ANKARA HACI BAYRAM VELİ ÜNİVERSİTESİ
LİSANSÜSTÜ EĞİTİM ENSTİTÜSÜ

# BARIŞ ZAMANI SİBER ESPİYONAJIN MÜDAHALE ETMEME İLKESİ BAĞLAMINDA DEĞERLENDİRİLMESİ

**Ali UZUN**

**Tez Danışmanı**

**Doç. Dr. Ali İbrahim AKKUTAY**

**KAMU HUKUKU BİLİM DALI**

**MİLLETLERARASI HUKUK ANABİLİM DALI**

**KASIM - 2023**


ankara
İBM

# BARIŞ ZAMANI SİBER ESPİYONAJIN MÜDAHALE ETMEME İLKESİ BAĞLAMINDA DEĞERLENDİRİLMESİ

**Ali UZUN**

**YÜKSEK LİSANS TEZİ**
**KAMU HUKUKU BİLİM DALI**
**MİLLETLERARASI HUKUK ANABİLİM DALI**

**ANKARA HACI BAYRAM VELİ ÜNİVERSİTESİ**
**LİSANSÜSTÜ EĞİTİM ENSTİTÜSÜ**

**KASIM 2023**

## ETİK BEYAN

Ankara Hacı Bayram Veli Üniversitesi Tez Yazım Kurallarına uygun olarak hazırladığım bu tez çalışmasında; tez içinde sunduğum verileri, bilgileri ve dokümanları akademik ve etik kurallar çerçevesinde elde ettiğimi, tüm bilgi, belge, değerlendirme ve sonuçları bilimsel etikve ahlak kurallarına uygun olarak sunduğumu, tez çalışmasında yararlandığım eserlerin tümüne uygun atıfta bulunarak kaynak gösterdiğimi, kullanılan verilerde herhangi bir değişiklik yapmadığımı, bu tezde sunduğum çalışmanın özgün olduğunu, bildirir, aksi bir durumda aleyhime doğabilecek tüm hak kayıplarını kabullendiğimi beyan ederim.

Ali UZUN

22.11.2023

TEZ ONAY SAYFASI

Ankara Hacı Bayram Veli Üniversitesi Lisansüstü Eğitim Enstitüsü Kamu Hukuku Anabilim Dalı Kamu Hukuku Yüksek Lisans Programı öğrencisi Ali UZUN tarafından hazırlanan Barış Zamanı Siber Espiyonajın Müdahale Etmeme İlkesi Bağlamında Değerlendirilmesi başlıklı tez çalışması 22/11/ 2023 tarih ve 13.00 saatinde yapılan tez savunma sınavında aşağıdaki jüri tarafından OY BİRLİĞİ ile YÜKSEK LİSANS tezi olarak KABUL edilmiştir.

| | **Kabul** | **Ret** |
|---|---|---|
| **Başkan (Unvan/Ad-Soyad/Kurum):** Prof. Dr. Cavid ABDULLAHZADE | x | |
| **Üye (Unvan/Ad-Soyad/Kurum):** Doç. Dr. Ali İbrahim AKKUTAY | x | |
| **Üye (Unvan/Ad-Soyad/Kurum):** Dr. Öğretim Üyesi Ali Şahin KILIÇ | x | |

BARIŞ ZAMANI SİBER ESPİYONAJIN MÜDAHALE ETMEME İLKESİ BAĞLAMINDA DEĞERLENDİRİLMESİ

(Yüksek Lisans Tezi)

Ali UZUN

ANKARA HACI BAYRAM VELİ ÜNİVERSİTESİ
LİSANSÜSTÜ EĞİTİM ENSTİTÜSÜ
Kasım 2023

## ÖZET

Espiyonaj konusunda uluslararası hukuk belirsizliğini sürdürmektedir. Bu belirsizliğin siber espiyonaj için sürdürülebilmesi, dijital dönüşüm trendi ve siber alanın fiziksel alana tahakkümü nedeniyle mümkün değildir. Bu tez, siber espiyonajı uluslararası teamül hukukunun bir ilkesi olan müdahale etmeme ilkesi bağlamında değerlendirerek mezkûr belirsizliğin giderilmesine cüzi bir katkı sunmayı amaçlamaktadır. Bu doğrultuda siber espiyonaj, geleneksel espiyonaj üzerinden siber alan gözetilerek tanımlanmıştır. Geleneksel ve siber espiyonaj bağlamında uluslararası hukuk incelenmiştir. Dijitalleşmenin etkisi de dikkate alınarak, müdahale etmeme ilkesinin kapsamı araştırılarak siber espiyonajın müdahale etmeme ilkesini ihlal edip etmeyeceği değerlendirilmiştir.

Bilim Kodu : 51201
Anahtar Kelimeler : Espiyonaj, Siber Espiyonaj, Müdahale Etmeme İlkesi
Sayfa Adedi : 95
Tez Danışmanı : Doç. Dr. Ali İbrahim AKKUTAY

EVALUATING PEACETIME CYBER ESPIONAGE IN THE CONTEXT OF THE PRINCIPLE OF NON-INTERVENTION

(M.Sc. Thesis)

Ali UZUN

ANKARA HACI BAYRAM VELI UNIVERSITY
THE INSTITUTE OF GRADUATE STUDIES
November 2023

## ABSTRACT

International law on espionage remains uncertain. This uncertainty cannot be sustained for cyber espionage due to the trend of digital transformation and the domination of cyberspace over physical space. This thesis aims to make a small contribution to the elimination of this uncertainty by evaluating cyber espionage in the context of the principle of non-interference, a principle of customary international law. In this respect, cyber espionage is defined in terms of traditional espionage by considering cyberspace. International law is examined in the context of traditional and cyber espionage. Taking into account the impact of digitalization, the scope of the principle of non-interference is explored and it is evaluated whether cyber espionage violates the principle of non-interference.

Science Code : 51201
Key Words : Espionage, Cyber Espionage, The Principle of Non-intervention
Page Number : 95
Supervisor : Doç. Dr. Ali İbrahim AKKUTAY

## TEŞEKKÜR

Tezimin nihayete ermesinde rehberliğini esirgemeyen danışmanım Doç. Dr. Ali İbrahim Akkutay'a müteşekkirim. Israrlı desteği ile yüksek lisans eğitimimi tamamlamama teşvik eden sevgili eşim Rümeysa'ya minnettarım.

# İÇİNDEKİLER

**Sayfa**

ÖZET ..... iv
ABSTRACT ..... v
TEŞEKKÜR ..... vi
İÇİNDEKİLER ..... vii
SİMGELER VE KISALTMALAR ..... x
1. GİRİŞ ..... 1
2. GELENEKSEL VE SİBER ESPİYONAJIN TANIMI VE KAPSAMI ..... 3
2.1. İstihbaratın Bir Bileşeni: Espiyonaj ..... 3
2.2. Geleneksel Espiyonaj ..... 3
2.3. Geleneksel Espiyonajdan Siber Espiyonaja ..... 5
2.4. Siber Espiyonaj ..... 7
2.4.1. Siber Espiyonajın Motivasyonu ..... 8
2.4.2. Siber Espiyonajın Hedefleri ..... 9
2.4.3. Siber Espiyonaj Metotları ..... 10
2.4.4. Siber Sömürü Operasyonu Olarak Siber Espiyonaj ..... 11
2.5. Siber Alan ..... 12
2.5.1. Siber Alanın Katmanları ..... 13
2.5.2. Siber Alanda Ülkesel Egemenlik ..... 14
2.5.3. Siber Alanın Regülasyonu ..... 15
2.5.4. Regülasyon Yaklaşımları ..... 16
2.5.4.1. Doğu yaklaşımı ..... 17
2.5.4.2. Batı yaklaşımı ..... 18
2.5.5. Siber Alanın Küresel Ortak Alan (Global Commons) Niteliği ..... 19
2.5.6. Regülasyon Çalışmaları ..... 20

**Sayfa**

2.5.6.1. BM Antlaşması kapsamında mevcut durum ..... 22

2.5.6.2. Sektörel ve bölgesel düzenlemeler ..... 24

2.5.6.2.1. Uluslararası Telekomünikasyon Birliği ..... 24

2.5.6.2.2. İnternet Tahsisli Sayılar ve İsimler Kurumu ve İnternet Atanmış Numaralar Otoritesi ..... 25

3. ULUSLARARASI HUKUK VE ESPİYONAJ ..... 29

3.1. Meşruluk Sorununa Geleneksel Cevap Arayışı ..... 31

3.1.1. Espiyonajın Meşru Olduğu Argümanı ..... 31

3.1.1.1. Uluslararası teamül hukuku ..... 32

3.1.1.1.1. Devlet uygulamaları ..... 32

3.1.1.1.2. Opinio iuris ..... 34

3.1.1.2. Espiyonajın izin verilen bir devlet eylemi olduğuna ilişkin yaklaşımlar ..... 36

3.1.2. Espiyonajın Meşru Olmadığı Argümanı ..... 37

3.1.2.1. Uluslararası teamül hukuku ..... 39

3.1.2.1.1. Devlet uygulamaları ..... 39

3.1.2.1.2. Opinio iuris ..... 40

3.1.2.2. Espiyonajın izin verilmeyen bir devlet eylemi olduğuna ilişkin yaklaşımlar ..... 41

3.2. Siber Espiyonaj ile Yeni Yaklaşımlar ..... 44

3.2.1. Siber Espiyonaj ve Uluslararası Barış ve Güvenlik ..... 45

3.2.2. Siber Espiyonaj ve Kuvvet Kullanma Yasağı ..... 48

3.2.3. Siber Espiyonaj ve Ülkesel Egemenlik ..... 52

4. SİBER ALANDA MÜDAHALE ETMEME İLKESİ VE SİBER ESPİYONAJ .. 55

4.1. Genel Olarak Müdahale Etmeme İlkesi ..... 55

4.2. Müdahale Etmeme İlkesinin Kaynakları ..... 56

4.2.1. Uluslararası Antlaşmalar Hukuku ..... 57

**Sayfa**

4.2.2. Uluslararası Teamül Hukuku ..... 60

4.2.3. Uluslararası Adalet Divanı Kararları ..... 62

4.3. Müdahale Etmeme İlkesinin Mahiyeti ..... 64

4.4. Dijital Dönüşümün Müdahale Etmeme İlkesine Etkisi ..... 66

4.4.1. Siber Alanda Müdahale Etmeme İlkesinin Kabulü ..... 68

4.4.2. Siber Alanda Müdahale Etmeme İlkesinin Uygulanabilirliği ..... 69

4.4.2.1. Tallinn Kılavuzunda müdahale etmeme ilkesinin uygulanabilirliği ..... 69

4.4.2.2. Çalışma grubu faaliyetlerinde müdahale etmeme ilkesinin uygulanabilirliği ..... 71

4.5. Siber Espiyonaj ve Müdahale Etmeme İlkesi ..... 73

4.5.1. Siber Espiyonaj ve Egemenlik ..... 73

4.5.2. Siber Espiyonaj ve Zorlayıcılık ..... 74

5. SONUÇ ..... 77

KAYNAKÇA ..... 81

ÖZGEÇMİŞ ..... 95

## SİMGELER VE KISALTMALAR

Bu çalışmada kullanılmış kısaltmalar, açıklamaları ile aşağıda sunulmuştur.

| Kısaltmalar | Açıklamalar |
|---|---|
| **ADOT** | Amerika Devletleri Organizasyonu Tüzüğü |
| **ARPANET** | Advanced Research Projects Agency Network |
| **BM** | Birleşmiş Milletler |
| **BMDHS** | Birleşmiş Milletler Deniz Hukuku Sözleşmesi |
| **CIA** | Central Intelligence Agency |
| **DDOS** | Distributed Denial of Service |
| **DİHVS** | Diplomatik İlişkiler Hakkında Viyana Sözleşmesi |
| **GCHQ** | Government Communications Headquarters |
| **IANA** | Internet Assigned Numbers Authority |
| **IBM** | International Business Machines |
| **ICANN** | Internet Corporation for Assigned Names and Numbers |
| **IGF** | Internet Governance Forum |
| **ITU** | International Telecommunications Union |
| **İHAS** | İnsan Hakları Avrupa Sözleşmesi |
| **KİHVS** | Konsolosluk İlişkileri Hakkında Viyana Sözleşmesi |
| **KSHUS** | Kişisel ve Siyasal Haklar Uluslararası Sözleşmesi |
| **NATO** | Kuzey Atlantik Antlaşması Örgütü |
| **NSA** | National Security Agency |
| **OSINT** | Açık Kaynak İstihbaratı |
| **ÖMDS** | Özel Misyonlara Dair Sözleşme |
| **ŞİÖ** | Şanghay İşbirliği Örgütü |
| **TRIPS** | Agreement on Trade-Related Aspects of Intellectual Property Rights |

| | |
|---|---|
| **UKUSA** | United Kingdom and United States of America Agreement |
| **UNITAR** | United Nations Institute for Training and Research |
| **UNOSAT** | The United Nations Satellite Centre |
| **WCT** | World Intellectual Property Organızatıon Copyrıght Treaty |
| **WIPO** | World Intellectual Property Organızatıon |
| **WSIS** | World Summit on the Information Society |

# 1. GİRİŞ

Uluslararası ilişkilerin girift hale gelmesi ile haber almaya atfedilen önem artmıştır. Geleneksel espiyonajın ihtiva ettiği risk ve zorlukları barındırmayan siber espiyonaj, sağladığı yarar ve verimlilik ile istihbarat faaliyetlerinde öncelikli olarak tercih edilmektedir. Siber alanın fiziksel alanın ayrılmaz bir parçası haline gelişi, günlük rutinlerin ve devlet faaliyetlerin siber alana entegre oluşu ve hatta fiziksel alanda gerçekleşen bir kısım iş ve işlemlerin siber alana taşınarak fiziksel alanda yürütümüne son verilmesi siber alanın kapsamını ve espiyonajın hedefi olan veri hacmini süratle artırmaktadır. Bu nedenle siber espiyonaj, uluslararası barış ve güvenliği geleneksel espiyonaja kıyasla daha fazla tehdit etmektedir.

Siber alanda artan devlet faaliyetleri ve siber alanın mevcut ve gelecekteki durumu, siber alanda devlet eylemlerinin düzenlenmesini uluslararası toplumun bir ihtiyacı haline getirmiştir. İlk aşamada bu ihtiyacın siber alana özgü çok taraflı bir uluslararası sözleşme ile karşılanabileceği ileri sürülmüşse de yeterli katılımcı sağlanamamıştır. Bugünkü durumda devletler mevcut uluslararası hukuk kurallarının siber alana uygulanabilir olduğu konusunda uzlaşı sağlamışlardır. Ancak bu kuralların ne şekilde uygulanacağı belirsiz durumdadır.

Uluslararası teamül hukukunun parçası olan müdahale etmeme ilkesi, devletin egemenlik alanını herhangi bir zorlayıcılığa maruz kalmadan yönetmesi anlamına gelmektedir. Kuvvet kullanma boyutuna ulaşmayan ancak başka bir devletin egemenliğini hedef alan siber espiyonajın müdahale etmeme ilkesini ihlal edebileceği makul bir şüphedir. Nitekim siber espiyonaj, bir devlete ait olan veri üzerinde o devletin kararlarını ortadan kaldıran bir etkiye sahiptir. Bu bağlamda ilk bakışta siber espiyonaj müdahale niteliğindedir.

Bu çalışma ile barış zamanı siber espiyonaj müdahale etmeme ilkesi bağlamında değerlendirilerek, uluslararası hukukun mevcut bir ilkesinin siber alana uygulanabilirliği, ne şekilde uygulanabileceği ve siber espiyonajın müdahale etmeme ilkesini ihlal edip etmediği araştırılacaktır.

Bu tez üç bölümden oluşmaktadır. İlk bölümde barış zamanı geleneksel ve siber espiyonaj kavramlarının sınırları ve içeriği belirlenmeye çalışılmıştır. Bu doğrultuda geleneksel espiyonaj üzerinden siber espiyonajın tanımı ve çerçevesi çizilmiştir. Siber alan ve bu alana yönelik regülasyon çalışmaları incelenerek siber

espiyonajın gerçekleştiği alan tanıtılmıştır. İkinci bölümde ise espiyonajın uluslararası hukuka göre meşruiyeti araştırılmıştır. Espiyonajı düzenleyen bir sözleşmenin olmaması bu araştırmanın uluslararası teamül hukuku kapsamında ağırlıklı olarak yürütülmesine neden olmuştur. Üçüncü bölümde siber espiyonajın oluşturduğu soruna çözüm olarak müdahale etmeme ilkesi incelenmiştir. Müdahale etmeme ilkesinin kapsam ve mahiyeti tespit edilmeye çalışılmış, dijitalleşmenin ilkeye etkisi değerlendirilmiştir.

Akademik eserlerde espiyonaj, savaş ve barış zamanı şeklinde ikili bir ayrım yapılarak incelenmektedir. Bu tez kapsamında espiyonaj yalnızca barış zamanı bağlamında ele alınarak, uluslararası hukuka göre durumu incelenmiş ve müdahale etmeme ilkesi bağlamında değerlendirilmiştir. Müdahale etmeme ilkesinin ihlalinin devlet eylemleri ile gerçekleşebilmesi nedeniyle siber espiyonaj devlet eylemi olarak benimsenmiştir. Dolayısıyla siber alanda yer alan diğer aktörlerin siber espiyonaj faaliyeti ve siber espiyonajın atfedilebilirliği tartışılmamıştır.

Bu tez ile siber espiyonajın uluslararası barış ve güvenlik ortamına yönelik tehdidinin boyutu ve uluslararası hukukta espiyonaja yönelik değerlendirmeler araştırılarak siber espiyonajın müdahale etmeme ilkesi bağlamında değerlendirilmesine katkı sunmak amaçlanmaktadır.

## 2. GELENEKSEL VE SİBER ESPİYONAJIN TANIMI VE KAPSAMI

### 2.1. İstihbaratın Bir Bileşeni: Espiyonaj

Politika oluşturma veya karar verme süreçlerinde istihbaratın esas alındığı kabul edilmektedir[1]. Diğer bir ifadeyle politikacılar ve komutanlar işlerini yapabilmek için istihbarata ihtiyaç duymaktadırlar[2]. Bu yönüyle istihbarat elde etmeye yönelik çalışmalar, ilgilinin müttefik veya hasım olup olmadığı fark etmeksizin icra edilmektedir[3].

İstihbarat, bilgi toplama ve analiz olmak üzere iki alt başlığa bölünebilir[4]. İstihbarat çalışanları da görevlerini planlama, toplama, işleme ve yayma olarak tanımlamaktadır[5]. Espiyonaj, istihbaratın bir alt başlığı olan bilgi toplamaya karşılık gelmektedir[6]. Analiz ise espiyonaj kapsamında değildir[7].

