf

Shahbaz, A., & Funk, A. (2021). The Global Drive to Control Big Tech. *Freedom House*. https://freedomhouse.org/sites/default/files/2021-09/FOTN_2021_Complete_Booklet_09162021_FINAL_UPDATED.pdf

Shapira, I. (2011, Şubat 28). Obama administration joins critics of U.S. nonprofit group that oversees Internet. *The Washington Post*. https://www.washingtonpost.com/local/obama-administration-joins-critics-of-us-nonprofit-that-oversees-internet/2011/02/16/ABI2XzJ_story.html

Shapiro, A. L. (1998). The Disappearance of Cyberspace and the Rise of Code. Berkman Klein Center. https://cyber.harvard.edu/works/shapiro/Disappearance.pdf

Shaw, M. (t.y.). States in international law. Britannica. https://www.britannica.com/topic/international-law/The-responsibility-of-states (10.10.2022).

Shaw, R. (2001). Should the Internet be Regulated? Pro: Why the Internet Should be Regulated. *CESifo Forum, ifo Institute - Leibniz Institute for Economic Research at the University of Munich, 2*(04), 1-42.

Shcherbovich, A. A. (2017). Multistakeholder approach and human rights in Internet Governance. *Business Informatics*, *39*(1), 7–13.

Sheakh, T. H. (2012). Cyber Law: Provisions and Anticipation. *International Journal of Computer Applications, 53*(7), 10-12.

Shen, H. (2016). China and global internet governance: toward an alternative analytical framework. *Chinese Journal of Communication, 9*(3), 304-324.

Shin, J., & Yu, J. (2021). Targeted advertising and consumer inference. Marketing Science, 40(5), 900-922.

Sigholm, J. (2013). Non-State Actors in Cyberspace Operations. *Journal of Military Studies, 4*(1), 1–37.

Simović, M. N., Rašević, Ž., & Simović, V. M. (2020, Aralık). Cyber Warfare and International Cyber Law: Whither? *Journal of Criminal Law & Criminology, 58*(3), 23-37.

Simplilearn. (2023, Aralık 8). What is Cyber Law - Everything You Need to Know. https://www.simplilearn.com/what-is-cyber-law-article

Slack, C. (2016). Wired yet Disconnected: The Governance of International Cyber Relations. *Global Policy, 7*(1), 69-78.

Smith, J., & Wu, C. (2014, Şubat). The United States, China, and the Global Commons. Center for American Progress. https://cdn.americanprogress.org/wp-content/uploads/2014/02/China_GlobalCommonsPaper.pdf

Snyder, J., Komaitis, K., & Robachevsky, A. (2016, Mayıs 9). The History of IANA: An Extended Timeline with Citations and Commentary. Internet Society. https://www.internetsociety.org/ianatimeline/

Solana, J., & Lehmann, A. P. (2015, Nisan 27). Global cyber governance: preparing for new business risks. EsadeGeo Center For Global Economy and Geopolitics & Zurich Insurance Group. https://itemsweb.esade.edu/wi/web/risk-nexus-april-2015-global-cyber-governance.pdf

SomCert. (t.y.). Why CERT. https://somcert.gov.so/why-cert/ (20.10.2022).

Songip, A. R., Md Zaki, Z., Jusoff, K., Prebagaran, J., & Ng. Boon-Beng. (2013). Cyberspace: The Warfare Domain. *World Applied Sciences Journal, 21*(1), 01-07.

Souter, D. (2017, Şubat 6). Inside the Information Society: Who are the stakeholders? Association for Progressive Communications. https://www.apc.org/en/node/22481/

Souter, D. (2021, Kasım 2). Inside the Digital Society: Eight challenges for internet governance. Association for Progressive Communications (APC). https://www.apc.org/en/blog/inside-digital-society-eight-challenges-internet-governance

Spector, C. (2012). Who is the Author of the Abstract of Monsieur l'Abbé de Saint-Pierre's 'Plan for Perpetual Peace'? From Saint-Pierre to Rousseau. *History of European Ideas*.

SSAC. (t.y.). How does SSAC document its work? https://www.icann.org/groups/ssac (05.06.2021).

Statista (2024). *Global internet penetration rate as of January 2024, by region*. https://www.statista.com/statistics/269329/penetration-rate-of-the-internet-by-region/

Statista. (2022, Aralık 22). Digital competitiveness rankings by country worldwide 2022. https://www.statista.com/statistics/1042743/worldwide-digital-competitiveness-rankings-by-country/

Statista. (2023). Internet usage worldwide – Statistics & Facts. https://www.statista.com/topics/1145/internet-usage-worldwide/#topicOverview

Statista. (t.y.). Worldwide digital population 2024. https://www.statista.com/statistics/617136/digital-population-worldwide/ (09.01.2024).

Stone, G. R., Miller, J., Posner, R. A., & Schoenfeld, G. (2012). WikiLeaks and the First Amendment. *American Academy of Arts & Sciences, Spring 2012*. https://www.amacad.org/news/wikileaks-and-first-amendment

Sullivan, P. (t.y.). Computer Emergency Response Team (CERT). *TechTarget*. https://www.techtarget.com/whatis/definition/CERT-Computer-Emergency-Readiness-Team (21.02.2022).

Sunstein, C. R. (2001). *Republic.com*. Princeton, N.J.: Princeton University Press.

Surman, M. (2016, Şubat 8). The Internet is a Global Public Resource. Mozilla. https://blog.mozilla.org/en/mozilla/the-internet-is-a-global-public-resource/

Sutherland, E. (2018). Trends in Regulating the Global Digital Economy. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3216772

Swaine, M. D. (2013, Ekim). Chinese Views on Cybersecurity in Foreign Relations. *China Leadership Monitor, 42*. https://carnegieendowment.org/files/CLM42MS.pdf

Szeghalmi, V. (2018). Difficulties Regarding the Right to Be Forgotten in the Case Law of the Strasbourg Court. *Athens Journal of Law, 4*(3), 255-270.

Şeker, E. (2020, Eylül 22). The Impact of Current Challenges for International Cyber Law on the Future of Cybersecurity. Medium. https://medium.com/digital-diplomacy/the-impact-of-current-challenges-for-international-cyber-law-on-the-future-of-cybersecurity-e2686f098e4c

Take, I. (2012). Regulating the Internet Infrastructure: A Comparative Appraisal of the Legitimacy of ICANN, ITU, and the WSIS. *Regulation & Governance, 6*(4), 499-523.

Taneja, H., & Wu, A. X. (2014). Does the Great Firewall Really Isolate the Chinese? Integrating Access Blockage With Cultural Factors to Explain Web User Behavior. *The Information Society, 30*(5), 297-309.

Tarhan, K. (2016). Siber Uzayda Realist Teorinin Değerlendirilmesi. *Cyberpolitik Journal*, *1*(2), 292-311.

Taylor, E. (2021, Mart 16). A Breakthrough for U.N. Governance of Cyberspace. World Politics Review. https://www.worldpoliticsreview.com/articles/29496/a-breakthrough-for-global-cyber-governance

Taylor, E., & Hoffmann, S. (2019). EU–US Relations on Internet Governance, International Security Department. *Chatham House Research Paper*.

The Guardian. (2013, Haziran 11). Edward Snowden: the whistleblower behind the NSA surveillance revelations. https://www.theguardian.com/world/2013/jun/09/edward-snowden-nsa-whistleblower-surveillance

The White House. (2011, Mayıs). International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World. https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf

The White House. (2022, Nisan 28). Fact Sheet: United States and 60 Global Partners Launch Declaration for the Future of the Internet. https://www.whitehouse.gov/briefing-room/statements-releases/2022/04/28/fact-sheet-united-states-and-60-global-partners-launch-declaration-for-the-future-of-the-internet/

The White House. (t.y.). *A Framework for Global Electronic Commerce Executive Summary*. https://clintonwhitehouse4.archives.gov/WH/New/Commerce/summary.html (20.10.2023).

Thomson, J. E. (1992). Explaining the Regulation of Transnational Practices: A State-Building Approach. İçinde J. N. Rosenau & E.-O. Czempiel (Eds.),

Governance without Government: Order and Change in World Politics (ss. 195-218). Cambridge University Press.