### 2.2. Geleneksel Espiyonaj

Bir klişe olarak tarihin en eski meslekleri arasında sayılan[8] espiyonajın tanımı üzerinde bir konsensüs oluşmamış ancak casusluk faaliyeti olarak özü oluşmuştur[9]. Birleşik Krallık Ulusal Altyapının Korunması Merkezi ve iç güvenlik teşkilatına göre espiyonaj, kamuya açık olmayan bilgilerin insan ya da teknik araçlar kullanılarak elde edilmesidir[10]. Kuzey Atlantik Antlaşması Örgütü (NATO) terminolojisi espiyonajı, bilgi sahibi ülkenin kanunlarına göre yasaklı bilgiyi gizli yollarla edinerek istihbarat

---

[1] Pun, D. (2017). "Rethinking espionage in the modern era", *Chicago Journal of International Law,* 18(1), 357; McDougal, M. S., Lasswell, H. D., ve Reisman, W. M. (1972). "The intelligence function and world public order", *Temp. LQ,* 46, 365-366; Baker, C. D. (2003). "Tolerance of international espionage: a functional approach", *Am. U. Int'l L. Rev.,* 19, 1094; Demarest bu kabulü aksiyom olarak değerlendirmektedir. Demarest, G. B. (1996). "Espionage in International Law", *Denver Journal of International Law and Policy*, 24(2), 322.

[2] Warner, M. (2002). "Wanted: A definition of intelligence", *Studies in Intelligence*, 46(3), 17.

[3] Tondini, M. (2018). "Espionage and International Law in the Age of Permanent Competition", *Military Law and Law of War Review,* 57(1), 25.

[4] Radsan, A. (2007). "The Unresolved Equation of Espionage and International Law", *Michigan Journal of International Law,* 28(3), 599; Sulmasy, G., & Yoo, J. (2006). "Counterintuitive: Intelligence Operations and International Law", *Mich. J. Int'l L., 28*, 625. Literatürde bu ayrım farklılaşmakta; bilginin yayılması, görevlendirme gibi başlıklar eklenerek kategorize edilmektedir. McDougal vd., a.g.m., 1972, 366; Pun, a.g.m., 2017, 357-358.

[5] Demarest, a.g.m., 1996, 323.

[6] Pun, a.g.m., 2017, 357.

[7] Demarest, a.g.m., 1996, 323.

[8] Chesterman, S. (2005). "The spy who came in from the Cold War: Intelligence and International Law", *Mich. J. Int'l L.*, 27, 1072; Radsan, a.g.m., 2007, 596; Totic, M. (2022). "The Importance and Role of Espionage at the International Level", *International Journal of Economics and Law*, 12, 238.

[9] Tondini, a.g.m., 2018, 25.

[10] Centre for the Protection of National Infrastructure. (2021). Espionage. https://www.cpni.gov.uk/espionage; Security Service MI5. Counter-Espionage. https://www.mi5.gov.uk/counter-espionage.

amaçlı kullanımı olarak tanımlamaktadır[11]. Amerika Birleşik Devletleri (ABD), Birinci Dünya Savaşı'na katılmasının ardından kabul etmiş olduğu yasa ile espiyonajı düzenlemiştir[12]. Mezkûr yasa, detaylı hükümleri ile espiyonajı ABD'nin dış ilişkilerine, tarafsızlığına ve dış ticaretine müdahale niteliğinde değerlendirmiş; ulusal savunmaya ilişkin bilgi toplanmasını, bunların ABD'nin zararına veya başka uluslara avantaj sağlayacak şekilde kullanılmasının espiyonaj kapsamında olduğunu düzenlemiştir[13].

Literatürde sıklıkla atıf alan Demarest'in tanımına göre espiyonaj; bilgi toplamanın bilinçli bir aldatıcılık gayesiyle, devlet ya da bir organizasyon emri altında ve hedefin yetkilendirmediği insan tarafından icra edilmesidir[14]. 1907 Lahey Sözleşmesi her ne kadar savaş zamanına ilişkin kuralları ihtiva etse de yirmi dokuzuncu maddesinde yer alan casus düzenlenmesi[15] geleneksel espiyonaj anlayışına uygun kabul edilmiştir. Buna göre casus, kimliğini gizleyerek bilgi toplamalıdır, aksi halde bilginin gizlilik derecesinin ne olduğu fark etmeksizin espiyonajdan bahsedilemeyecektir[16].

Toplanan bilginin mahiyeti de espiyonaj değerlendirmesinde önemlidir. Kamuya açık kaynaklardan elde edilen bilgi, espiyonaj olarak değerlendirilemeyecektir[17]. Nitekim bilginin kamuya açılması, bilginin gizliliğine ilişkin tartışmaları anlamsız kılmaktadır. Yine diplomatik personel, askeri ateşe ya da diğer yurt dışı misyon görevlileri, görevlerinin bir parçası olarak bulundukları ülkeyle ilgili kamuya açık kaynaklardan bilgi toplamakta ve analiz etmektedir. Açık kaynak

[11] NATO Standardizasyon Ofisi. (2020). The Official NATO Terminology Database. https://nso.nato.int/natoterm/Web.mvc.
[12] U.S. Statutes at Large, Volume 40 (1917-1919), 65th Congress. 217. https://tile.loc.gov/storage-services/service/ll/llsl//llsl-c65/llsl-c65.pdf.
[13] Espionage Act of 1917. 15 June 1917. Section 1.
[14] Demarest, a.g.m., 1996, 325-326.
[15] Convention (IV) respecting the Laws and Customs of War on Land and its annex: Regulations concerning the Laws and Customs of War on Land. The Hague, 18 October 1907. Article 29. https://ihl-databases.icrc.org/applic/ihl/ihl.nsf/Article.xsp?action=openDocument&documentId=090BE405E194CECBC12563CD005167C8. Ayrıca mezkûr sözleşme hükümlerine göre savaş zamanı kimliğini gizlemeden bilgi toplama faaliyetinde bulanan şahıslar casus olarak değerlendirilmemiştir.
[16] Delupis, I. (1984). "Foreign Warships and Immunity for Espionage", *The American Journal of International Law*, 78(1), 62.
[17] Pun, a.g.m., 2017, 358.

istihbaratı (OSINT) olarak adlandırılan bu istihbarat türü hukuksal bir problem olarak değerlendirilmemektedir[18].

Espiyonajın tanımına ilişkin tartışmalarla birlikte gizli/örtülü operasyon/eylem (covert action) terimine değinilmesi kavramın sınırlarının çizilmesini kolaylaştıracaktır. Örtülü eylem[19] teriminin en net tanımı ABD hukukunda yer almaktadır. Konunun muhtevası gereği devletler tanım getirmekte ihtiyatlıdır. Örneğin Birleşik Krallık örtülü eylemi "diğer görevler" olarak nitelendirerek hususi bir tanım yapmamıştır[20]. ABD hukukunda yer alan tanıma göre örtülü eylem "…*Birleşik Devletler Hükümeti'nin rolünün açıkça görülmemesi veya alenen kabul edilmemesinin amaçlandığı, yurtdışındaki siyasi, ekonomik veya askeri koşulları etkilemeye yönelik bir faaliyet veya faaliyetler anlamına gelir…"*şeklinde tanımlanmıştır[21].

Örtülü eylem teriminde yer alan "örtülü" kelimesi, eylemden sorumlu devlet tarafından eylemin resmi olarak tanınmama durumunu ifade etmektedir[22]. Diğer bir ifade ile makul ölçüde inkâr edilebilir olması söz konusu eylemi örtülü kılmaktadır[23]. Eylem ise hedefi, amaca uygun şekilde etkilemek ya da zorlamaktır[24]. Bu kapsamda örtülü eylem, espiyonaj olarak değerlendirilemeyecektir[25]. Espiyonajdan daha fazla müdahaleci niteliğe sahip olan örtülü eylem, destek veya hazırlık olarak espiyonajdan faydalanabilecektir[26].

### 2.3. Geleneksel Espiyonajdan Siber Espiyonaja

Teknolojinin gelişmesi siber alanda bulunan veri hacmini ve çeşitliliğini artırarak değerli bir hedef haline getirmektedir[27]. Yine bu gelişim, neredeyse tüm fiziksel varlıklar içerisinde siber alan oluşturulmasını sağlamaktadır. Bu nedenle siber

[18] Chesterman, a.g.m., 2005, 1073.
[19] Detaylı bilgi ve örtülü eylemin uluslararası hukuka göre durumu hakkında bkz. Reisman, W. M., Reisman, W. M. R., William Michael, R., ve Baker, J. E. (1992*). Regulating covert action: practices, contexts, and policies of covert coercion abroad in international and American law*. Yale University Press.
[20] Intelligence Services Act 1994. Section 1. https://www.legislation.gov.uk/ukpga/1994/13/section/1.
[21] The National Security Act of 1947. Section 503(e). https://www.dni.gov/index.php/ic-legal-reference-book/national-security-act-of-1947.
[22] Perina, A. H. (2014). "Black Holes and Open Secrets: The Impact of Covert Action on International Law", *Colum. J. Transnat'l L.,* 53, 511-512.
[23] Senate. (1991). Report. No. 102–85, 43. https://www.intelligence.senate.gov/sites/default/files/publications/10285.pdf.
[24] Perina, a.g.m., 2014, 512; Tondini, a.g.m., 2018. 29.
[25] Radsan. a.g.m., 2007, 599.
[26] Tondini, a.g.m., 2018, 29.
[27] Pun, a.g.m., 2017, 355.

alana ilişkin endişeler ve buna paralel olarak bu alanın güvenliğine ilişkin yatırımlar artmaktadır. 2021 yılında yaşanan veri ihlallerinin maliyetine ilişkin International Business Machines (IBM) tarafından hazırlanan rapor[28] konunun maddi boyutunu ortaya koymaktadır. Buna göre 2020 yılında bir veri ihlalinin ortalama toplam maliyeti 3.86 milyon dolar olarak gerçekleşmiş, 2021 yılında ise 4.24 milyon dolara yükselmiştir. Bu maliyet; enerji, sağlık veya finans gibi bazı sektörlerde gerçekleşen ihlallerde daha yüksektir. Bu maliyetler karşısında devletlerin önlem alması kaçınılmazdır. Örneğin veri ihlallerinin sıkça gerçekleştiği ABD siber güvenlik için 2 milyar dolarlık bir yatırım bütçesi oluşturmuştur[29].

Diğer taraftan bu gelişim, geleneksel espiyonaj faaliyetlerinin ve insan kaynaklarının korunmasını zorlaştırmaktadır[30]. Teknolojinin günlük rutinlere nüfuzunu her geçen gün artırması (finansal aktiviteler, konum bilgileri, akıllı binalar ve şehirler vb. gelişmeler) geleneksel espiyonajın, hedef tarafından tespitini ve önleme imkânını artırmaktadır.

Geleneksel espiyonaj ile elde edilmesi umulan bilginin maliyeti ve riskleri karşısında siber espiyonaj, düşük maliyet ve risk barındırması[31] itibarıyla öncelikli olarak tercih edilebilir. Yine siber espiyonajın makul ölçüde inkâr edilebilirlik sağlaması ve kullanılan araçların çok yönlü donanımda olması[32] bilgi toplama faaliyetini etkili kılmaktadır.

Geleneksel espiyonaj ile aynı amacı paylaşan siber espiyonaj, espiyonajın başka bir biçimidir[33]. Siber espiyonajın geleneksel espiyonaja kıyasla az risk içermesi

---

[28] IBM. *Cost of a Data Breach Report 2021*. https://www.ibm.com/security/data-breach.

[29] The White House. (2021). FACT SHEET: Top 10 Programs in the Bipartisan Infrastructure Investment and Jobs Act That You May Not Have Heard About. https://www.whitehouse.gov/briefing-room/statements-releases/2021/08/03/fact-sheet-top-10-programs-in-the-bipartisan-infrastructure-investment-and-jobs-act-that-you-may-not-have-heard-about/.

[30] NBC News. (2021). Former CIA officer says traditional spying is 'dead' due to technology, internet. https://www.nbcnews.com/now/video/former-cia-officer-says-traditional-spying-is-dead-due-to-technology-internet-122990661534.

[31] Merritt, D., ve Mullins, B. (2011). *Identifying cyber espionage: Towards a synthesis approach*. Reading: Academic Conferences International Limited. https://www.proquest.com/conference-papers-proceedings/identifying-cyber-espionage-towards-synthesis/docview/1011054838/se-2?.

[32] Örneğin birçok ülkenin siyasi, ekonomik ve medya konumlarında yer alan hedeflerin bilgisayarlarına yerleşen Ghostnet, hedefin bilgisi olmadan dosya silebilmekte, klavye vuruşlarını kaydetmekte veya kameraları ve ses girişlerini aktif edebilme özelliklerine sahipti. Deibert, R. J., Rohozinski, R., Manchanda, A., Villeneuve, N., ve Walton, G. M. F. (2009). *Tracking GhostNet: investigating a cyber espionage network*. Munk Centre for International Studies, University of Toronto.

[33] Weissbrodt, D. (2013). "Cyber-conflict, cyber-crime, and cyber-espionage", *Minnesota Journal of International Law*, 22(2), 371; Totic, a.g.m., 2022, 238.

ve çok yarar sağlaması bu durumu değiştirmemektedir. Bu nedenle espiyonaj için geçerli olan devletlerin iç hukuk ve uluslararası hukuk kuralları, siber espiyonaj için de geçerli olacaktır.

Birinci Dünya Savaşı'nda Almanlar istihbarat toplamak için güvercinleri kullanırken, İkinci Dünya Savaşı'nda "Colossus" adlı programlanabilen ilk bilgisayar ile Almanya'nın şifreli yazışmaları çözümlenmiştir[34]. Teknolojide yaşanan gelişim ve dönüşüm, espiyonaj metodolojisini değiştirerek bilginin elde edilmesinde coğrafi limitlerin olmadığı, yakalanma riskini barındırmayan, hedef dilinin ve kültürünün engel teşkil etmediği siber espiyonaja altın çağını[35] yaşatmaktadır.

### 2.4. Siber Espiyonaj

Siber espiyonaj, geleneksel espiyonajın amacına siber teknoloji kullanılarak ulaşılmasıdır[36]. NATO mükemmeliyet merkezlerinden biri olan Siber Savunma Mükemmeliyet Merkezi'nin daveti üzerine Uluslararası Uzmanlar Grubu tarafından hazırlanan Siber Operasyonlara Uygulanabilir Uluslararası Hukuk Kuralları Hakkında Tallinn Kılavuzu 2.0'da (Tallinn Kılavuzu) barış zamanı siber espiyonaj *"siber yetenekler kullanılarak gizlice veya yanlış izlenim uyandırarak (under false pretences) bilgi toplamak ya da teşebbüs etmek"* olarak tanımlanmıştır[37]. Yine aynı kuralda, siber yeteneklerin elektronik ortamda iletilen veya saklanan verilerin gözetlenmesi, yakalanması ya da sızdırılması amacıyla kullanımının, örnek olarak sayıldığı vurgulanmak suretiyle, siber espiyonaj kapsamında olduğu belirtilmiştir. Farklı bir yönü de vurgulayan Avustralya Siber Güvenli Merkezi ise siber espiyonajı "*İstihbarat amacıyla bir hedefin bilgisayar sistemlerinden, bu sistemlere zarar vermeden gizlice bilgi toplamak için tasarlanmış kötü amaçlı faaliyet."* şeklinde tanımlamıştır.

Siber espiyonajda kullanılan teknik imkânlar, geleneksel espiyonaja göre daha uzun süreli faaliyet yürütülmesini ve daha çok veriye erişilmesini mümkün kılabilir. Örneğin ABD Personel Yönetim Ofisi, 2015 yılında uhdesinde bulunan federal devlet

[34] Wallace, D. A., McCarthy, A. H., ve Visger, M. (2018). "Peeling Back the Onion of Cyber Espionage after Tallinn 2.0.", *Md. L. Rev.*, 78(2), 211.
[35] Ziolkowski, K. (Ed.). (2013). *Peacetime regime for state activities in cyberspace: International law, international relations and diplomacy*. NATO Cooperative Cyber Defence Centre of Excellence, Tallinn. 425.
[36] Pun, a.g.m., 2017, 357.
[37] Schmitt, M. (2017). *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations (2nd ed.)*. Cambridge: Cambridge University Press. Kural 32, 168.

çalışanlarına ve bağlantılı kişilere ilişkin sosyal güvenlik numaraları da dâhil olmak üzere hassas bilgilerin yetkisiz kişilerce ele geçirildiği ve bu veri ihlalinin 21.5 milyon kişiyi etkilediğini duyurmuştur[38]. Söz konusu espiyonajda kullanılan zararlı yazılım (*malware*), Çin Halk Cumhuriyeti (Çin) destekli bilinmeyen bir grup tarafından muhtemelen 2012 yılında sistemlere yerleştirilmiş ve 30 Haziran 2015 tarihine kadar işlevini yerine getirmiştir[39]. Başka bir örnek olarak; Rusya'nın siber espiyonaj yoluyla ABD Demokratik Ulusal Komite'den elde ettiği bilgi ile ABD başkanlık seçimlerine müdahale ederek seçim sonucunu belirlediğine yönelik değerlendirmeler gösterilebilir[40].

### 2.4.1. Siber Espiyonajın Motivasyonu

Sowbug adlı siber casusluk örgütü Güney Amerika ve Güneydoğu Asya'da yer alan devlet kurumlarını hedeflemişlerdir[41]. Bu faaliyet, özellikle dış politikaya yönelik çalışan kurumlara ve spesifik belgelere yoğunlaşmıştır. Örneğin ilk aşamada 11 Mayıs 2015 sonrası değiştirilen belgeler hedeflenirken sonrasında başka tarih esaslı hedef belirlenmiştir. Ayrıca fark edilmemek için kurumların çalışma saati dışındaki saatlerde casusluk faaliyeti gerçekleştirilmiştir. Yine Rusya merkezli ve devlet destekli olduğu düşünülen Fancy Bear adlı grup Rus hükümetinin kullanabileceği askeri ve güvenlik bilgilerini hedeflemektedir[42]. Çin, özellikle ekonomik ve endüstriyel varlıkları hedef alarak birçok casusluk faaliyeti yürütmektedir[43]. Anılan casusluk faaliyetleri, münferit olmayıp aksine sıklıkla yaşanan ve sıradanlaşan[44] espiyonaj vakalarına örneklerdir. Tespit edilen vakalar dikkate alındığında espiyonaj; askeri, ekonomik veya politik motivasyon ile gerçekleştirilmektedir.

---

[38] Cybersecurity Resource Center. *What Happened.* https://www.opm.gov/cybersecurity/cybersecurity-incidents/.

[39] Office of Personnel Management data breach (2015). (2021, June 4). International cyber law: interactive toolkit, https://cyberlaw.ccdcoe.org/w/index.php?title=Office_of_Personnel_Management_data_breach_(2015)&oldid=2417.