Timberg, C. (2014, Mart 14). U.S. to relinquish remaining control over the Internet. *Washington Post*. https://www.washingtonpost.com/business/technology/us-to-relinquish-remaining-control-over-the-internet/2014/03/14/0c7472d0-abb5-11e3-adbc-888c8010c799_story.html

Tjahja, N., Meyer, T., & Shahin, J. (2021). What is civil society and who represents civil society at the IGF? An analysis of civil society typologies in internet governance. *Telecommunications Policy*, 45(6).

Tsagourias, N. (2015). The legal status of cyberspace. İçinde *Research Handbook on International Law and Cyberspace* (ss. 13-29). Edward Elgar Publishing.

Tucker, J. A., Guess, A., Barberá, P., Vaccari, C., Siegel, A., Sanovich, S., Stukal, D., & Nyhan, B. (2018, Mart). Social Media, Political Polarization, and Political Disinformation: A Review of the Scientific Literature. Hewlett Foundation.

U.S. Department of State. (2015). Internet Governance. https://2009-2017.state.gov/documents/organization/255010.pdf

U.S. Government Publishing Office. (2016). *Examining the Multistakeholder Plan for Transitioning the Internet Assigned Number Authority*. https://www.govinfo.gov/content/pkg/CHRG-114shrg23872/html/CHRG-114shrg23872.htm

UN News. (2023, Kasım 1). First Committee Approves New Resolution on Lethal Autonomous Weapons, as Speaker Warns 'An Algorithm Must Not Be in Full Control of Decisions Involving Killing'. https://press.un.org/en/2023/gadis3731.doc.htm

UN Report. (2004, Ağustos 23). *Report of the Secretary-General: The rule of law and transitional justice in conflict and post-conflict societies*. https://www.unhcr.org/media/rule-law-and-transitional-justice-conflict-and-post-conflict-societies-report-secretary

UN Society. (t.y.). Internet Governance Forum. https://www.eafit.edu.co/estudiantes/grupos-estudiantiles/unsociety/eafitmun/SiteAssets/Paginas/EAFITMUN/internet%20governance%20forum.pdf(09.12.2023).

UN Task Team. (2013, Ocak). Global governance and governance of the global commons in the global partnership for development beyond 2015.

https://www.un.org/en/development/desa/policy/untaskteam_undf/thinkpieces/24_thinkpiece_global_governance.pdf

UN. (1948, Aralık 10*). Universal Declaration of Human Rights*. https://www.un.org/en/about-us/universal-declaration-of-human-rights

UN. (2001, Ocak 8). *United Nations Convention against Transnational Organized Crime*. A/RES/55/25. https://www.unodc.org/pdf/crime/a_res_55/res5525e.pdf

UN. (2023, Ekim 17). Advancing Rule of Law, Justice for All through Technology Must Include Equal Internet Access, Human Rights Compliance, Sixth Committee Speakers Stress. Meetings Coverage: General Assembly Sixth Committee. https://press.un.org/en/2023/gal3694.doc.htm

UNCTAD. (2015). Mapping of international Internet public policy issues. Commission on Science and Technology for Development Eighteenth session. https://unctad.org/system/files/official-document/ecn162015crp2_en.pdf

UNCTAD. (2017, Ekim 23). Information Economy Report 2017: Digitalization, Trade and Development. https://unctad.org/system/files/official-document/ier2017_en.pdf

UNCTAD. (t.y.). Cybercrime Legislation Worldwide. https://unctad.org/page/cybercrime-legislation-worldwide (15.10.2022).

UNDP. (1997). *Governance for Sustainable Human Development: A Policy Document*. New York, NY: United Nations.

UNEP. (t.y.). IEG of the Global Commons. DELC: Division of Environmental Law and Conventions. https://cil.nus.edu.sg/wp-content/uploads/2015/12/Ses4-7.-UNEP-Division-of-Environmental-Law-and-Conventions-Global-Commons.pdf (15.10.2022).

UNESCO. (1984). IBI Second World Conference on Transborder Data Flows Policies. https://www.unesco.org/archives/multimedia/document-1800

UNESCO. (2015). Keystones to foster inclusive knowledge societies: access to information and knowledge, freedom of expression, privacy and ethics on a global internet. UNESDOC Digital Library.