[40] Lipton E., Sanger D. E. ve Shane S. (2016). "The Perfect Weapon: How Russian Cyberpower Invaded the U.S.", *The New York Times*. https://www.nytimes.com/2016/12/13/us/politics/russia-hack-election-dnc.html.

[41] Bangladesh Government's e-Government Computer Incident Response Team. Sowbug: targets South American and Southeast Asian governments [source: symantec]. https://www.cirt.gov.bd/sowbug-cyber-espionage-group-targets-south-american-and-southeast-asian-governments-source-symantec/.

[42] Mandiant. (2014). APT28: A Window into Russia's Cyber Espionage Operations?. https://www.mandiant.com/resources/blog/apt28-a-window-into-russias-cyber-espionage-operations.

[43] Natıonal Counterıntellıgence And Securıty Center. (2018).Foreign Economic Espionage in Cyberspace. https://www.dni.gov/files/NCSC/documents/news/20180724-economic-espionage-pub.pdf.

[44] Watt, E. (2017). *Cyberspace, Surveillance, Law and Privacy*. PhD thesis University of Westminster Law, 60.

Ekonomik amaç, sektörel düzeyde farklılık gösterebilme ihtimali saklı tutulmak kaydıyla, tespit edilen olayların %85'inden fazlasında esas durumdadır[45]. Bu tespit, olayların büyüklüğü değil; tespiti sayısal olarak mümkün olanlar arasından yapılmıştır. Yine siber alanın kolaylıkla ulaşılabilir oluşu bu alanda faaliyet gösteren aktör sayısını ve çeşitliliğini artırmaktadır. Siber espiyonaj olaylarının tespiti zorken bunların amaçlarının da tam olarak tespit edilmesi mümkün görünmemektedir. Ayrıca, hedefin zayıf olması veya ideolojik nedenlerle yürütülen faaliyet sonrasında ekonomik amaca dönüşebilmektedir.

### 2.4.2. Siber Espiyonajın Hedefleri

Verizon'un yayımlamış olduğu raporda tespit edilen veri ihlallerinin sektörel dağılımı gösterilmiştir[46]. Buna göre 2022 yılı için tespit edilen 5212 veri ihlalinin; 690'ı finans, 681'i hizmet, 571'i sağlık, 537'si kamu, 651'i belirlenemeyen ve kalanları ise diğer sektörlerde farklı yoğunlukta gerçekleşmiştir. Her veri ihlali siber espiyonaj yoluyla olmamakta, bir kısmı bu yolla gerçekleşmektedir[47].

Bölgesel olarak siber espiyonaj çoktan aza olmak üzere sırasıyla; Asya-Pasifik, Avrupa, Orta Doğu ve Afrika ve Kuzey Amerika'da görülmektedir[48]. Veri ihlali olarak bakıldığında ise Kuzey Amerika ilk sırada yer almaktadır.

Espiyonaj doğası itibarıyla gizlilik içinde yürütülmektedir. Dolayısıyla tespit edilmesini zorlaştıracak önlemler alınmaktadır. Bu bağlamda siber espiyonajın istatistiklere yansımayan kısmının bulunduğunun kabulü gerekir. Diğer taraftan devletler espiyonaj mağduriyetlerini saklama eğilimindedirler. Bu da espiyonaj hakkında isabetli bir istatiksel değerlendirme yapılmasına engel olmaktadır. Ancak son yıllarda yaşanan ihlalleri inceleyen çalışmalarda siber espiyonajın ağırlıklı olarak devlet kurumlarını hedef aldığını göstermektedir[49].

---

[45] Verizon. (2022a). 2022 Data Breach Investigations Report, 50. https://www.verizon.com/business/en-gb/resources/2022-data-breach-investigations-report-dbir.pdf.
[46] Verizon, a.g.e., 2022a, 50.
[47] Verizon. (2022b) 2020-2021 Cyber-Espionage Report, 11. https://www.verizon.com/business/resources/T69/reports/2020-2021-cyber-espionage-report.pdf.
[48] Verizon, a.g.e., 2022b, 10.
[49] Bendovschi, A. (2015). "Cyber-attacks–trends, patterns and security countermeasures", *Procedia Economics and Finance*, 28, 27-28.

### 2.4.3. Siber Espiyonaj Metotları

Siber espiyonaj aktörlerinin takip ettikleri sürecin sırasıyla; hedef tespiti, zafiyet araştırması, zafiyetten faydalanma, amaca yönelik eylem, veri toplama ve son olarak izlerin silinmesi aşamalarından oluştuğu varsayılabilir[50]. Ancak bu aşamaları birbirinden kesin çizgiler ile ayırmak her zaman mümkün olmayabilir. Hedefin niteliğine göre iç içe geçebilir ya da biri diğerinin önüne geçebilir. Uygulanmasına karar verilen yöntem, aşamaların sıralamasını belirlemektedir.

Siber espiyonaj ile ulaşılmak istenen amaca ağırlıklı olarak sosyal mühendislik, sistem veya ağa sızma ve zararlı yazılım yerleştirme yöntemleri kullanılarak erişildiği tespit edilmiştir[51]. Sosyal mühendislik, bilgiye yetkisiz erişimde insan etkileşiminin kullanılmasını açıklamaktadır[52]. Sistem veya ağa sızma ise hedefin güvenlik açıklarının kullanılması ile bilgiye yetkisiz erişimi tanımlamaktadır[53]. Zararlı yazılım yerleştirme, bilgiye yetkisiz erişimi sağlaması için üretilmiş programların kullanılmasıdır[54]. Sıklıkla kullanılan ve sosyal mühendisliğin bir formu olan yemleme/oltalama (phishing) olarak adlandırılan teknik bir başka yöntem olarak kullanılmaktadır. İki uç arasındaki iletişim trafiğini araya girerek ve trafiği kendi üstüne alarak tüm trafiğe hâkim olan yöntem ise ortadaki adam (man in the middle) olarak adlandırılmaktadır[55].

Diğer taraftan casusluk faaliyetini yürüten ile muhatap olan taraf arasındaki rekabet her iki tarafı yeni yöntemler ve önlemler geliştirmeye teşvik etmektedir[56]. Yoğun rekabet ortamında muhtelif motivasyonlara sahip olan bilgiye yetkisiz erişmek isteyen taraf, yöntemini tatbik ederken sadece dışardan değil içeriden de hedefe ulaşabilmektedir. Bilgi, yetkisiz erişmek isteyen kişiler tarafından kuşatılmış bir vaziyette korunmaya çalışılmaktadır.

---

[50] Kara, I. (2022). "Cyber-Espionage Malware Attacks Detection and Analysis: A Case Study", *Journal of Computer Information Systems*, 62(6), 1254; Rivera, R., Pazmiño, L., Becerra, F., & Barriga, J. (2022). "An Analysis of Cyber Espionage Process", In Developments and Advances in Defense and Security: Proceedings of MICRADS 2021, *Springer Singapore,* 4-5, 10.
[51] Verizon, a.g.e., 2022b, 4; Rivera, vd. a.g.m., 2022, 8
[52] Bendovschi, a.g.m., 2015, 25; Rivera, vd. a.g.m., 2022, 4.
[53] Verizon, a.g.e., 4.
[54] Bendovschi, a.g.m., 2015, 25.
[55] Bendovschi, a.g.m., 2015, 25.
[56] Kara, a.g.m., 2022, 1254.

### 2.4.4. Siber Sömürü Operasyonu Olarak Siber Espiyonaj

Uluslararası hukukun mevcut kurallarının siber alana uygulanabilir olduğu tartışmaları ekseninde siber alanda gerçekleşen operasyonlar, geleneksel kavramlar ile açıklanmaya veya tasnif edilmeye çalışılmaktadır. Kuvvet kullanma, silahlı çatışma veya silahlı saldırı kavramlarını siber operasyonlar çerçevesinde inceleyen birçok çalışma mevcuttur[57]. Siber operasyonların, aşina olunan ve kuralları belli olan kavramlar kapsamında ele alınması da devletler açısından pratiktir.

Siber alanda veya siber alan yoluyla siber kabiliyetlerin bir amacı gerçekleştirmek üzere tatbik edilmesi siber operasyon olarak tanımlanabilir[58]. Siber operasyonun, siber saldırı veya siber sömürü[59] olmak üzere iki şekilde gerçekleşebileceği kabul edilmektedir[60]. Siber saldırı, hedef aldığı sistemi veya bilgiyi; değiştirmeyi, bütünlüğünü bozmayı, güvenilemez veya kullanılamaz duruma getirmeyi amaçlamaktadır[61]. Siber sömürü ise hedef sistemde veya ağda yer alan bilgiyi ele geçirmek amacıyla genellikle gizli olarak yürütülen bir faaliyettir[62]. Siber saldırı, yıkıcı niteliği ile hedefi saldırıdan haberdar ederken; siber sömürü, hedefi rahatsız etmeyen ve dikkat çekmeyen[63] bir operasyon yürütür. Diğer taraftan hem siber saldırı hem de siber sömürü bir güvenlik açığına ihtiyaç duymaları ve bu zafiyeti kullanarak faaliyetlerini yürütebilmeleri cihetiyle benzerlik göstermektedirler[64]. Siber

[57] Örneğin bkz. Waxman, M. C. (2011). "Cyber-attacks and the use of force: Back to the future of article 2 (4)", *Yale J. Int'l L.*, 36.; Roscini, M. (2014). *Cyber operations and the use of force in international law*, Oxford University Press, USA; Schmitt, M. (2012). "Classification of cyber conflict", *Journal of conflict and security law*, 17(2).

[58] Literatürde ve bir kısım devletlerin iç hukukunda siber operasyon yerine bilgisayar ağı saldırısı (computer network attack [CNA]) veya siber saldırı (cyber intrusion) terimleri de kullanılmaktadır.

[59] Hedefin bilişim sistemlerinden veya ağlarından bilgi toplanması operasyonu olarak tanımlanan *Computer Network Exploitation* (CNE) ifadesine mukabil olarak siber sömürü ifadesi tercih edilmiştir.

[60] Lin, H. (2011). "Responding to Sub-Threshold Cyber Intrusions: A Fertile Topic for Research and Discussion", *Georgetown Journal of International Affairs*, 128; Wallace vd., a.g.m., 2018, 215; Buchan, R. (2015). "Cyber espionage and international law". *In Research Handbook on International Law and Cyberspace*. Cheltenham, UK: Edward Elgar Publishing, 168-169.

[61] Lin, a.g.m., 2011, 129; Goldsmith, J. (2011). "What is the government's strategy for the cyber-exploitation threat?", *Lawfare.* https://www.lawfareblog.com/what-governments-strategy-cyber-exploitation-threat.

[62] Lin, a.g.m., 2011, 129.

[63] Sander, B. (2019). "The Sound of Silence: International Law and the Governance of Peacetime Cyber Operations", *In 2019 11th International Conference on Cyber Conflict (CyCon),* Vol. 900, 364; Lin, a.g.m., 2011, 129-130.

[64] Lin, a.g.m., 2011, 129.

espiyonaj, bilgi toplama gayesi ile hareket eden[65] ve hedefin mevcut ve gelecekteki fonksiyonlarına etki etmeyen[66] bir siber sömürü operasyonudur[67].

Siber saldırı ve sömürünün birçok unsuru ile örneklendiği bir vaka Kanada'da yaşanmıştır[68]. Buna göre Karma ve Conti adlı fidye yazılımı kullanan iki grup "ProxyShell" zafiyetini kullanarak aynı sağlık kuruluşunun verilerine erişim sağlamışlardır. Karma adlı grup hedefin sağlık kuruluşu olması nedeniyle verileri ele geçirmekle yetinmiş, Conti ise verileri şifreleyerek erişilemez duruma getirmiştir.

### 2.5. Siber Alan

Siber alan terimi ilk olarak Amerikalı-Kanadalı yazar William Gibson tarafından 1982 yılında Omni adlı dergide yayımlanan bir hikâyede ve ardından 1984 yılında Neuromancer adlı kitabında kullanılmıştır[69]. Kavram her ne kadar 1982 yılında ilk kez kullanılmış olsa da temeli, 1960'lı yılların sonlarına doğru ABD Savunma Bakanlığı tarafından desteklenen İleri Araştırma Projeleri Ajans Ağına (Advanced Research Projects Agency Network - ARPANET) dayanmaktadır. Bilgisayarların iletişimini sağlamak amacıyla geliştirilen proje, iletişim devrimine evrilmiştir[70].

Literatürde siber alanın kapsamı ve tanımı üzerinde uzlaşı oluşmasa da birçok tanım mevcuttur. Tallinn Kılavuzu'na göre siber alan, bilgisayar ağları vasıtasıyla verilerin depolanabildiği, değiştirilebildiği veya takas edilebildiği fiziksel ve fiziksel olmayan parçalardan oluşan ortam/alandır[71]. ABD Savunma Bakanlığı Askeri ve İlişkili Terimler Sözlüğü, bilgi teknolojisi altyapılarının birbirine bağlı ağlarından ve yerleşik verilerden oluşan bilgi ortamı dahilinde global bir alan olarak siber alanı

[65] Sander, a.g.e., 2019, 370.
[66] Hathaway, O. A., Crootof, R., Levitz, P. ve Nix, H. (2012). "The law of cyber-attack", *Calif. L. Rev.*, 100, 829.
[67] Weissbrodt, a.g.m., 2013, 372. Diğer taraftan bir kısım araştırmalarda siber espiyonajın siber saldırı olarak kabul edilerek siber espiyonaj hedefi olan devlete espiyonaja karşı silahlı meşru müdafaa hakkı tanımak suretiyle caydırıcılık oluşturacağı savunulmaktadır. Todd, G. H. (2009). "Armed attack in cyberspace: deterring asymmetric warfare with an asymmetric definition", *AFL Rev.*, 64(1), 97-98.
[68] Gallagher, S. (2022). "Conti and karma actors attack healthcare provider at same time through proxyshell exploits", Sophos News. https://news.sophos.com/en-us/2022/02/28/conti-and-karma-actors-attack-healthcare-provider-at-same-time-through-proxyshell-exploits/.
[69] Bussell, J. (2013). "Cyberspace". Encyclopedia Britannica. https://www.britannica.com/topic/cyberspace.
[70] Defense Advanced Research Projects Agency. *ARPANET*. https://www.darpa.mil/about-us/timeline/arpanet.
[71] Schmitt, a.g.e., 2017, 564.

tanımlamıştır[72]. T.C. Ulaştırma ve Altyapı Bakanlığı tarafından hazırlanan Ulusal Siber Güvenlik Stratejisi ve Eylem Planı (2022-2023) ise siber alanı *"Doğrudan ya da dolaylı olarak internete, elektronik haberleşme ve bilgisayar ağlarına bağlı olan tüm sistem ve hizmetler"*[73] şeklinde tanımlamıştır.

Nihayetinde siber alanın, bilgi teknolojisi yapısı üzerine inşa edilmiş insan yapımı fiziksel ve teknik bileşenlerinin olduğu kavramsal ve küresel bir alan olduğu söylenebilir. Askerî açıdan ise siber alan; kara, deniz, hava ve uzaydan sonra savaşın beşinci alanı olarak kabul edilmektedir[74].

### 2.5.1. Siber Alanın Katmanları

Siber alan tek bir alan olarak ifade edilse de esasında birbiriyle ilişki içerisinde olan birçok katmandan oluşmaktadır. Soyut yapısı ve aynı zamanda somut bileşenlerinin oluşu bu alanın tarifini ve analizini zorlaştırmaktadır. Katmanlar halinde siber alanın incelenmesi bu alanın doğasını ve yapısını anlaşılır kılmaktadır.

Katmanların tasnifinde farklı yaklaşımlar bulunsa da araştırmacıların çoğunluğu tarafından benimsenmiş ya da küçük değişiklikler ile kabul görmüş bir model oluşmuştur. Buna göre siber alan dört katmana bölünerek incelenmiştir[75]. Bu katmanlar; fiziksel, mantıksal, bilgi ve insan olarak sıralanabilir.

Fiziksel katmanda siber alana hayat veren unsurlar yer almaktadır. Bilgisayarlar, sunucular, veri merkezleri, kablolar veya uydular gibi somut olup bilgi teknolojisine dair olan unsurlardır.

Siber alanın kökleri fiziksel katmanda olsa dahi siber alanın doğası mantıksal katmanda oluşmaktadır. Mantıksal katmanda siber alanın gücü ve sınırları

---

[72] Department Of Defense, *Dıctıonary Of Mılıtary And Assocıated Terms*. 60. https://apps.dtic.mil/sti/pdfs/AD1029823.pdf.

[73] T.C. Ulaştırma ve Altyapı Bakanlığı. *Ulusal Siber Güvenlik Stratejisi ve Eylem Planı (2022-2023).* https://hgm.uab.gov.tr/uploads/pages/siber-guvenlik/ulusal-siber-guvenlik-stratejisi-ep-2020-2023.pdf.

[74] Hall, C. H. (2011). Operational Art in the Fifth Domain, Joint Military Operations Department, 2. https://apps.dtic.mil/sti/pdfs/ADA546255.pdf.

[75] Clark, D. D. (2010). "Characterizing cyberspace: Past, present and future", MIT Political Science Department, 2-4; Choucri, N., & Clark, D. D. (2013). "Who controls cyberspace*?", Bulletin of the Atomic Scientists*, 69(5), 24; Askeri doktrin açısından siber arazi tasnifi için bkz. Raymond, D., Cross, T., Conti, G., & Nowatkowski, M. (2014). "Key terrain in cyberspace: Seeking the high ground", In 2014 6th International Conference On Cyber Conflict, IEEE.

belirlenmekte, siber alana şekil verilmektedir[76]. Bu katmanda internet yönetişimi, servisler veya uygulamalar bulunmaktadır.

Mantıksal katman bilgi ile işlevsel hale gelmektedir. Tüm bu sistem çoğunlukla bilgiyi oluşturma, yakalama, saklama, iletme veya işleme gibi amacı mantıksal katmanda belirlenmiş işlemleri yerine getirmek üzere çalışmaktadır. Bilgi katmanında fotoğraflar, videolar, konum bilgileri gibi internet ortamında görülen içerikler yer almaktadır.

Son katman olarak insan, yalnızca tüketici değil; nasıl kullanacağını seçerek siber alanı tanımlayan ve şekil verendir[77]. İnsanın bilgi katmanına katkısının şekli, mantıksal katmanın alacağı şekle de karar vermektedir.

### 2.5.2. Siber Alanda Ülkesel Egemenlik

Egemenlik, devletlerin kendi topraklarında ve diğer devletlerle olan ilişkilerinde sahip olduğu haklar ve yükümlülükler bütünüdür[78]. Egemenlikten kaynaklanan bir devlet hakkı[79] olan ülkesel egemenlik, devletlerin egemen eşitliği ilkesinin doğal bir sonucu[80] ve uluslararası ilişkilerin temelidir[81]. Devletin kendi topraklarında tam ve münhasır yetkili olarak[82] örneğin topraklarına kimlerin giriş yapacağına karar vermesi ülkesel egemenliğin sonucudur.

Ülkesel egemenlik; kara topraklarında, iç sularda, karasularında, ulusal hava sahasında bulunan tüm teknik ve diğer fiziksel bileşenleri içermektedir[83]. Dolayısıyla, siber altyapı ve bu alanlardaki siber faaliyetler üzerinde ilgili devlet ülkesel egemenlikten doğan yetkisini tatbik etme hakkına sahiptir. Ayrıca siber altyapı, ilgili devletin ülkesinde yer alsa da küresel bir yapının parçası olduğu gerekçesiyle ülkesel egemenlik kapsamında olmadığı anlamına gelmeyecektir[84]. Diğer taraftan bir bütün

[76] Clark, a.g.m., 2010, 2.
[77] Clark, a.g.m., 2010, 4.
[78] Individual Opinion By Judge Alvarez, Corfu Channel Case, 43.
[79] Island of Palmas Case (Netherlands v. USA) 4 April 1928, Reports of International Arbitral Awards, Volume II, 838.
[80] Ziolkowski, a.g.e., 2013, 162.
[81] Corfu Channel Case (United Kingdom v. Albania); Merits, International Court of Justice (ICJ), 9 April 1949, 35.
[82] von Heinegg, W. H. (2012). "Legal implications of territorial sovereignty in cyberspace", *In 2012 4th International Conference on Cyber Conflict* (CYCON 2012), IEEE. 2; The Lotus Case. (France v Turkey). (1927). No. 10 (PCIJ), 18.
[83] von Heinegg, a.g.m., 2012, 5.
[84] Ziolkowski, a.g.e., 2013, 162.

olarak siber alan, bir devletin veya bir devlet grubunun egemenlik iddiasına konu edilemeyecek niteliktedir[85].

### 2.5.3. Siber Alanın Regülasyonu

1996'da Davos'ta gerçekleştirilen Dünya Ekonomik Forumunda dijital haklar aktivisti olan John Perry Barlow Siber Alan Bağımsızlık Bildirisini[86] kaleme almıştır. Bu bildiri, siber alanın regülasyonuna karşı çıkan romantik bir başkaldırıdır. Barlow, fiziksel dünyaya ilişkin olan kimlik, mülkiyet, ifade ve harekete ilişkin kavramların siber alanda bir geçerliliği olmadığı belirterek siber alanda zihin medeniyeti kuracağını bildirmiştir.

Barlow'un bildirisine yer verilen şüphelere benzer şüpheleri ifade eden akademik çalışmalarda, siber alanın fizibilitesinin devletlerin geleneksel uygulamalarına uygun olup olmadığı incelenmiş, özellikle yargı yetkisi, meşruiyet ve icra bağlamında sorgulanmıştır[87]. Yine bu alanın kurallarını kendi kendine üretmesi gerektiği vurgulanmıştır.

Siber alana yönelik özgürlükçü yaklaşımları eleştiren akademik çalışmalar, siber alanın regülasyona uygun olduğunu ancak alana özgü kuralların oluşabileceğini belirtmektedir[88]. Siber alan her ne kadar sanal bir alan olarak var olsa da sonuçları gerçek dünyayı etkilemektedir. Dolayısıyla sonuçlara katlanan tarafın siber alanı regülasyona tabi tutmasında hukuki menfaati bulunduğu ifade edilmektedir[89].

Teknoloji ve hukukun etkileşime girdiği bu alanın regülasyonunun dengeli ve düzenlenmek istenen alanın gereklerine uygun olması gerekmektedir[90]. Örneğin siber alanda mahremiyet veya anonimite, bir taraftan özgür toplumu desteklerken diğer taraftan bilgi üzerindeki kişilerin ve kamunun yararlarını sınırlamaktadır. Bu bağlamda siber alan bir denge içerisinde ele alınarak bazı konuların genel hatlarıyla

---

[85] von Heinegg, a.g.m., 2012, 3; Ziolkowski, a.g.e., 2013, 162-163.

[8686] Barlow, J. (2019-2020). "Declaration of the Independence of Cyberspace", *Duke Law & Technology Review*, 18, 5-7.

[87] Örneğin bkz. Burk, D. L. (1995). "Federalism in cyberspace", *Conn. L. Rev.*, 28, 1095; Hardy, I. T. (1993). "The proper legal regime for cyberspace", *U. Pitt. L. Rev.*, 55, 993; Johnson, D. R., & Post, D. (1996). "Law and borders: The rise of law in cyberspace", S*tanford Law Review*.

[88] Goldsmith, J. L. (1998). "Against Cyberanarchy*", The University of Chicago Law Review*, 65(4); Lessig, L. (2003). "Law Regulating Code Regulating Law", *Loyola University Chicago Law Journal*, 35(1).

[89] Goldsmith, a.g.m., 1998, 1200.

[90] Lessig, a.g.m., 2003, 3.

düzenlenmesi yeterli olabilecekken bazı konuların hiçbir düzenlemeye tabi tutulmaması yeterli olabilecektir.

### 2.5.4. Regülasyon Yaklaşımları

Devletlerin egemenliklerini fiziksel alanla birlikte siber alana da tatbik arzuları kaçınılmaz olarak bu alandaki faaliyetleri kurala bağlama çabalarını da tetiklemiştir. Siber alanın ve özellikle internetin yönetimine ilişkin tartışma 1990'lı yıllarda başlamıştır. Öncelikle siber alan, regülasyona tabi tutulabilir mi? sorusu tartışılmış; sonrasında ise bunun nasıl ve hangi ülkeler öncülüğünde olacağı tartışılmaktadır[91].

Devletler, siber alanın kendi iç işlerinin çok ötesinde olduğunu, bu alanın tek başına hareket eden tek bir ulus tarafından ele alınmasının mümkün olmadığını fark etmişlerdir[92]. Siber alanın dağıtık ve sınırsız yapısı bu alanın yönetişim yoluyla ele alınmasını zorunlu kılmaktadır. Örneğin X ülkesinden yönetilen bir botnet, A, B ve C ülkelerinde yer alan zombi bilgisayarlar vasıtasıyla herhangi bir ülkeye siber saldırı gerçekleştirmek amacıyla kullanılabilir. Bu halde bu saldırının sorumlularının bulunması veya saldırının engellenmesi ve zararlarının azaltılması birçok ülkenin iş birliğini gerektirmektedir.

Siber alanda yer alan aktörlerin zararlı faaliyetlerini az çaba ve masrafla kolay şekilde gerçekleştirebilir olmaları devletlerin güvenlik endişelerini artırmıştır. Nitekim son yıllarda gerçekleşen siber olaylar devletlerin endişelerindeki haklılıklarını güçlendirmiştir. Örneğin 2007 yılında Rusya Federasyonu (Rusya) ile Estonya Cumhuriyeti (Estonya) arasında yaşanan politik gerilim neticesinde Estonya, dağıtık hizmet reddi (DDOS - Distributed Denial of Service) saldırısına 22 gün boyunca maruz kalmıştır[93]. Bu süre boyunca devlet ve ticari internet sitelerine erişim kesintiye uğramıştır.

Siber alanın regülasyona uygun olup olmadığı tartışmaları teorik olarak sürerken devletler güvenlik ekseninde bu alana yönelik yaklaşımlarını ortaya koymaya başlamışlardır. Mezkûr yaklaşımlar doğu ve batı olmak üzere iki başlık altında

[91] Watt, a.g.e., 2017, 60.
[92] Mačák, K. (2017). "From cyber norms to cyber rules: re-engaging states as law-makers", *Leiden Journal of International Law*, 30(4), 879..
[93]Ottis, R. (2008). "Analysis of the 2007 cyber attacks against Estonia from the information warfare perspective", In Proceedings of the 7th European Conference on Information Warfare (p. 163).

toplanabilir. Rusya ve Çin gibi düşünen ülkeler doğu yaklaşımını oluştururken, ABD gibi düşünen ülkeler batı yaklaşımını oluşturmaktadır.

#### 2.5.4.1. Doğu yaklaşımı

Doğu yaklaşımı temelde ABD hegemonyasına ve rejimlerine yönelik olarak algıladıkları liberal düzene karşı olmalarının doğal bir sonucu olarak siber alanda da batı yaklaşımının karşısında yer almaktadır[94]. Bu itibarla doğu yaklaşımı esasında siber alanda egemenlik ve dolayısıyla bilginin dolaşımının sınırlandırılmasını savunmaktadır.

Siber alanda serbest dolaşımda olan bilginin; propaganda amaçlı kullanılması, internet medyasının ulusal güvenliğe tehdit oluşturacak şekilde çalıştırılması ve özellikle "twitter devrimlerine" neden olması doğu yaklaşımının endişelerine örnek olarak sayılabilir[95].

Doğu yaklaşımını benimseyen ülkeler endişelerini Birleşmiş Milletler (BM) Genel Kuruluna göndermiş oldukları mektupta vurgulamışlardır[96]. Burada özellikle internetle ilgili toplumsal sorunlar hakkında politika belirleme yetkisinin devletlerin egemenlik hakları kapsamında olduğu belirtilmiştir. Yine bilgi ve iletişim teknolojileri vasıtasıyla ayrılıkçı ve aşırılığa teşvik eden veya devletlerin ekonomik, sosyal ya da manevi istikrarına zarar veren faaliyetlerle mücadelede iş birliği çağrısında bulunulmuştur.

Çin, ulusal ölçekte güvenlik duvarı[97] inşa ederek siber alanı endişeleri doğrultusunda şekillendirmeye çalışmaktadır. Bu duvar ile Çin internet trafiğini ve içeriğini kontrol etmeyi amaçlamaktadır. Başka bir ifadeyle Çin, siber alanda egemenlik sınırlarını kontrol etmek istemektedir.

Netice itibariyle doğu yaklaşımı, siber alanda bilginin serbest dolaşımına karşı çıkmaktadır. Bu alanda egemenlik tesis ederek kontrol ve gözetimde bulunmak suretiyle iç işlerinin bir uzantısı kapsamında hareket etmeyi istemektedir.

---

[94] Broeders, D., L. Adamson and R. Creemers. (2019). "Coalition of the unwilling? Chinese and Russian perspectives on cyberspace", The Hague Program For Cyber Norms Policy Brief, 2.
[95] Broeders vd, a.g.e., 2019, 2-3.
[96] Letter dated 12 September 2011 from the Permanent Representatives of China, the Russian Federation, Tajikistan and Uzbekistan to the United Nations addressed to the Secretary-General (2011). A/66/359. https://digitallibrary.un.org/record/710973.
[97] Detaylı teknik bilgi için bkz. Ensafi, R., Winter, P., Mueen, A., & Crandall, J. R. (2015). "Analyzing the great firewall of china over space and time", *Proc. Priv. Enhancing Technol*., 2015(1).

### 2.5.4.2. Batı yaklaşımı

ABD'nin siber alanda güçlü ve batı yaklaşımının öncüsü olması şaşırtıcı bir durum değildir. Nitekim ABD 1960'lı yıllarda geliştirmiş olduğu projeler ile iletişim devrimine gidilen yola büyük katkılar sağlamıştır. Genel olarak ABD'nin siber alana ilişkin ortaya koyduğu duruş başta beş göz müttefikleri[98] olmak üzere birçok devleti temsil etmektedir[99].

Batı yaklaşımının esası, 2010 yılında dönemin ABD Dışişleri Bakanı olan Hillary Clinton'ın "İnternet Özgürlüğüne İlişkin Notlar" başlıklı açıklaması[100] ve aynı muhtevada olan 2011 yılında ABD tarafından yayımlanan Uluslararası Siber Alan Stratejisi[101] adlı belge ile ortaya konulmuştur.

Bilgi, hiçbir zaman siber alandaki kadar özgür olmamıştır[102]. Bilginin özgür olmasıyla birlikte bilgiye erişimin de elverişli hale gelmesi, gerçeklere ulaşmayı kolaylaştırmış ve insanları sorgulamaya yöneltmiştir. Böylece hükümetler daha denetlenebilir ve hesap sorulabilir hale gelmiştir. Bu bağlamda batı yaklaşımı, bilginin siber alanda serbest dolaşımını demokrasilerin işleyişine hizmet eden ve toplum bilincini ve farkındalığını artıran bir teknoloji olarak değerlendirmektedir. Bilginin siber alandaki dolaşımına müdahale edilmesi, otoriter rejimlerin menfaatlerini korumak üzere giriştiği bir faaliyet olarak değerlendirilmektedir.

Diğer taraftan siber alana ilişkin endişeler de dile getirilmektedir. Siber alandaki aktörlerin faaliyetleri, ulusal veya ulus ötesi sorunlara neden olmakla birlikte; uluslararası barış ve güvenliği tehlikeye atabilecek nitelikte olabilir. Dolandırıcılık, kimlik hırsızlığı, çocuk istismarı, fikri mülkiyet hırsızlığı ya da siber alana yönelik müdahaleler sorunlu faaliyetlere örnek olarak gösterilmektedir[103].

---

[98] Beş Göz ittifakı ikinci dünya savaşı sonunda ABD ve İngiltere öncülüğünde kurulan sonrasında Avustralya, Kanada ve Yeni Zelanda devletlerinin katıldığı bir istihbarat ittifakıdır. Sinyal istihbaratı konusunda işbirliği üzerine kuruludur. Bu ittifakın çok sayıda istihbarat ittifakları ve devletler ile işbirliği mevcuttur. Detaylı bilgi için bkz. Pfluke, C. (2019). "A history of the five eyes alliance: possibility for reform and additions: a history of the five eyes alliance: possibility for reform and additions", *Comparative Strategy*, 38(4).

[99] Watt, a.g.e., 2017, 67.

[100] Rodham Clinton, H. (2010). Remarks on Internet Freedom. US Department of State. https://2009-2017.state.gov/secretary/20092013clinton/rm/2010/01/135519.htm.

[101] US White House. (2011). International Strategy for Cyberspace. Prosperity, Security and Openness in a Networked Wold. https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf.

[102] Rodham Clinton, a.g.e., 2010.

[103] US White House, a.g.e., 2011, 4.

Batı yaklaşımı siber alan politikasını; temel özgürlükler, mahremiyet ve serbest bilgi akışının biri diğerinin önüne geçmeden ve denge içerisinde korunması olarak açıklamaktadır[104]. Söylem olarak özgürlükçü bir tutum ortaya konulsa da tıpkı gerçek dünyada olduğu gibi siber alanda da hakların sınırları olduğu belirtilmektedir. Şiddete teşvik eden ifadeler ya da kamu güvenliğini tehdit eden faaliyetler özgürlüklerin sınırlarına örnek olarak sayılabilir.

Diğer taraftan fısıltı halinde konuşulan fakat gerçekleşen bazı sızıntılar ile doğruluğu teyit edilen siber alanda ABD tarafından yürütülen sınırları aşan gözetim (*surveillance*) faaliyetleri, belge ve beyanlar ile ortaya konulan siber alan politikasının pratikte geçerli olmadığını göstermektedir. 2013 yılında ABD Merkezi İstihbarat Teşkilatı (Central Intelligence Agency - CIA) çalışanı olan Edward Snowden tarafından ifşa edilen gizli devlet belgeleri ABD'nin Ulusal Güvenlik Ajansı (National Security Agency - NSA) aracılığı ile siber alanda gözetim faaliyeti yürüttüğünü ortaya koymuştur[105]. Buna göre Prism adlı gözetleme programı ile Google, Facebook ve Microsoft gibi büyük şirketlerin sunucularına girerek internet trafiğini gözetlemiştir.

### 2.5.5. Siber Alanın Küresel Ortak Alan (*Global Commons*) Niteliği

Küresel ortak alan herhangi bir devletin kontrolü altında bulunmayan ancak devletlerin, kurumların veya kişilerin kullanımına açık olan alanlardır[106]. Başka bir ifade ile bir ulusun yetki kapsamında olmayan ve bütün ulusların erişebildiği alanlardır. Bu alanların idaresi uluslararası sözleşmeler ile belirlenmektedir. Antarktika, 1959 tarihli Antarktika Antlaşması ile; açık denizler, 1982 tarihli Birleşmiş Milletler Deniz Hukuku Sözleşmesi ile dış uzay ve 1967 tarihli, Ay ve Diğer Gök Cisimleri Dâhil, Uzayın Keşif ve Kullanılmasında Devletlerin Faaliyetlerini Yöneten İlkeler Hakkında Anlaşma ile yönetişimi belirlemiştir.

Bu noktada bir alanın evrensel ortak alan olarak nitelendirilmesi için hususi bir antlaşmaya ihtiyaç olmadığını vurgulamak gerekir[107]. Nitekim evrensel ortak alan ilkesi, antlaşma ile bu niteliği vurgulanmamış alanlardan da yararlanılması durumunda

[104] US White House, a.g.e., 2011, 5.
[105] BBC. (2014). Edward Snowden: Leaks that exposed US spy programme. https://www.bbc.com/news/world-us-canada-23123964.
[106] Murphy, T. (2010). "Security Challenges in the 21st Century Global Commons", *Yale Journal of International Affairs*, 5(2), 30.
[107] Ziolkowski, a.g.e., 2013, 181.

uluslararası teamül hukukunun bir parçası olarak dikkate alınmaktadır[108]. Dolayısıyla siber alanın küresel ortak alan olarak nitelendirilmesinde, bir antlaşmaya konu olup olmamasının teorik açıdan önemi azdır.

Küresel ortak alanların yönetişimi ve kullanımında riayet edilmesi beklenen ortak kurallar mevcuttur. Bu alanlarda devletler, egemenlik iddia etmemeli ve birlikte yönetime rıza göstermelidir[109]. Yine bu alanlar insanlığın ve gelecek nesillerin faydası gözetilerek barışçıl amaçlar ile kullanılmalıdır.

Siber alanda egemenlik tesis edilmesinin taraftarı olan devletlerin teşebbüsleri göz önüne alındığında muhtelif devletlerin siber alanı küresel ortak alan olarak nitelemesinin[110] azınlık görüşü olarak kalması makuldür. Yine devletlerin ve diğer aktörlerin siber alandaki faaliyetlerinin, küresel ortak alanlarda beklenen kullanım amaçlarına uygun olmadığı da aşikârdır.

Diğer taraftan siber alanın niteliğinin küresel ortak alan olmaya uygunluğu siber alan katmanları üzerinden değerlendirilebilir. Fiziksel katman siber alanın gerçek dünyadaki altyapısını barındırmaktadır. Bu altyapının sahibi ağırlıklı olarak devletler, kurumlar, şirketler ya da gerçek kişilerdir. Altyapı üzerindeki mülkiyet ve dolayısıyla egemenlik, siber alana dâhil olma nedeniyle son bulmayacaktır. Mantıksal katmanda ise fikri mülkiyet hakları gündeme gelecektir. Bilgi katmanı ise bireye dair veriyi kullanması nedeniyle gizlilik, özel hayat veya kişisel verilerin korunması gibi birçok hukuksal sorunu gündeme getirecektir.