UNGA. (2002, Ocak 31). *Resolution adopted by the General Assembly: World Summit on the Information Society*. https://www.itu.int/net/wsis/docs/background/resolutions/56_183_unga_2002.pdf

UNGA. (2006). *Fragmentation of international law: Difficulties arising from the diversification and expansion of international law: Report of the Study Group of the International Law Commission* (A/CN.4/L.702, 18 Temmuz 2006). https://legal.un.org/ilc/documentation/english/a_cn4_l702.pdf

UNGA. (2015, Ocak 13). *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.

UNGA. (2016, Şubat 1). *Resolution adopted by the General Assembly on 16 December 2015*. https://undocs.org/en/A/RES/70/125

UNGGE. (2013, Haziran 24). *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, A/68/98. https://digitallibrary.un.org/record/799853

UNGGE. (2015, Temmuz 22). *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, A/70/174. https://digitallibrary.un.org/record/799853?v=pdf

UNGGE. (2021). *Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security*, A/76/135. https://front.un-arm.org/wp-content/uploads/2021/08/A_76_135-2104030E-1.pdf

UNHRC. (2016, Haziran 27). The promotion, protection and enjoyment of human rights on the Internet. https://digitallibrary.un.org/record/845728

UNIDO. (2021, Ekim 14). Standards & Digital Transformation: Good Governance in a Digital Age. https://www.unido.org/sites/default/files/files/2021-10/standard_digital_transformation_onlıne_fınal.pdf

UNODA. (2013, Ekim). Seoul framework for the commitment to open and secure cyberspace. https://disarmament.unoda.org/wp-content/uploads/2019/10/

UNODA. (t.y.). Developments in the field of information and telecommunications in the context of international security. https://disarmament.unoda.org/ict-security/ (27.11.2022).

USSC. (2018). *Bitcoin Glossary: 2018 Annual National Seminar*. https://www.ussc.gov/sites/default/files/pdf/training/annual-national-training-seminar/2018-materials/emerging-tech_glossary-crypto.pdf

Ülgen, S. (2016). Governing Cyberspace: A Road Map for Transatlantic Leadership. Carnegie Endowment for International Peace. https://carnegieendowment.org/files/Sinan_Cyber_Final.pdf

Valeriano, B., & Maness, R. C. (2018). International relations theory and cybersecurity, in *Oxford Handbook Intern. Pol. Theo.* Oxford, 259–272.

van der Spuy, A. (2017). *What if we all governed the Internet?: Advancing multistakeholder participation in Internet governance*. UNESCO Publishing: Series on Internet Freedom.

van Eeten, M. J., & Mueller, M. (2013). Where is the governance in Internet governance? *New Media & Society, 15*(5), 720-736.

van Horenbeeck, M. (2018). Cybersecurity Culture, Norms and Values: Background paper to the IGF Best Practices Forum on Cybersecurity. IGF. https://www.intgovforum.org/en/system/files/filedepot/13/igf_2018_-_bpf_on_cybersecurity_background_paper_-_culture_norms_and_values_0.pdf

van Schewick, B. (2010). *Internet Architecture and Innovation*. Cambridge, MA: The MIT Press.

Vasist, P. N., Chatterjee, D., & Krishnan, S. (2023). The Polarizing Impact of Political Disinformation and Hate Speech: A Cross-country Configural Narrative. *Information Systems Frontiers.* Advance online publication. https://doi.org/10.1007/s10796-023-10390-w

Veale, M., & Brown, I. (2020). Cybersecurity. *Internet Policy Review, 9*(4), 1-22.

Vedder, A., Schroers, J., Ducuing, C., & Valcke, P. (Eds.). (2019). *Security and Law. Legal and Ethical Aspects of Public Security, Cyber Security and Critical Infrastructure Security*. Cambridge, Antwerp, Chicago: Intersentia.

Venables, A. (2021, Kasım). Modelling Cyberspace to Determine Cybersecurity Training Requirements. *Frontiers in Education, 6*. https://www.frontiersin.org/articles/10.3389/feduc.2021.768037/full

Verhelst, A., & Wouters, J. (2020). Filling Global Governance Gaps in Cybersecurity: International and European Legal Perspectives. *International Organisations Research Journal, 15*(2), 105-124.

Vigna, G. (2003). A Topological Characterization of TCP/IP Security. İçinde K. Araki, S. Gnesi, & D. Mandrioli (Eds.), *FME 2003: Formal Methods*. Lecture

Notes in Computer Science, vol 2805. Berlin, Heidelberg: Springer, ss. 914–939.

von Bernstorff, J. (2007). Non-State Actors in law-making and in the shaping of policy On the legality and legitimacy of NGO participation in international law. Konrad-Adenauer-Foundation's Conference on International Law. https://www.kas.de/c/document_library/get_file?uuid=4e2e1560-2408-8bfd-9f85-5dea3e38c200&groupId=252038

W3C. (t.y.a.). Facts About W3C. https://www.w3.org/Consortium/facts (17.05.2021).

W3C. (t.y.b.). W3C Mission. https://www.w3.org/Consortium/mission (17.05.2021).

W3C. (t.y.c.). People of the W3C. https://www.w3.org/People (11.05.2021).

W3C. (t.y.d.). Current Members. https://www.w3.org/Consortium/Member/List (17.05.2021).

W3C. (t.y.e.). Membership Fees. https://www.w3.org/Consortium/fees (17.05.2021).

Walker, S. (2021, Haziran 2). Contested domain: UN cybercrime resolution stumbles out of the gate. Global Initiative. https://globalinitiative.net/analysis/un-cybercrime-resolution/

Walzer, M. (1977). *Just and Unjust Wars: A Moral Argument with Historical Illustrations*. Basic Books.

Wang, A., Li, Y., Lin, L., Wu, Q., & Zhou, X. (2010). A study on the expansion and deployment model of root DNS servers. *The Journal of China Universities of Posts and Telecommunications*, 17(Supplement 2), 110-117.

Watt, E. (2017). *Cyberspace, Surveillance, Law and Privacy*. PhD Thesis, University of Westminster: London.

Weber, R. H. (2010). Internet of Things – New security and privacy challenges. *Computer Law & Security Review, 26*(1), 23-30.

Weber, R. H. (2011). The Right to Be Forgotten: More Than a Pandora's Box? *JIPITEC, 2*, 120-130.

Weiss, T. G. (2000). Governance, good governance and global governance: conceptual and actual challenges. *Third World Quarterly, 21*(5), 795.

Weiss, T. G., & Ozgercin, K. V. (2009). The Evolution of Global Governance: Theory and Practice. İçinde J. Wiener & R. A. Schrire (Eds.), *International Relations*. EOLSS Publications. https://www.eolss.net/sample-chapters/C14/E1-35-03-04.pdf

Welchman, L. (2015). Managing Chaos: Digital Governance by Design. *New York, Rosenfeld Media*.

Wendt, A. (1992). Anarchy Is What States Make of It: The Social Construction of Power Politics. *International Organization, 46*(2), 391-425.

Wendt, A. (1999). *Social Theory of International Politics*. Cambridge Studies in International Relations: 67.

Wessel, R. A., & Blockmans, S. (2014). *The Legal Status and Influence of Decisions of International Organizations and other Bodies in the European Union*. European Legal Studies: Research Papers in Law. https://aei.pitt.edu/63289/1/researchpaper_1_2014_wessel_blockmans.pdf

WGIG Report. (2005, Haziran). *Report of the Working Group on Internet Governance*. https://www.wgig.org/docs/WGIGREPORT.pdf

WG-IMP Report. (2015). 'IGF Policy Options for Connecting the Next Billion': Draft Compilation. https://gobernanzadeinternet.co/apc-aa-files/1c0ec76a20bd91fdc9938d30b87da6c0/igf-policy-options-for-connecting-the-next-billion-compilation.pdf

Wigley, B., & Cary, N. (2018, Mart 2). The Future is Decentralised: Block Chains, Distributed Ledgers, & The Future of Sustainable Development. https://www.undp.org/sites/g/files/zskgke326/files/publications/The-Future-is-Decentralised.pdf

Wilkinson, I. (2023, Ağustos 2). What is the UN cybercrime treaty and why does it matter? *Chatham House*. https://www.chathamhouse.org/2023/08/what-un-cybercrime-treaty-and-why-does-it-matter

Wilson, R. R. (1953). *The International Law Standard in Treaties of the United States*. Harvard University Press.