### 2.5.6. Regülasyon Çalışmaları

Doğu yaklaşımı olarak Çin ve Rusya'nın siber alanda egemenlik için düzenleme talepleri, devletlerin kendilerini hukuki olarak bağlayacak ifadelerden kaçınması nedeniyle karşılık bulmamıştır[111]. Devletlerin siber alanda yönetişime duyduğu ihtiyacın iptidai hali, Fransa'nın teklifi üzerine 1996 yılında Avrupa Birliği

[108] Wolfrum, R. (1983). "The principle of the common heritage of mankind", *Heidelberg Journal of International Law,* 43(2), 336.
[109] Wolfrum, a.g.m., 1983, 316-317.
[110] Public Safety Canada, National Cyber Security Strategy. 35. https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ntnl-cbr-scrt-strtg/ntnl-cbr-scrt-strtg-en.pdf. Burada siber alan evrensel ortak alan olarak tanımlanmıştır; Aynı yönde çalışmalar için bkz. USA Department Of Defence, Strategy for Homeland Defense and Civil Support, 12. https://apps.dtic.mil/sti/pdfs/ADA435357.pdf.
[111] Mačák, a.g.m., 2017, 877.

Bakanlar Konseyinin onayladığı İnternette Uluslararası İşbirliği Şartı[112] ile kendi göstermiştir. Yine siber alana ilişkin endişeleri dile getiren uluslararası mekanizmaları harekete geçirmek isteyen başkaca girişimler de olmuştur. 2011 yılında Çin ve Rusya öncülüğünde Şanghay İşbirliği Örgütü devletlerince hazırlanan "Bilgi güvenliği için uluslararası etik kurallar" başlıklı teklif[113] BM Genel Kuruluna sunularak BM nezdinde müzakere edilmesi çağrısında bulunulmuştur. Ancak devletler siber alan hakkında, 2013 yılına kadar uluslararası toplumu şamil uzlaşı sağlayamamıştır.

2013 yılında uluslararası hukukun siber alana uygulanabilir olduğuna dair uzmanlar grubunun bağlayıcı olmayan raporu[114] ile farklı yaklaşıma sahip olan devletlerin birbirlerine yakınsamaya başladıkları söylenebilir. Nitekim mezkûr raporda aralarında Rusya, Çin, Fransa Cumhuriyeti (Fransa) ve ABD'nin de bulunduğu 15 farklı devletin uzmanlarının imzası bulunmaktadır. Bu itibarla, uluslararası toplumun siber alana ilişkin ortak anlayışı bu raporla oluşmaya başlamıştır[115].

Siber alanda devletlerden, devlet destekli veya devlet dışı aktörlerden kaynaklanan mevcut ve istikbaldeki tehditlerin görmezden gelinemeyecek hale gelmesi[116] ve bu tehditlerin uluslararası toplumun genelini etkileyen boyutlarda olması söz konusu raporun hazırlanmasında etkili olmuştur. Rapor, bilgi ve iletişim teknolojileri ile değişen güvenlik tehditlerinin uluslararası güvenlik anlayışı üzerindeki değişimini vurgulamaktadır. Akabinde bir kısım öneriler getirmektedir[117]. Başlıca; devletleri siber alanda sorumlu eylemlerde bulunmaya, devletlerarası iş birliği ve güveni artırmaya ve kapasite geliştirmeye davet etmiştir.

2015 yılında uzmanlar grubu, yirmi devlet uzmanının katılımlarıyla 2013 ve 2010 yıllarında hazırlanan raporların dikkate alındığı Uluslararası Güvenlik

---

[112] Wu, T. S. (1996)." Cyberspace sovereignty--the Internet and the international system", *Harv. JL & Tech.*, 10, 660.
[113] A/66/359; 2015 yılında bu teklif revize edilerek tekrar BM Genel Kuruluna sunulmuştur. 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 (2015). A/69/723. https://digitallibrary.un.org/record/786846.
[114] Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security. (2013). A/68/98. https://digitallibrary.un.org/record/753055.
[115] Mačák, a.g.m., 2017, 879.
[116] A/68/98, 4.
[117] A/68/98, 7-10.

Bağlamında Bilgi ve Telekomünikasyon Alanındaki Gelişmelere İlişkin Hükümet Uzmanları Grubu Raporunu[118] hazırlamıştır. Raporda, 2011 yılında Rusya ve Çin öncülüğünde sunulan "Bilgi güvenliği için uluslararası etik kurallar" adlı teklifin dikkate alındığı belirtilmiştir.

Devletlerin siber alandaki eylemleri, BM Antlaşmasından kaynaklanan yükümlülüklere aykırı olmaması gerekmektedir[119]. Bu bağlamda, uluslararası hukukun siber alana nasıl uygulanacağına dair soruna ilk aşamada BM Antlaşması çerçeve kabul edilerek yanıt verilmiştir. Bununla birlikte devletlerin bilgi ve iletişim teknolojilerini kullanırken siber alanın; stabil, erişilebilir, güvenli, açık ve barışçıl bir ortam olarak sürdürülmesine katkı sağlaması vurgulanmıştır. Siber alanda devlet faaliyetlerine uluslararası hukukun uygulanabilirliğinin tetkikinde sayılan bu yükümlülüklerin esas olduğu tespit edilmiştir.

BM nezdindeki siber alana özgü gelişmeler bağlayıcı olmayan tavsiye niteliğindedir. Devletlerin uluslararası hukuka göre sorumluluk doğuracak ifade veya girişimlerden sakınması politik endişeler ya da kasıtlı bir strateji nedeniyle olabilir[120]. Devletlerin siber alandaki faaliyetlerini sınırlayan düzenlemelerin olmamasının siber alanın güvenli ve barışçıl ortamına yönelik riskleri artırdığı söylenebilir. Diğer taraftan 2015 yılında hazırlanan raporda devlet eylemlerine ilişkin bağlayıcı olmayan kuralların gönüllü uyum ile siber alana yönelik riskleri azaltabileceği ifade edilmiştir[121]. Bu tür kuralların; devletleri bir şey yapmaktan veya yapmamaktan menetmediği, uluslararası toplumun beklentilerini ortaya koyduğu ve toplumlara devlet faaliyetlerini izleme ve değerlendirme imkânı verdiği belirtilmiştir.

#### 2.5.6.1. BM Antlaşması kapsamında mevcut durum

BM nezdindeki çalışmalar sonucunda uluslararası hukukun siber alana uygulanabilir olduğu sonucuna ulaşılmıştır. Uluslararası hukukun siber alana özgü kurallarının bulunmaması siber faaliyetler için bir sınırlama olmadığı anlamına

[118] Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security. (2015). A/70/174. https://digitallibrary.un.org/record/799853.
[119] A/70/174, 12.
[120] Mačák, a.g.m., 2017, 881.
[121] A/70/174, 7.

gelmemektedir[122]. Siber alanın yapısına özgü kuralların geliştirilmesi gerekliliği uluslararası hukukun mevcut kurallarını geçersiz kılmamaktadır[123].

Uluslararası Adalet Divanının (Divan) nükleer silah tehdidi veya kullanımının meşruluğu üzerine vermiş olduğu danışma görüşünde, BM Antlaşmasının ilgili hükümlerinin ve silahlı çatışma hukukunun uygulanması için nükleer silahların mahiyeti ve kapasitesinin dikkate alınarak tatbik edileceği belirtilmiştir[124]. Burada ilk olarak BM Antlaşmasında nükleer silahların spesifik olarak yasaklanmamasının güç kullanma bağlamında değerlendirilmesine engel olmadığı tespit edilmiştir. Kullanılan silahın ne olduğu fark etmeksizin herhangi bir güç kullanımı durumunda BM Antlaşmasının ilgili kuralları geçerli olacaktır[125]. İkinci olarak ise uluslararası hukukun mevcut kurallarının nasıl uygulanacağına, uygulanacak alanın nitelikleri dikkate alınarak karar verilecektir.

Yine Divanının Nikaragua'da ve Nikaragua'ya Karşı Askeri Ve Paramiliter Faaliyetlere İlişkin Dava (Nikaragua davası) kapsamında vermiş olduğu kararda ölçü ve etki analizi sistemi ortaya konulmuştur[126]. Geleneksel olmayan aktivitelerin ölçeği ve etkileri dikkate alınarak geleneksel aktiviteler ile mukayese edildiğinde, geleneksel olmayan aktivitenin geleneksel olan ile aynı uluslararası hukuk kuralını ihlal edebileceği belirtilmiştir.

Divanının ortaya koymuş olduğu sistem siber alan için de geçerlidir[127]. Bu itibarla siber alan bağlamında BM antlaşması çerçevesinde değerlendirme yapılırken kullanılan araçtan ziyade oluşan sonuçların ölçeği ve etkisine itibar edilerek bir ihlalin mevcut olup olmadığı tespit edilebilecektir[128].

[122] Mačák, a.g.m., 2017, 883.
[123] US White House, a.g.e., 2011, 9.
[124] Legality of The Threat or Use of Nuclear Weapons, Advisory Opinion of 8 July 1996, 244. https://www.icj-cij.org/public/files/case-related/95/095-19960708-ADV-01-00-EN.pdf.
[125] Legality of The Threat or Use of Nuclear Weapons, 244.
[126] Case Concerning Military And Paramilitary Activities in and Against Nicaragua, Judgment Of 27 June 1986, 103-104. https://www.icj-cij.org/public/files/case-related/70/070-19860627-JUD-01-00-EN.pdf.
[127] Schmitt, a.g.e., 2017, 328.
[128] Schmitt, a.g.e., 2017, 328.

### 2.5.6.2. Sektörel ve bölgesel düzenlemeler

Devletlerin bağlayıcı kurallardan kaçınması ve siber alanın göreceli olarak yeni bir alan oluşu[129] siber faaliyetleri doğrudan düzenlemeye yönelik girişimleri başarısız kılmıştır. Ancak siber alanın genişlemesi ve birkaç devlet hâkimiyetinin hissedilir olmasıyla devletlerin ilgisi ve endişesi artmıştır[130]. Devletler siber alanı, bölgesel veya sektörel düzenlemeler ile hukuk zeminine taşımış ve yönetişime ortak olmuşlardır.

#### 2.5.6.2.1. Uluslararası Telekomünikasyon Birliği

Telekomünikasyonun sektörel olarak regülasyonu; 1865 tarihli Uluslararası Telgraf Sözleşmesi ile başlamış, bugünkü haline ise 1992 tarihli Uluslararası Telekomünikasyon Birliği'nin Kuruluşu ve Sözleşmesi[131] ile gelmiştir. Uluslararası Telekomünikasyon Birliği (International Telecommunications Union - ITU) BM'nin bilgi ve iletişim teknolojileri konusunda uzmanlaşmış kuruluşudur[132]. 193 üye ülke ile ITU; başta telefon, internet veya uydu olmak üzere iletişim ile ilgili standartları ve politikaları belirlemektedir. Başka bir ifade ile ITU, insanların birbirleriyle bağlantı kurmasına hizmet etmektedir[133].

BM Genel Kurulu, 2001 yılında ITU'nun iki aşamalı olarak düzenlemeyi öngördüğü Dünya Bilgi Toplumu Zirvesinin (World Summit on the Information Society - WSIS) ITU liderliğinde yapılmasını ve desteklenmesini onaylamıştır[134]. İlk aşama 10-12 Aralık 2003 tarihleri arasında Cenevre'de, ikinci aşama ise 16-18 Kasım 2005 tarihleri arasında Tunus'ta gerçekleştirilmiştir. Cenevre aşamasında bilgi toplumunun inşası için somut adımlar atılmak üzere politik beyanlar geliştirmek ve teşvik etmek amaçlanmıştır[135]. Tunus aşamasında ise ilk aşama ile ortaya konulan

---

[129] Schmitt, M. N., & Vihul, L. (2014). The Nature of İnternational Law Cyber Norms. Tallinn Papers, (5), 12.
[130] Watt, a.g.e., 2017, 87-88.
[131] Uluslararası Telekomünikasyon Birliği'ne esas sözleşmelerin tümü için bkz. https://www.itu.int/en/history/Pages/ConstitutionAndConvention.aspx.
[132] İTU. About International Telecommunication Union. https://www.itu.int/en/about/Pages/default.aspx.
[133] ITU. Our vision,. https://www.itu.int/en/about/Pages/vision.aspx.
[134] World Summit on the Information Society : resolution / adopted by the General Assembly, UN. General Assembly (56th sess.: 2001-2002). A/RES/56/183. https://digitallibrary.un.org/record/455403.
[135] Cenevre aşaması sonucunda Cenevre İlkeler Bildirgesi ve Cenevre Eylem Planı hazırlanmıştır. Arzulanan bilgi toplumu için konulan ilkeler ışığında eylem planı ile ilgililere görevler ve sorumluluklar verilmiştir. Declaration of Principles Building the Information Society: a global challenge in the new Millennium. WSIS-03/GENEVA/DOC/4-E. https://www.itu.int/net/wsis/docs/geneva/official/dop.html; Geneva Plan of Action, WSIS-03/GENEVA/DOC/0005. https://www.itu.int/net/wsis/docs/geneva/official/poa.html.

eylem planını uygulamaya koymak ve internetin yönetişimine ve finansmanına ilişkin sorunlarına çözüm ve uzlaşı sağlamak amaçlanmıştır[136]. BM Ekonomik ve Sosyal Konseyi, WSIS çıktılarını takip ve izleme usulüne dair aldığı kararda, Kalkınma için Bilim ve Teknoloji Komisyonunun çalışmaları çerçevesinde raporlama yapılacağını belirtmiştir[137]. Mezkûr rapor komisyonun yıllık raporu ile konsey tarafından BM Genel Kurulunun bilgisine sunulmaktadır.

WSIS günümüzde de düzenli olarak gerçekleştirilmektedir. Süreç içerisinde başkaca forumlar veya zirveler de gerçekleştirilerek paydaşların görüşlerini toplayarak fikir ayrılıklarına çözüm üretilmesine ve bilgi toplumunun gelişmesine katkı sağlamaktadır. WSIS çıktılarından olan ve 2006 yılından itibaren düzenli olarak gerçekleştirilen İnternet Yönetişim Forumu (Internet Governance Forum – IGF)[138] ile internet yönetişimine ilişkin sorunlar için paydaşlar arasında diyaloğu geliştirmek amaçlanmaktadır.

#### 2.5.6.2.2. İnternet Tahsisli Sayılar ve İsimler Kurumu ve İnternet Atanmış Numaralar Otoritesi

Paydaşlar arası diyaloğu geliştirme çabaları yönetişim düzeninde değişikliğe gitme ihtiyacını doğurmuştur. İnternetin yönetişim düzeninin çok paydaşlı yapıya uygun olmadığına dair devlet görüşleri İnternet Tahsisli Sayılar ve İsimler Kurumunu (Internet Corporation for Assigned Names and Numbers – ICANN) gündeme getirmiştir[139]. 1988 yılında kurulan ICANN eşsiz tanımlayıcılar (internet protokolü adres alanı tahsisi, protokol tanımlayıcı ataması, ülke kodu vs.) vasıtasıyla çalışan evrensel internet yapısının güvenli ve istikrarlı çalışmasına hizmet etmektedir[140]. Kuruluşundan çok kısa süre sonra ICANN ve ABD Ticaret Bakanlığı arasındaki

[136] Tunis Commitment. WSIS-05/TUNIS/DOC/7. https://www.itu.int/net/wsis/docs2/tunis/off/7.html; Tunis Agenda for the Information Society, WSIS-05/TUNIS/DOC/6 (rev. 1). https://www.itu.int/net/wsis/docs2/tunis/off/6rev1.html.
[137] Follow-up to the World Summit on the Information Society and review of the Commission on Science and Technology for Development, UN. Economic and Social Council (2006, substantive sess. : Geneva). E/RES/2006/46. https://www.un.org/en/ecosoc/docs/2006/resolution%202006-46.pdf.
[138] IGF. https://www.intgovforum.org/en.
[139] Watt, a.g.e., 2017, 89.
[140] ICANN. https://www.icann.org/get-started.

mutabakat[141] ve akabinde geçiş anlaşması[142] yürürlüğe konulmuştur. Buna göre, ABD Savunma Bakanlığı ile bir sözleşme kapsamında internet adreslerinin atanmasını yönetmek için 1983 yılında kurulan İnternet Atanmış Numaralar Otoritesi'nin (Internet Assigned Numbers Authority - IANA)[143] görevlerini ICANN denetiminde yerine getirmesi ve bunun ABD'nin onayı ve gözetimi kapsamında olması kararlaştırılmıştır. Böylece ABD internet üzerinde yerel olan politika belirleme yetkisini uluslararası zemine taşımıştır[144].

İnternetin yönetiminin önemli bir bölümü olan ICANN, internetin ilk tasarımına sahip olan ABD hegemonyasına karşı çıkan görüşler ve uluslararası toplumun beklentisi üzerine yapısal değişikliğe uğramıştır. IANA'nın fonksiyonunun ICANN uhdesinde yerine getirileceğine dair anlaşmanın 1 Ekim 2016 tarihinde sona ermesi ile çok paydaşlı internet yönetişimi mümkün hale gelmiştir.

Uluslararası kuruluşlar nezdinde birtakım gelişmeler de yaşanmıştır. Avrupa Konseyi, Budapeşte Konvansiyonu ve protokolleri[145] ile sanal ortamda işlenen suçlar konu edilmiş ve paydaşlar arası deneyim aktarımı amaçlanmıştır. Şanghay İşbirliği Örgütü (ŞİÖ), ŞİÖ Üye Devletleri Arasında Uluslararası Bilgi Güvenliğinin Sağlanmasında İşbirliği Anlaşması[146] ile siber savaşa, siber terörizme, siber suçlara ve başka devletlerin siber alandaki pozisyonlarını kullanarak üye devletlere yönelik faaliyetlerine karşı iş birliğini konu almıştır. Afrika Birliği, Siber Güvenlik ve Kişisel Verilerin Korunmasına İlişkin Afrika Birliği Sözleşmesi[147] ile siber alana ilişkin güvenlik ve hukuki çerçeve belirlenmiştir.

Siber alana ilişkin uluslararası hukukun tanımlanması ve geliştirilmesinde devletler farklı kamplarda yer alsa da netice itibarıyla uluslararası hukukun

[141] ICANN & DoC. (1998). Memorandum of understanding between the US Department of Commerce and Internet corporation for assigned names and numbers. https://www.icann.org/resources/unthemed-pages/icann-mou-1998-11-25-en.
[142] ICANN, USC/ICANN Transition Agreement. https://www.icann.org/resources/unthemed-pages/usc-icann-transition-2012-02-25-en
[143] ICANN. (2014). The IANA Functions in 180 Seconds (Video). Youtube. https://www.youtube.com/watch?v=D__mAX-2sXo.
[144] Watt, 93.
[145] Council Of Europe, The Budapest Convention (ETS No. 185) and its Protocols https://www.coe.int/en/web/cybercrime/the-budapest-convention.
[146] Agreement on Cooperation in Ensuring International Information Security between the Member States of the SCO. (2009). http://eng.sectsco.org/documents/.
[147] African Union Convention on Cyber Security and Personal Data Protection. (2014). https://au.int/sites/default/files/treaties/29560-treaty-0048_-_african_union_convention_on_cyber_security_and_personal_data_protection_e.pdf.

uygulanabilir olduğunda hem fikir olmuşlardır. Bağlayıcı olmayan düzenlemeler siber alana ilişkin kuralların gelişim aşamasında olduğunu göstermektedir[148]. ITU ile BM'nin rolünün artması ve ICANN üzerinde ABD'nin kontrolünün azalması siber alanın yönetişiminde kamplar arası mesafenin azaldığına işaret etmektedir[149].

[148] Huang, Z., & Mačák, K. (2017). "Towards the international rule of law in cyberspace: Contrasting Chinese and western approaches", *Chinese Journal of International Law,* 16(2), 308.
[149] Huang vd., a.g.m., 2017, 309.

## 3. ULUSLARARASI HUKUK VE ESPİYONAJ

Uluslararası hukukun barış zamanı espiyonajı düzenlememesi ikilem oluşturmaktadır: Uluslararası hukuku, espiyonaja uygulamamak uluslararası hukukun bütünlüğüne ve otoritesine zarar verirken; espiyonaja uygulamak ise devletleri ulusal güvenlikleri için faydalandıkları önemli bir araçtan yoksun bırakacaktır[150]. Uluslararası hukukun espiyonaj konusundaki sessizliğinin[151] nedeni olarak uluslararası hukukun nezaket ve insandan oluşan özünün espiyonajın ihanet ve aldatma olan özüyle tezat oluşturduğu belirtilmiştir[152]. Buradan hareketle espiyonajın, hukukun ötesinde olduğu kabul edilerek, uluslararası hukuka konu edilmemesinin daha isabetli olabileceği belirtilmiştir[153].

Geleneksel espiyonajın tolere edilebilir vaziyeti, yeni ve etkili yöntemlerle değişerek uluslararası hukukun ilgisini cezbetmektedir. Tehditlerin devingen ve çok yönlü olduğu[154] siber alan ve siber espiyonaj süratle gelişen yapısıyla bu ilgiyi canlı tutmaktadır.

Siber espiyonaj, istihbarat teşkilatlarına ve personellerine yönelik riskleri azaltan bir araçtır[155]. Nitekim siber espiyonaj, geleneksel espiyonaja nazaran daha incelikli operasyon yürütme imkânı vermekle birlikte; ilişkilendirme, hasar tespiti, önleme veya sorumluluk kavramları muğlak hale gelmektedir[156]. Siber espiyonaj tehdidinin potansiyel büyüklüğünün vurgulanabilmesi açısından internete bağlı cihaz sayısının belirtilmesi yerinde olacaktır. Siber espiyonajın hedefi haline gelebilecek muhtemel varlık sayısı 2019'da 10 milyar, 2022'de yaklaşık olarak 16.5 milyardır ve 2025'te bu sayının tahminen 31 milyarı bulması beklenmektedir[157].

Keza siber espiyonaj, sofistike şekilde kurgulanarak operasyon sırasında başkaca fonksiyonların eklemlenmesiyle etkisi artırılabilmektedir. ABD Personel

---

[150] Navarrete, I., ve Buchan, R. (2018). "Out of the legal wilderness: Peacetime espionage, international law and the existence of customary exceptions", *Cornell Int'l LJ*, 51, 898-899.
[151] Uluslararası hukukun sessizliğini yasal bir boşluktan ziyade kasıtlı bir suskunluk olduğu değerlendirilmektedir. Chesterman, a.g.m., 2005, 1072.
[152] Radsan. a.g.m., 2007, 596.
[153] Radsan. a.g.m., 2007, 597.
[154] Buchan, a.g.m., 2015, 168.
[155] Ziolkowski, a.g.e., 2013, 425.
[156] Kilovaty, I. (2016). "World Wide Web of Exploitations-The Case of Peacetime Cyber Espionage Operations Under International Law: Towards a Contextual Approach", *Colum. Sci. & Tech. L. Rev.*, 45.
[157] Vailshery L. S. (2020). Iot and non-iot connections worldwide 2010- 2025. https://www.statista.com/statistics/1101442/iot-number-of-connected-devices-worldwide/.

Yönetim Ofisinin hedef olduğu siber espiyonaj ile yaklaşık 22 milyon kişinin bilgileri ele geçirilmiş[158]; ABD Demokratik Ulusal Komitenin hedef alındığı başka bir siber espiyonaj ile ABD başkanlık seçimlerine müdahale edilebilme imkanının sağlandığı değerlendirilmiştir[159]. Fikri mülkiyet açısından tarihin en büyük servet transferi olarak değerlendirilen "Shady Rat" isimli operasyon ile onlarca devlet, uluslararası hukuk kuruluşları ve özel şirketler hedef alınmıştı[160]. Yine "Flame" olarak adlandırılan zararlı yazılım ile başta İran olmak üzere İsrail ve Lübnan gibi Orta Doğu ve Kuzey Afrika ülkelerini hedef alarak bilgiye yetkisiz erişim sağlamıştır[161]. Anılan bu ve benzeri sayısız olaylar uluslararası hukuk kapsamında siber espiyonajın meşruluğuna ve uluslararası hukukun devletleri siber espiyonajdan korumaya elverişli olup olmadığına dair soruları daha kuvvetli olarak gündeme getirmiştir[162].

Siber espiyonajın tahmin edilemeyecek boyutlara ulaşan tehlikeleri ve sonuçları karşısında devletler siber espiyonajı, ulusal düzeyde suç olarak düzenleyip ulusal güvenliğin bir parçası olarak tatbik ederken, uluslararası düzeyde siber espiyonajın meşruluğuna dair sessizlik içerisindeler[163]. Başka bir ifade ile devletlerin rutin olarak casusluk faaliyeti yürütmelerine rağmen espiyonajı uluslararası hukuka uygun bulduklarına dair emare yoktur[164].

Günlük yaşamın neredeyse tamamına temas eden[165] ve devlet/devlet dışı aktörlerin çok sayıda olduğu siber alanda devletlerin suskunluğu nedeniyle oluşan hukuksal belirsizlik[166], devletler tarafından yanlış algılama ve değerlendirme suretiyle gerilimin artmasına veya en kötü şartlarda çatışmaya neden olabilir[167]. Devletlerin

[158] Bkz. dipnot 37.
[159] Bkz. dipnot 39.
[160] Finkle J. (2011). "Q+A: Massive cyber attack dubbed "Operation Shady RAT", Reuters. https://www.reuters.com/article/us-cyberattacks-qa-idUSTRE7720IS20110803.
[161] Zetter K. (2012). "Meet 'Flame,' The Massive Spy Malware Infiltrating Iranian Computers", Wired. https://www.wired.com/2012/05/flame/.
[162] Buchan, a.g.e., 2015, 170.
[163] Sander, a.g.m., 2019, 370; Ziolkowski, a.g.e., 2013, 441.
[164] Shull, A. (2013). "Cyber Espionage and International Law", *In GigaNet: Global Internet Governance Academic Network, Annual Symposium*, 1-2.
[165] UN Secretary-General, "Foreword" , *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, UN Doc A/68/98, 24 June 2013, 4.
[166] Macak, a.g.m., 2017, 888; Efrony, D., & Shany, Y. (2018). "A Rule Book on the Shelf? Tallinn Manual 2.0 on Cyberoperations and Subsequent State Practice", *American Journal of International Law*, 112(4), 647-648.
[167] Egan, B. J. (2017). "International law and stability in cybershpace", *Berkeley J. Int'l L.*, 35, 171-172.

siber alana ilişkin bekle ve gör politikasına[168] karşılık, uluslararası hukukun siber alana nasıl uygulanacağı üzerine akademik çalışmalar yapılmaktadır[169]. Ancak bu çabalar devletlerin görüş ve eylemlerini tüm yönüyle ortaya koymamaktadır[170].

### 3.1. Meşruluk Sorununa Geleneksel Cevap Arayışı

Siber espiyonajı düzenleyen özel bir antlaşma veya kurallar bulunmadığı gibi siber espiyonaja mukayese yolu ile uyarlanabilecek geleneksel espiyonajı düzenleyen bir kaynak da bulunmamaktadır[171]. Ancak mantıksal olarak espiyonajın uluslararası hukuka göre meşru olup olmadığına ya olumlu ya da olumsuz cevap verilebilecektir.

#### 3.1.1. Espiyonajın Meşru Olduğu Argümanı

Espiyonajın meşru olduğuna ilişkin temel hareket noktası, uluslararası hukukta espiyonajı yasaklayan bir düzenlemenin bulunmamasıdır[172]. Buna paralel olarak Uluslararası Daimi Adalet Divanı, Lotus davasında temel bir prensip ortaya koymuştur. Buna göre uluslararası hukukta yasaklayıcı bir hüküm bulunmuyorsa egemenlik kavramı kapsamında devletler uygun gördüğü ilkeleri benimsemekte geniş takdir yetkisine sahiptir[173].

Meşru müdafaa hakkının geniş bir yorumu olarak önleyici meşru müdafaa kapsamında espiyonajın[174] uluslararası hukuku ihlal etmediği belirtilmektedir[175]. Buna göre BM Antlaşmasının kuvvet kullanmadan kaçınılmasına ilişkin ikinci maddesinin dördüncü fıkrasına uygun hareket edebilmek için casusluk faaliyetinde bulunabilirler. Özellikle uluslararası hukuka saygılı olmayan taraflar ile angajman ihtimalinin artması meşru müdafaa kapsamında espiyonajı meşru kılmaktadır[176].

---

[168] Sander, a.g.m., 2019, 363.
[169] Sander, a.g.m., 2019, 362.
[170] Egan, a.g.m., 2017, 172.
[171] Buchan, R. J. (2016). "The International Legal Regulation of State-Sponsored Cyber Espionage", *International Cyber Norms: Legal, Policy & Industry Perspectives*, 68.
[172] Scott, R. D. (1999). "Territorially Intrusive Intelligence Collection and International Law", *Air Force Law Review*, 220.
[173] The Lotus Case,1927, 18-19.
[174] Bu argümanın temeli, Sovyet bölgesinde ABD ordusu için bilgi toplamayla görevli U-2 adlı keşif uçağının 1960 yılında Sovyetler tarafından düşürülmesi sonrasında ABD'nin U-2'nin eylemlerinin uluslararası hukuka uygun olduğunu savunmasına dayanmaktadır. Demarest, a.g.m., 1996, 340-341; Ziolkowski, a.g.e., 2013, 437.
[175] Melnitzky, A. (2012). "Defending america against chinese cyber espionage through the use of active defenses", *Cardozo Journal of International and Comparative Law*, 20(2), 564;Sulmasy ve Yoo, a.g.m., 2006, 636; Baker, C. D. (2003). "Tolerance of international espionage: a functional approach", *Am. U. Int'l L. Rev.*, 19, 1095.
[176] Sulmasy ve Yoo, a.g.m., 2006, 636.

Uluslararası barış ve güvenliği tehdit eden uluslararası terörizm ve kitle imha silahlarının yaygınlaşmasının önlenmesinde ve potansiyel çatışmaların barışçıl yöntemlerle çözümlenmesinde espiyonajın hayati öneme sahip olduğu cihetiyle gerekliliği tespit edilmiştir[177].

### 3.1.1.1. Uluslararası teamül hukuku

Uluslararası teamül hukukunun uluslararası hukukun kaynaklarından olduğu maruftur. Divan Statüsü'nde belirtildiği üzere[178] ihtilafların çözümlenmesinde Divanının başvuracağı kaynakların arasında uluslararası teamül hukuku yer almaktadır. Statünün otuz sekizinci maddesinin birinci fıkrasının (b) bendine ve akademik çalışmalara[179] göre uluslararası teamül hukuku iki unsurdan oluşmaktadır[180]: Yerleşik, yaygın ve istikrarlı devlet uygulaması (*state practice*) ve bu uygulamanın uluslararası hukuka göre gerekli veya meşru olduğu inancı (*opinio iuris*).

Bu bağlamda devletlerin, istihbarat kurumları aracılığı ile yürüttükleri faaliyetler ve espiyonaja ilişkin sessizlik politikası benimsemelerinin anılan unsurları oluşturduğundan bahisle espiyonajın uluslararası teamül hukukuna göre meşru olduğu savunulmaktadır[181]. Uluslararası barış ve güvenliğin istikrarına hizmet eden espiyonaj, gerekli olmadıkça güç kullanılmaması ve krizlerin proaktif yöntemlerle çözülmesine katkı sağlayarak[182] espiyonajın uluslararası hukuka göre gerekli veya meşru olduğu inancını desteklemektedir.

#### 3.1.1.1.1. Devlet uygulamaları

Devletlerarası ilişkilerin sabiti haline gelen espiyonaj, devletin yasal bir işlevi olarak uluslararası teamül hukuku kapsamında meşrudur[183]. Nitekim diplomatik örtü altında operasyon icra eden istihbarat memurları ifşa olduklarında hedef devlet

---

[177] Sulmasy ve Yoo, a.g.m., 2006, 637-638.
[178] Uluslararası Adalet Divanı Statüsü madde otuz sekiz.
[179] Wolfrum, R. (2011). "Sources of international law", *Max Planck Encyclopedia of Public International Law*, 9, 306 vd.; Evans M.D.(Editör) (2010). *International law,* Oxford University Press, 102 vd.
[180] Uluslararası teamül hukukunun unsurlarını etraflıca inceleyen ve sıklıkla atıf alan Divan kararları için bkz. North Sea Continental Shelf Cases (Federal Republic of Ger. v. Den.; Federal Republic of Ger. v. Neth.), Judgment, 1969, Internatıonal Court Of Justıce; Judgment; Case Concerning Military And Paramilitary Activities in and Against Nicaragua.
[181] Smith, J. H. (2007). "Keynote Address at the University of Michigan Journal of International Law Symposium: State Intelligence Gathering and International Law", *Mich. J. Int'l L,* 544.
[182] Chesterman, a.g.m., 2005, 1076.
[183] Smith, a.g.m., 2007, 544.

tarafından istenmeyen kişi *(persona non grata)* olarak ilan edilirken, uluslararası hukukun ihlal edildiğinden bahsedilmez[184].

Yine devletler, memurları tarafından yürütülen istihbarat operasyonlarını yasaklamamakta ve hatta iç hukuk kuralları ile istihbarat faaliyetlerini düzenlemektedirler[185]. Örneğin İngiltere, 1994 İstihbarat Hizmetleri Yasası ile ve ABD, 1947 Ulusal Güvenlik Yasası ile espiyonajı düzenlemiştir. Diğer taraftan hedef devletin kendisine yönelik espiyonajı suç olarak düzenlemesi caydırıcı ve maliyet artırıcı nitelikte olup espiyonajın uluslararası hukuk bağlamında ihlal olarak değerlendirildiği anlamına gelmemektedir[186].

Espiyonaj, şüphesiz devletlerin geleneksel bir uygulamasıdır[187]. Bu uygulama yalnızca hasımlara değil müttefiklere karşı da gerçekleştirilmektedir. Nitekim NSA'nın Berlin'deki Amerikan Elçiliğini dinleme üssü olarak kullandığı ve aralarında dönemin Almanya Şansölyesi'nin de bulunduğu hedeflere yönelik operasyon yürüttüğü ifşa olmuştur[188]. ABD eski başkanı Obama, sinyal istihbaratı hakkında değerlendirmelerinde, tüm ulusların istihbarat servisleri gibi ABD istihbaratının bilgi toplamaya devam edeceğini belirtmiştir[189]. Devletler istihbarat operasyonlarını inkâr etmemekte; insanların mahremiyet kaygısı ve güvenlik endişesi ekseninde dengeli olarak operasyon icra ettiklerini belirtmektedirler[190]. Mevcut durumda devletleri, espiyonajın varlığı değil boyutu endişelendirmektedir[191].

---

[184] Smith, a.g.m., 2007, 544.
[185] Sulmasy ve Yoo, a.g.m., 2006, 624.
[186] Chesterman, a.g.m., 2005, 1077.
[187] Scott, a.g.m.,1999, 226; [187] Navarrete ve Buchan, a.g.m., 2018, 915-916.
[188] von SPIEGEL Staff. (2013). The NSA's Secret Spy Hub in Berlin. https://www.spiegel.de/international/germany/cover-story-how-nsa-spied-on-merkel-cell-phone-from-berlin-embassy-a-930205.html;
[189] The White House Office President Barack Obama. (2014), *Remarks by the President on Review of Signals Intelligence*. https://obamawhitehouse.archives.gov/the-press-office/2014/01/17/remarks-president-review-signals-intelligence.
[190] Rubin A. J. (2013). French Condemn Surveillance by N.S.A, The New York Times. https://www.nytimes.com/2013/10/22/world/europe/new-report-of-nsa-spying-angers-france.html.
[191] Fransa Dış İşleri eski Bakanı NSA'nın Fransa'daki operasyonlarıyla ilgili olarak yapmış olduğu bir açıklamada; operasyonun boyutunun şok edici olduğunu, neticede herkesin herkesi dinlediğini belirtmiştir. LoGiurato B. (2013). "Former French Foreign Minister Nails It On The Outrage Over US Spying On Foreign Leaders", Insider. https://www.businessinsider.com/nsa-spying-outrage-merkel-germany-obama-france-hollande-2013-10.

### 3.1.1.1.2. Opinio iuris

Uluslararası teamül hukukunun ikinci unsuru olan *opinio iuris,* devlet uygulamalarına eşlik etmediği sürece teamül hukukunun varlığından söz edilemez[192]. Diğer bir ifadeyle devlet uygulamaları ne kadar yaygın ve istikrarlı olursa olsun *opinio iuris* olmadan yetersiz kalacaktır[193].

Devlet uygulamalarında hukuksal inancın (*opinio iuris*) kaynağı tadadi olarak; uluslararası teamül hukukunu yansıtan sözleşmelerin uygulanması, uluslararası kuruluşlar nezdinde veya devletlerarası konferanslarda kabul edilen kararlarla bağlantılı olarak hareket edilmesi, devletlerin resmi yayınları ve hukuki görüşleri, diplomatik yazışmalar veya ulusal mahkemelerin kararları sayılabilir[194]. Ancak devletlerin espiyonaj konusunda sessizlik politikası içerisinde olmaları ve buna ilişkin çözümleri uluslararası hukukun muhtelif alanlarında aramaları hukuksal inancın tespitini engellemektedir[195].