World Bank. (2016). *World Development Report 2016: Digital Dividends*. https://www.worldbank.org/en/publication/wdr2016

World Conference on International Telecommunications (WCIT-12). (2012, Aralık 3-14). http://files.wcitleaks.org/public/S12-WCIT12-INF-0005!!MSW-E.pdf

Wroblewski, A. (2020, Ekim 1). What The .Org Domain Sale Would Mean For Nonprofits: Jacqueline Lipton And Rick Lane. *Arts Management & Technology Laboratory*. https://amt-lab.org/podcasts-interviews/2020/10/jacqueline-lipton-and-rick-lane-dot-org

WSIS. (2003, Aralık 12). Declaration of Principles Building the Information Society: a global challenge in the new Millennium. https://www.itu.int/net/wsis/docs/geneva/official/dop.html

WSIS. (t.y.). What was the Civil Society Bureau? https://www.itu.int/net/wsis/basic/faqs.asp (05.06.2021).

Xiaoju, Z. (2015). Dilemma and Solution of Global Governance of Cyber Space. *Law Review*. https://www.semanticscholar.org/paper/Dilemma-and-Solution-of-Global-Governance-of-Cyber-Xiaoju/a5ebac9073c04dc3f600d310621235a5e1ee7fc7

Yan, L. (2019). Global Cyberspace Governance: State Actors and the China-US Cyber Relationship. *CIR, 29*(2), 105-124.

Yıldız, S. (2002). İnternet Servis Sağlayıcılar ve Cezai Sorumlulukları. *SÜ İİBF Sosyal ve Ekonomik Araştırmalar Dergisi, 1*(3), 167–184.

Yli-Huumo, J., Ko, D., Choi, S., Park, S., & Smolander, K. (2016). Where Is Current Research on Blockchain Technology? – A Systematic Review. *PLoS ONE, 11*(10).

Yongping, G. (2023). The Past, Conundrums, and Future of International Cybersecurity Governance. *International Journal of Frontiers in Sociology, 5*(4), 61-65.

York, D. (2019, Nisan 7). Celebrating 50 Years of the RFCs That Define How the Internet Works. Internet Society. https://www.internetsociety.org/blog/2019/04/celebrating-50-years-of-the-rfcs-that-define-how-the-internet-works/

Zacher, M. W. (1992). The Decaying Pillars of the Westphalian Temple: Implications for International Order and Governance. İçinde J. N. Rosenau & E.-O. Czempiel (Eds.), *Governance without Government: Order and Change in World Politics* (ss. 58-101). Cambridge University Press.

Zangl, M. (2021). *Internet Governance and the Freedom of Speech: Analysis of Current Frameworks on Disinformation in the US and EU*. Master Thesis, Central European University: Vienna.

Zeleke, T. A. (2019). The Quandary of Cyber Governance in Ethiopia. *Journal of Public Policy and Administration, 3*(1), 1-7.

Zhang, C., Liu, J., & Chhachhar, A. R. (2020). A comparative study of the global internet governance system between China and the United States. *Indian Journal of Science and Technology, 13*(23), 2303-2310.

Zhang, D., Wang, G., Wang, X., Li, Z., & Li, W. (2018). Cyberspace Security for Future Internet. *Security and Communication Networks, 2018*.

Zhu, X., & Tang, J. (2023). The interplay between soft law and hard law and its implications for global marine fisheries governance: A case study of IUU fishing. *Aquaculture and Fisheries.*

Zimmermann, V., & Renaud, K.V. (2019). Moving from a 'human-as-problem' to a 'human-as-solution' cybersecurity mindset. *Int. J. Hum. Comput. Stud.*, 131, 169-187.

Zürn, M. (2018a). Contested Global Governance. *Global Policy, 9*(1), 138-145.

Zürn, M. (2018b). The Rise of the Global Governance System: A Historical-Institutionalist Account. İçinde *A Theory of Global Governance: Authority, Legitimacy, and Contestation*. Oxford University Press.