1981 yılında Sovyet denizaltısının İsveç tarafından askeri olarak korunan bölgede karaya oturması üzerine, her ne kadar Sovyet deniz altısının istihbarat amacıyla bölgede olduğu bilinse de[196], çevresel koşullara ve egemenlik alanına ilişkin kaygılar ile İsveç tarafından protesto edilmiştir[197]. Siber espiyonaj kapsamında "Moonlight Maze[198]" ve "Titan Rain[199]" olayları karşısında da ABD sessizliğini

[192] Buchan, a.g.m, 2016, 83.
[193] Buchan, a.g.m, 2016, 83; Report of the International Law Commission, Seventieth session, U.N. Doc. A/73/10, 124.
[194] A/73/10, 120.
[195] Navarrete ve Buchan, a.g.m., 2018, 928.
[196] Frank J. Prial. (1981). "Sovıet Sub Spends Sıxth Day Grounded On Swedısh Coast", The New York Times, https://www.nytimes.com/1981/11/02/world/soviet-sub-spends-sixth-day-grounded-on-swedish-coast.html.
[197] Ziolkowski, a.g.e., 2013, 439.
[198] 1998-1999 yıllarında tespit edilen ve 1996 yılında ilk sızmanın gerçekleştiği tahmin edilen olayda Rusya ve Çin destekli olduğu düşünülen bir grup, ABD Savunma ve Enerji Bakanlıklarına, Ulusal Havacılık ve Uzay Dairesi (National Aeronautics and Space Administration - NASA) ve bir kısım araştırma tesislerinin bilgisayar sistemlerine girerek aralarında kritik belgelerinde bulunduğu sayısız dosyayı sistematik olarak incelemişlerdir. K. Thakur, M. L. Ali, N. Jiang and M. Qiu, "Impact of Cyber-Attacks on Critical Infrastructure," *2016 IEEE 2nd International Conference on Big Data Security on Cloud (BigDataSecurity), IEEE International Conference on High Performance and Smart Computing (HPSC), and IEEE International Conference on Intelligent Data and Security (IDS)*, 2016. https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7502286.
[199] 2003 yılından itibaren Çin menşeli olduğu düşünülen sızma girişimleri ile başta ABD olmak üzere birkaç ülkenin savunma bakanlıkları özelinde devlet kurumları hedef alınmıştır. Richard Norton-Taylor. (2007). "Titan Rain - how Chinese hackers targeted Whitehall", The Guardian. https://www.theguardian.com/technology/2007/sep/04/news.internet.

korumuştur[200]. Beş göz ittifakının[201] temeli olan Birleşik Krallık ve ABD Anlaşması (United Kingdom and United States of America Agreement - UKUSA )[202] kapsamında ABD öncülüğünde oluşturulan ECHELON adlı sistem ile ABD ve müttefikleri lehine küresel iletişimin her hali ele geçirilmektedir[203]. ECHELON sisteminin ve hatta benzer sistemlerin varlığını tespit eden resmi rapor dahi devletlerin sessizliğine son vermemiştir[204]. Nitekim 2003 yılında NSA ve İngiltere Hükümet İletişim Merkezi (Government Communications Headquarters –GCHQ) tarafından BM Güvenlik Konseyi delegasyonunun ev ve ofis telefonlarının ve elektronik yazışmaların takip edildiğinin ifşası[205] karşısında BM, ABD ile temasa geçeceğini belirtmekle yetinmiştir[206].

Devletlerin sessizlik hali, hukuksal inançlarının tespitine engel olsa da devletlerin genel ve tutarlı uygulamalarının meşru bir hak duygusunu barındırdığından[207] bahisle uluslararası hukukun espiyonaj nedeniyle ihlali mümkün kurallarına "istisna[208]" oluşturduğu belirtilmiştir[209]. Burada öncelikle devletlerin sessizlik politikasına espiyonajı onaylama anlamı yüklenmiş, sonrasında ise bunun bir istisna oluşturduğu kabul edilmiştir. Dolayısıyla espiyonajın bazı şekillerinin uluslararası hukuku ihlal edebileceği de kabul edilmiştir. Hülasa devletlerin espiyonaj uygulamalarının sıradanlığının boyutu *opinio iuris*i oluşturarak uluslararası hukuk kurallarına istisna getirmektedir.

---

[200] Ziolkowski, a.g.e., 2013, 440.
[201] Bkz. dipnot 88.
[202] Government Communications Headquarters (GCHQ). A Brief History of the UKUSA agreement. https://www.gchq.gov.uk/information/brief-history-of-ukusa
[203] Sloan, L. D. (2001). "Echelon and the legal restraints on signals intelligence: need for reevaluation", *Duke Law Journal*, 50(5), 1467-1468;
[204] European Parliament. "REPORT on the existence of a global system for the interception of private and commercial communications (ECHELON interception system) (2001/2098(INI))". https://www.europarl.europa.eu/comparl/tempcom/echelon/pdf/rapport_echelon_en.pdf.; Ziolkowski, a.g.e., 2013, 440.
[205] Martin Bright, Ed Vulliamy ve Peter Beaumont. (2003). "Revealed: US dirty tricks to win vote on Iraq war", The Guardian. https://www.theguardian.com/world/2003/mar/02/usa.iraq.
[206] Reuters. (2013). "United Nations says it will contact United States over spying report". https://www.reuters.com/article/us-usa-security-nsa-un-idUSBRE97P0O720130826.
[207] Forcese, C. (2011). Spies without Borders: International Law and Intelligence Collection. Journal of National Security Law & Policy, 5(1), 201.
[208] Divan, uluslararası hukuk kurallarının kapsamını değiştiren uluslararası teamül hukuku gelişmelerini istisna olarak tanımlamaktadır. Bkz. Judgment; Concerning Military And Paramilitary Activities in and Against Nicaragua, 207.
[209] Melnitzky, a.g.m., 2012, 564; Sulmasy ve Yoo, a.g.m., 2006, 628.

### 3.1.1.2. Espiyonajın izin verilen bir devlet eylemi olduğuna ilişkin yaklaşımlar

Devletlerin espiyonajı daha etkin gerçekleştirmek için teknolojik gelişmelerden yararlanması kaçınılmazdır[210]. Nitekim deniz, hava ve uzay araçlarının ortaya çıkışı ve gelişmesiyle bu alanlar espiyonaj için kullanılmaya başlanmıştır[211]. Egemenlik iddiasının geçerli olmadığı ve rejimlerinin sözleşme ile düzenlendiği açık denizler, dış uzay ve Antarktika alanlarında espiyonajın genel olarak kabul edildiği belirtilmiştir[212]. Hatta şeffaflık ve güven sağladığı için uluslararası toplumun yararına olduğu belirtilmiştir[213].

Açık denizlerde espiyonaj, açık denizlerin serbestliği prensibi kapsamında değerlendirilmektedir[214]. Meşruluğu Birleşmiş Milletler Deniz Hukuku Sözleşmesi (BMDHS) seksen yedinci maddesine isnat edilen espiyonajın devlet uygulamaları ile de istikrar kazandığı iddia edilmiştir[215]. 1967 tarihli Ay ve Diğer Gök Cisimleri Dahil, Uzayın Keşfi ve Kullanımında Devletlerin Faaliyetlerini Düzenleyen İlkeler Hakkında Antlaşma'nın, antlaşmaya konu tüm istasyon ve eklentilerin antlaşmaya taraf devletler tarafından ziyaret edilebileceğini düzenlemesi; 1979 tarihli Devletlerin Ay ve Diğer Gök Cisimleri Üzerindeki Faaliyetlerini Düzenleyen Anlaşma'nın anlaşmaya taraf devletlere Ay'da bulunan istasyon ve diğer unsurların mezkur anlaşmaya uygun kullanılıp kullanılmadığını denetleme hakkı barındırması dış uzayda espiyonaja izin verildiği anlamında değerlendirilmiştir[216]. Uluslararası alanda gerçekleşen espiyonaja ilişkin bu değerlendirme, egemenlik iddia edilebilen alanların egemenlik iddia edilemeyen alanlardan ayrı incelenmesini; espiyonajın başka bir adla da olsa (stratejik gözlem, keşif gibi) izin verildiğinin kabul edilmesiyle herhangi bir uluslararası kuralın ihlalinden kaçınılmasını sağlamaktadır[217].

Aynı yönde ve somut olarak gözetleme uydularını yasaklayan ya da bunların kullanılmasını protesto eden devlet bulunmamaktadır[218]. Hatta Birleşmiş Milletler

---

[210] Kilovaty, a.g.m., 2016, 62.
[211] Buchan, a.g.m, 2016, 66.
[212] Kraska, J. (2015). "Putting Your Head in the Tiger's Mouth: Submarine Espionage in Territorial Waters", *Colum. J. Transnat'l L.*, 54, 173.
[213] Kraska, a.g.m., 2015, 169.
[214] Kraska, a.g.m., 2015, 174.
[215] Ziolkowski, a.g.e., 2013, 443.
[216] Ziolkowski, a.g.e., 2013, 443;
[217] Jupillat, N. (2016). "From the Cuckoo's Egg to global surveillance: cyber espionage that becomes prohibited intervention", *NCJ Int'l L.*, 42, 962.
[218] Chesterman, a.g.m., 2005, 1085; McDougal vd., a.g.m., 1972, 434.

Eğitim ve Araştırma Enstitüsü (United Nations Institute for Training and Research - UNITAR) uhdesinde bulunan Birleşmiş Milletler Uydu Merkezi (The United Nations Satellite Centre - UNOSAT) karar verme süreçlerine coğrafi-mekânsal veriler ile destek sağlamaktadır[219]. Yine, Rusya'ya ait bir teknenin ABD karasuları dışında istihbarat faaliyeti yürüttüğü bilinmesine rağmen uluslararası sularda yer aldığı için müdahale edilmemesi[220] devletlerin açık denizde espiyonaja yönelik perspektiflerine örnek gösterilebilir.

Espiyonaj ve diplomasi genellikle birlikte hareket etmektedir[221]. Nitekim 1961 tarihli Diplomatik İlişkiler Hakkında Viyana Sözleşmesi (DİHVS) kabul eden devletteki koşulları ve gelişmeleri meşru yöntemler ile tespit ederek gönderen devlete aktarmayı diplomatik misyonların fonksiyonları arasında saymıştır[222]. Koşullar ve gelişmelerden maksut, kabul eden devletin politik, kültürel, sosyal veya ekonomik aktiviteleri dâhil olmak üzere genel olarak gönderen devletin ilgilendiği tüm alanlardır[223]. Anılan düzenlemenin, devletlere espiyonaj hakkını tanıdığı savunulmuştur[224]. Keza DİHVS kapsamında sağlanan diplomatik dokunulmazlık, istihbarat faaliyetlerinin maliyetini düşürerek devletleri diplomatik misyonlar aracılığı ile espiyonaja teşvik etmektedir[225].

### 3.1.2. Espiyonajın Meşru Olmadığı Argümanı

Espiyonaj, uluslararası hukuk tarafından konu alınmasa[226] dahi uluslararası hukuku ihlal edeceği savunulmaktadır[227]. Bu değerlendirmenin kaynaklarından biri, devletlerin iç hukuklarında espiyonajı suç olarak düzenlemesidir[228]. Uluslararası hukuka göre bir şeyin meşruluğu için onun devletler tarafından da yasal olarak

[219] Unıted Natıons Satellıte Centre, About Us. https://unosat.org/about-us/.
[220] Jupillat, a.g.m., 2016, 964.
[221] Chesterman, a.g.m., 2005, 1087.
[222] DİHVS, (1961) United Nations, Treaty Series, vol. 500, madde 3.
[223] Report of the International Law Commission covering the work of its Tenth Session, 28 April 4 July 1958, Official Records of the General Assembly, Thirteenth Session, Supplement No. 9. Extract from the Yearbook of the International Law Commission:1958, vol. II. A/CN.4/117. https://legal.un.org/ilc/documentation/english/reports/a_cn4_117.pdf.
[224] Kilovaty, a.g.m., 2016, 62-63.
[225] Radsan. a.g.m., 2007, 598-599.
[226] Demarest, a.g.m., 1996, 338.
[227] Garcia-Mora, M. R. (1964). "Treason, Sedition and Espionage as Political Offenses Under the Law of Extradition", *U. Pitt. L. Rev.,* 26, 79-80.
[228] Ziolkowski, a.g.e., 2013, 431; Radsan. a.g.m., 2007, 604.

tanınması gerekmektedir[229]. Espiyonaj ise devletler tarafından suç olarak düzenlenmektedir.

BM Antlaşmasının ikinci maddesi dördüncü fıkrası kapsamında espiyonaj, egemenlik ilkesinin ihlali anlamına geldiğinden bahisle uluslararası hukuka göre illegaldir[230]. Espiyonaj, kuvvet kullanımı veya tehdidi olarak değerlendirilebilecek bir durumun ön hazırlığı olması durumunda hem uluslararası hukukun ihlaline hem meşru müdafaa hakkının haklı kullanımına neden olabilecektir[231]. Fiziksel olarak sızmayı da gerektiren espiyonaj türleri, egemenlik ilkesi özelinde ülkesel egemenliği ihlal edecektir[232]. Yine başka bir değerlendirmeye göre espiyonaj amacıyla bir istihbarat memurunun görevlendirilmesi, izinsiz giriş gerçekleşmese dahi devletlerin barışçıl iş birliği ilkesini ihlal edeceğinden uluslararası hukuka göre illegal olacaktır[233].

Devletler, makul derecede inkâr edilebilirlik niteliğini yitiren espiyonaj hakkında sessizlik haline son vererek söz konusu espiyonaja sahip çıkarak meşruluğunu savunsalar da karşılık bulamamıştır[234]. 1960 yılında ABD keşif uçağı U-2'nin[235] yürüttüğü faaliyetin, Sovyetler Birliğinin egemenliğini ihlal ettiği sonucuna varılmıştır. Yine 1982'de Nikaragua bölgesinde ABD tarafından yapılan düzenli keşif uçuşlarının, Nikaragua hükümetinin ABD'nin ve diğer ulusların güvenliğini tehdit ettiği gerekçesine dayanılarak meşru olduğu ABD tarafından savunulmuş[236] ancak kabul görmemiştir[237].

[229] Radsan. a.g.m., 2007, 604. Bu değerlendirmeye karşı olarak; Uluslararası Adalet Divanı Statüsü'nün 38'inci maddesinin birinci fıkrasının (c) bendinde yer alan düzenleme ile uyuşmadığı belirtilmektedir. Espiyonajın bireysel ceza sorumluluğu kapsamında düzenlenmesinin *uygar uluslarca kabul edilen genel hukuk ilkeleri* kapsamında olmadığından devletlerin iç hukuk düzenlemeleri bu bağlamda uluslararası hukukun kaynağı olarak değerlendirilmemelidir. Ziolkowski, a.g.e., 2013, 432.
[230] Forcese, a.g.m., 2011, 198.
[231] Forcese, a.g.m., 2011, 199.
[232] Kilovaty, a.g.m., 2016, 62-63; Forcese, a.g.m., 2011, 198; Diğer taraftan bu yaklaşım, ülkesel egemenlik iddiasının bulunmadığı alanlarda tek ve yalnızca espiyonajın uluslararası hukuku ihlal etmediğini kabul etmektedir. Jupillat, a.g.m., 2016, 954.
[233] Delupis, a.g.m., 1984, 67.
[234] Navarrete ve Buchan, a.g.m., 2018, 941.
[235] Bkz. dipnot 22.
[236] Security Council official records, 37th year, 2335th meeting, 25 March 1982, New York. S/PV.2335, 12. https://digitallibrary.un.org/record/83326#record-files-collapse-header.
[237] Judgment; Case Concerning Military And Paramilitary Activities in and Against Nicaragua, 147.

### 3.1.2.1. Uluslararası teamül hukuku

Devletlerin uygulamaları ile *opinio iuris*leri zıt yönde hareket etmektedirler[238]. Nitekim devletler, hedef oldukları istihbarat faaliyetlerini kınarken[239] kendi yürüttükleri istihbarat faaliyetlerine haklılık inancı değil haksızlık inancı eşlik etmektedir[240]. Ayrıca devletlerin iç hukukları ile istihbarat faaliyeti yürütmeyi meşrulaştırırken; hedef alınmayı suç olarak düzenlemeleri, espiyonajın uluslararası teamül hukukuna göre meşruluğunun sorgulanmasında çelişkili bir durum oluşturmaktadır[241].

#### 3.1.2.1.1. Devlet uygulamaları

Uluslararası teamül hukuku bağlamında devlet uygulamalarının genel ve tekdüze olması gerekmektedir.[242] Diğer bir ifade ile çıkarları etkilenen devletlerin yaygın uygulamaları ve katılımı uluslararası teamül hukuku kuralının oluşması için gereklidir. Uluslararası teamül hukukunun tanımlanmasına ilişkin ikinci raporda[243] devlet eylemlerinin gizli oluşunun genel uluslararası teamül hukukunun oluşumuna veya tanımlanmasına olan katkısının tespitini güçleştirdiği belirtilmiştir. Bu bağlamda espiyonajın doğasının özünde gizlilik oluşu devlet uygulamaları için aranan genel ve tekdüzeliği sağlayıp sağlamadığının tespitini zorlaştırmaktadır[244].

Uluslararası teamül hukukunun gelişimini destekleyecek devlet uygulamaları kamusal olmalıdır[245]. Uluslararası Hukuk Derneği (International Law Association) tarafından hazırlanan raporda, uluslararası toplumun bilgisi dâhilinde olmayan eylemlerin uluslararası teamül hukukunun unsuru olan devlet uygulaması sayılmaması gerektiği belirtilmiştir[246]. Yine aynı raporda, devletlerin gizli eylemleri kamunun bilgisine dâhil olsa bile ilgili devlet tarafından söz konusu eylemin meşru olduğu savunulmadığı sürece uluslararası teamül hukuku bağlamında devlet uygulaması

[238] Chesterman, a.g.m., 2005, 1072; Buchan, a.g.m, 2016, 85.
[239] Chesterman, a.g.m., 2005, 1072.
[240] Buchan, a.g.m, 2016, 85.
[241] Chesterman, a.g.m., 2005, 1077.
[242] North Sea Continental Shelf Cases, Judgment, 43.
[243] Wood M., Second Report on Identification of Customary International Law, Identification of Customary International Law, 184, U.N. Doc. A/CN.4/672.
[244] Navarrete ve Buchan, a.g.m., 2018, 917.
[245] Navarrete ve Buchan, a.g.m., 2018, 919.
[246] Committee On Formation Of Customary (General) International Law. (2000). Final Report of The Committee Statement Of Principles Applicable To The Formation of General Customary International Law, International Law Association, 15.

olarak kabul görmeyecektir. Siber alan özelinde devletler görüşlerini açıklayarak uluslararası toplumda devlet eylemlerine ilişkin öngörülebilirlik sağlanabilecektir[247]. Böylece devlet eylemlerinin alenileşmesi ile uluslararası teamül hukukunun gelişimine katkı sağlanacaktır[248].

#### 3.1.2.1.2. Opinio iuris

Devletlerin kendi istihbarat faaliyetleri hakkındaki sessizlikleri, politik bir ifade olup hukuksal bir değerlendirme değildir**.** Diğer bir ifade ile devletlerin espiyonaj kapsamındaki inançları, *opinio iuris* niteliğinde değildir[249]. Pratik olarak sessizlik, operasyon yürüten devletin görevdeki istihbarat memurlarını ve operasyonu korumaya hizmet etmektedir[250]. Dolayısıyla politik bir tutum olarak sessizlik politikası, devletlerin kendilerine yönelik operasyonları kapsamamakta ve *opinio iuris* olarak değerlendirilmemesi gerekmektedir.

Devletler, diğer devletler hakkında yürüttükleri istihbarat faaliyetlerini istikrarlı olarak reddetmişlerdir. Çin kaynaklı olduğu değerlendirilen Aurora adlı siber operasyon ile aralarında Yahoo, Adobe, Morgan Stanley ve Google gibi büyük firmaların yer aldığı Amerikan özel sektörü hedef alınarak ticari sırlar ele geçirilmiştir[251]. Google söz konusu operasyonu teyit etmiş ve bir kısım insan hakları aktivistlerine ilişkin bilgilerin gizliliğini yitirdiğini belirterek; Çin'deki faaliyetlerini gözden geçireceğini duyurmuştur[252]. 2010 yılında ABD Dışişleri Bakanı Clinton, Çin'in siber alandaki faaliyetlerini eleştirerek, Aurora operasyonu ile ilgili olarak Çin'i suçlamıştır.[253] Çin Dışişleri Bakanlığı Sözcüsü siber espiyonajın en büyük kurbanlarından birinin Çin olduğunu, ortak mücadele ve iş birliğinin önemini

[247] Egan, a.g.m., 2017, 172.
[248] Navarrete ve Buchan, a.g.m., 2018, 919.
[249] Terry, P. C. (2015). "Absolute Friends: United States Espionage against Germany and Public International Law", *Revue Quebecoise de Droit International,* 28(2), 183-184.
[250] Navarrete ve Buchan, a.g.m., 2018, 937.
[251] Mark Clayton. (2012). "Stealing US business secrets: Experts ID two huge cyber 'gangs' in China", The Christian Science Monitor. https://www.csmonitor.com/USA/2012/0914/Stealing-US-business-secrets-Experts-ID-two-huge-cyber-gangs-in-China; Operation Aurora, Council on Foreign Relations. https://www.cfr.org/cyber-operations/operation-aurora.
[252] David Drummond. (2010). "Statement from Google: A new approach to China", The Washington Post. https://www.washingtonpost.com/wp-dyn/content/article/2010/01/12/AR2010011202903.html?tid=a_inl_manual.
[253] Chris McGreal ve Bobbie Johnson. (2010). "Hillary Clinton criticises Beijing over internet censorship", The Guardian. https://www.theguardian.com/world/2010/jan/21/hillary-clinton-china-internet-censorship.

vurgularken ABD'yi gerçeklere saygı duymaya ve Çin'e yönelik eylemlerine son vermeye davet etmiştir[254].

Espiyonaj hakkında devletlerin birbirlerini suçlaması, doğru ve uygun eylem hakkında mesaj vermek suretiyle *opinio iuris* gelişimine katkı sunabilecektir[255]. Suçlamanın tıpkı uluslararası teamül hukuku bağlamında devlet uygulamaları gibi yaygın ve istikrarlı olması ile hukuksal inancın oluşmasına etkili bir katkı sağlayabilecektir.

Devlet eylemleri, inkâr edildiği veya kınandığı sürece bu eylemlerin *opinio iris* oluşturduğu söylenemez[256]. Nitekim inkâr edilen eylem, devlet uygulaması niteliğini haiz değildir. Espiyonaj ile ilgili olarak inkâr ya da sessizlik halinde, espiyonajın sorgulanabilir yapısı ve yanlışlık duygusu barındırması etkilidir[257]. Keza tarihsel olarak istihbarat memuru yakalanan devletler; memurlarının mahkûm edilmesine, sınır dışı edilmesine veya istenmeyen kişi ilan edilmesine itiraz etmemişlerdir[258].

#### 3.1.2.2. Espiyonajın izin verilmeyen bir devlet eylemi olduğuna ilişkin yaklaşımlar

Espiyonajın bireylere dönük neticelerinden biri mahremiyetlerinin ihlal edilmesidir. Kişisel ve Siyasal Haklar Uluslararası Sözleşmesi (KSHUS) on yedinci maddesine göre kişilerin haberleşmelerine keyfi veya hukuksuz olarak müdahale edilemeyeceği düzenlenmiştir. KSHUS devletlere, sözleşme hükümlerine saygı gösterme ve egemenlik alanlarında uyulmasını temin etme sorumluluğu getirmiştir[259]. Aynı yönde İnsan Hakları Avrupa Sözleşmesi (İHAS), mahremiyet hakkını düzenlemiş[260] ve devletleri yetki alanları içerisinde herkesin bu haktan yararlanmasını temin etme ile yükümlü kılmıştır[261]. Yine İnsan Hakları Amerikan Sözleşmesi[262] ve

[254] Ma Zhaoxu. (2010). Foreign Ministry Spokesperson Ma Zhaoxu's Remarks on China-related Speech by US Secretary of State on "Internet Freedom", Embassy Of The People's Republıc of Chına In The Kıngdom of Sweden. http://se.china-embassy.gov.cn/eng/fyrth/201001/t20100122_2879230.htm.
[255] Finnemore, M., ve Hollis, D. B. (2020). "Beyond naming and shaming: accusations and international law in cybersecurity", *European Journal of International Law*, 31(3), 984.
[256] Navarrete ve Buchan, a.g.m., 2018, 936.
[257] Jupillat, a.g.m., 2016, 956; Lubin, A. (2020). "The liberty to spy", *Harv. Int'l LJ*, 61, 225.
[258] Jupillat, a.g.m., 2016, 956.
[259] KSHUS, madde 2(1).
[260] İHAS, madde 8(1).
[261] İHAS, madde 1.
[262] İnsan Hakları Amerikan Sözleşmesi 11'inci madde ile hakkı, 1'inci madde ile devletlerin sorumluluğunu düzenlemiştir.

İnsan Hakları Arap Sözleşmesi[263] de mahremiyet hakkını ve devletlerin sorumluluğunu benzer şekilde düzenlemiştir. ITU tüzüğüne göre uluslararası yazışmaların gizliliğinin korunması amacıyla devletler gerekli tüm tedbirleri alabilmektedir[264]. Mezkûr sözleşme düzenlemeleri ile devletlerin, kendi yetki alanları içerisinde yer alan kişileri diğer ülkelerin istihbarat faaliyetlerinden koruma yükümlülüğü bulunduğu belirtilebilir[265].

Ekonomik alana özgü olarak devletlere, yetki alanları kapsamında olmak üzere, sorumluluk yükleyen düzenlemeler de mevcuttur. Sınai Mülkiyetin Korunmasına İlişkin Paris Sözleşmesi'nin (Paris Convention for the Protection of Industrial Property – Paris Konvansiyonu) haksız rekabete ilişkin düzenlemesi[266], Ticaretle Bağlantılı Fikri Mülkiyet Anlaşması'nın (Agreement on Trade-Related Aspects of Intellectual Property Rights - TRIPS) açıklanmamış bilgilerin korunmasına ilişkin düzenlemesi[267] bu kapsamdadır. Aynı bağlamda Dünya Fikri Mülkiyet Örgütü Telif Hakları Anlaşması (World Intellectual Property Organızatıon [WIPO] Copyrıght Treaty - WCT), Edebiyat ve Sanat Eserlerinin Korunmasına İlişkin Bern Sözleşmesi'nin kapsamını dijital ortama genişleterek özellikle veri tabanlarını[268] ve bilgisayar programlarını[269] koruma altına almıştır. Ekonomik alana ilişkin anılan düzenlemeleri taraf devletler, kendi egemenlik alanlarında tesis ve temin etmekle sorumludur[270].

DİHVS, 1963 tarihli Konsolosluk İlişkileri Hakkında Viyana Sözleşmesi (KİHVS) ve 1969 Özel Misyonlara Dair Sözleşme (ÖMDS) düzenlemeleri kabul eden devletin istihbarat faaliyetlerine karşı koruma sağlamaktadır. DİHVS yirmi dördüncü ve yirmi yedinci maddeleri misyona ilişkin yazışmaların, evrakların ve arşivlerin dokunulmaz olduğunu düzenlemektedir. KİHVS; otuz üçüncü maddesi ile konsolosluk arşiv ve belgelerinin dokunulmazlığını, otuz beşinci maddesi ile konsolosluk haberleşmesinin dokunulmazlığını, elli sekiz ve altmış birinci maddeleri ile fahri

[263] İnsan Hakları Arap Sözleşmesi 21'inci madde ile hakkı, 2'nci madde ile devletlerin sorumluluğunu düzenlemiştir.
[264] ITU Tüzüğü, madde 37.
[265] Ziolkowski, a.g.e., 2013, 434-435.
[266] Paris Konvansiyonu, madde 10*bis*.
[267] TRIPS, madde 39.
[268] WCT, madde 5.
[269] WCT, madde 4.
[270] Devletlere egemenlik alanları ile sınırlı olarak yükümlülükler getirilmiş olsa da bundan espiyonajın yasaklandığı sonucu çıkarılamaz. Nitekim anlaşmalar ve uluslararası platformlarda espiyonaja temas edilmemiştir. Devletlerin, espiyonajı tolere etme durumu kendilerinin de espiyonajdan faydalanması ile açıklanabilir. Ziolkowski, a.g.e., 2013, 436.

konsolosluk memurlarına ilişkin dokunulmazlığı düzenlemektedir. ÖMDS yirmi altı ve yirmi sekizinci maddeleri özel misyonların arşiv, doküman ve haberleşme dokunulmazlıklarını düzenlenmiştir. Malumdur ki teknolojinin sağladığı imkanlar arşiv ve iletişime yeni biçimler kazandırmaktadır. Elektronik posta, bulut depolama veya kabul eden devletin topraklarında bulunan sunucuda depolama gibi şekillerde gerçekleşen arşiv ve iletişim de anılan düzenlemeler kapsamındaki dokunulmazlıktan faydalanacaktır[271].

Diğer taraftan, DİHVS'nin kırk birinci maddesi, KİHVS'nin elli beşinci maddesi ve ÖMDS'nin kırk yedinci maddesi, misyon ve konsolosluk görevlilerinin kabul eden devletin kanun ve düzenlenmelerine saygı göstermesini; misyon ve konsolosluk binalarının misyonun görevleri ile bağdaşmayan işler ile kullanılmamasını düzenlemiştir. Bu itibarla misyon ve konsolosluk personelinin kabul eden devlette istihbarat faaliyeti yürütmeleri DİHVS, KİHVS ve ÖMDS hükümlerinin ihlali olarak değerlendirilebilecektir.

Uluslararası deniz hukuku bağlamında espiyonaj, belirli durumlarda sınırlandırılmıştır. BMDHS'nin on dokuzuncu maddesine göre zararsız geçiş, sahildar devletin barışına, düzenine veya güvenliğine zarar vermeyecek mahiyette olmalıdır. Hangi eylemlerin geçişi zararlı kılacağının belirtildiği ikinci fıkranın (c) bendinde "Sahildar devletin savunmasına veya güvenliğine zarar verecek şekilde bilgi toplanması", (j) bendinde "Araştırma veya ölçüm faaliyetlerinde bulunulması" ve (k) bendinde "Sahildar devletin herhangi bir haberleşme sisteminin veya diğer herhangi bir deniz teçhizat veya tesisinin işleyişini engelleyecek her türlü faaliyette bulunulması" sayılmıştır[272]. Dolayısıyla geçişin zararsız olabilmesi için istihbarat faaliyeti yürütülmemesi de gerekmektedir[273].

[271] Diplomatik dokunulmazlık, dokunulmaz nitelikte olan arşiv, haberleşme veya evrak yönelik espiyonaja yasak getirmemektedir. Ziolkowski, a.g.e., 2013, 444.
[272] Sözleşmenin Türkçe çevirisi için bkz. Adalet Bakanlığı Dış İlişkiler ve Avrupa Birliği Genel Müdürlüğü, Birleşmiş Milletler Sözleşmeleri. https://diabgm.adalet.gov.tr/arsiv/sozlesmeler/coktarafli-soz/bm/bm_26.pdf.
[273] Ziolkowski, a.g.e., 2013, 445.

### 3.2. Siber Espiyonaj ile Yeni Yaklaşımlar

Geleneksel espiyonaj, insanlık tarihi kadar eski bir fenomendir[274]. Siber espiyonaj ise göreceli olarak yeni bir fenomendir[275]. Siber espiyonajın karakteri, bir kısım özelliklerini öne çıkarmaktadır. Geleneksel espiyonaj ile ulaşılması mümkün olmayan veri büyüklüğüne siber espiyonaj ile ulaşılabilir[276]. Günümüzde siber alanın içerdiği veri miktarı tahmin edilememektedir[277]. Siber espiyonaj ve siber saldırının metotlarının benzerliği, birbirlerinden ayırt edilmesini zorlaştırmaktadır[278]. Nitekim her ikisi de hedefin zafiyetlerinden faydalanarak yetkisiz erişim sağlamak suretiyle amaçlarını gerçekleştirmeye yönelmiştir.

Öne çıkan başka bir özellik ise siber espiyonajın uzaktan erişim yoluyla gerçekleştirilebilmesidir. Böylece hedef devletin espiyonajı suç olarak düzenleyerek sağladığı caydırıcılık, etkisini yitirmektedir[279]. Yine siber alanın anonimiteye elverişliliği ve herkes tarafından kolay erişilebilir olması siber espiyonajın maliyetini düşürmektedir. Ayrıca siber espiyonaj ile toplanan veri sadece yetkisiz erişim sağlayanın kontrolünde kalmamakta; dünyaya yayılarak bireyler, kuruluşlar ve demokratik değerler üzerinde kalıcı bir tehdit halini almaktadır[280].

Siber espiyonaj, kendine özgü doğası ile geleneksel espiyonajdan ayrışmaktadır. Uluslararası hukukun uluslararası toplumun yeni ihtiyaçlarına uyum sağlamasını sağlayan soyut ve esnek yapısı[281] siber espiyonaja özel bir yaklaşım sergilenmesine müsaade etmektedir[282]. Bu itibarla geleneksel espiyonaja ilişkin suskunluk veya belirsizlik siber espiyonaj için sürdürülmemelidir. Geleneksel espiyonajdan daha ciddi ve tehlikeli olan siber espiyonajı düzenleyecek ve sınırlayacak uluslararası hukuk imkânlarının değerlendirilmesi gerekmektedir[283].

---

[274] Ziolkowski, a.g.e., 2013, 425.
[275] Buchan, a.g.e., 2015, 170.
[276] Goldsmith, J. (2013). "How cyber changes the laws of war", *European Journal of International Law*, 24(1), 135.
[277] Kilovaty, a.g.m., 2016, 67.
[278] Goldsmith, a.g.m., 2013, 132,135.
[279] Ziolkowski, a.g.e., 2013, 447.
[280] Kilovaty, a.g.m., 2016, 69.
[281] Ziolkowski, a.g.e., 2013, 450.
[282] Kilovaty, a.g.m., 2016, 69.
[283] Kilovaty, a.g.m., 2016, 78.

### 3.2.1. Siber Espiyonaj ve Uluslararası Barış ve Güvenlik

Uluslararası topluluğun kurucu belgesi olan[284] BM Antlaşmasına göre uluslararası ilişkiler, devletlerin egemen eşitliği ilkesine dayanmaktadır[285]. Bu ilke gereği devletler birbirlerinin politik bütünlüğüne ve iç işlerine karışmamalıdır[286]. Devletlerin egemenliği, küresel uygulanabilirliği olan BM Antlaşması ile korunarak devletleri bu düzenlemeye uymaya zorlamaktadır. Bu itibarla uluslararası barış ve güvenlik uluslararası düzenlemeler ile sürdürülmektedir[287].

Diğer taraftan uluslararası barış ve güvenliğin sürdürülebilirliğinde devletlerarası güç dengesinin önemli olduğu ve bu dengenin espiyonaj yoluyla korunduğu savunulmaktadır[288]. Buna göre espiyonaj yoluyla devletler birbirlerinin niyet ve potansiyelleri hakkında bilgi edinerek isabetli karar almakta ve eyleme geçmektedirler. Böylece devletler kendi güçlerini diğer devletlerin güçleri ile dengede tutmak için gerekli bilgiye sahip olmaktadır[289]. Nihayetinde espiyonaj, hedef hakkında faydalı bilgi sağlasa dahi yine de hedef devletin güvenliğine yönelik düşmanca bir eylem olarak uluslararası barış ve güvenliğe tehdit olabilecektir.

Soğuk savaş zamanı uluslararası barış ve güvenlik, silahlı çatışmanın engellenmesi üzerine kurulmuştur[290]. Sovyetlerin dağılmasıyla birlikte barış ve güvenlik anlayışı genişleyerek terörizm, silahlanma yarışı, çevresel ve iklimsel sorunlar, göç, salgın hastalıklar ve insan hakları ihlalleri gibi dünya düzenine yönelik sorunları da kapsamına almıştır[291]. Bu sorunlar ve tehditler, uluslararası kuruluşlar nezdinde devletlerin iş birliğine ve koordinasyonuna yönelik yükümlülük ve sorumluluk getiren uluslararası rejimler veya anlaşmalar vasıtasıyla çözülebilir[292]. Nitekim ulusal sınırları aşan problemler uluslararası iş birliği ile çözülebilir.

Devletlerin taraf oldukları uluslararası rejimler veya anlaşmalar kapsamındaki yükümlülüklerine uyup uymadığının tespiti ve takibi genellikle uluslararası kuruluşlar

---

[284] Fassbender, B. (1998). "The united nations charter as constitution of the international community", *Columbia Journal of Transnational Law*, 36(3), 616.
[285] BM Antlaşması, madde 2.
[286] Judgment; Case Concernıng Military And Paramilitary Activities in and Against Nicaragua, 202.
[287] Buchan, a.g.m., 2015, 175.
[288] Genel olarak bkz. Herman, M. (1996). *Intelligence power in peace and war*. Cambridge University Press.
[289] Herman, a.g.e., 1996, 85.
[290] Baker, a.g.m., 2003, 1112.
[291] Demarest, a.g.m., 1996, 342 vd.
[292] Baker, a.g.m., 2003, 1098-1099.

veya uluslararası mahkemeler vasıtasıyla yapılmaktadır[293]. Ancak devletler bu denetim mekanizmalarını atlatma yolları arayarak ve bularak söz konusu uluslararası rejim veya anlaşmaların etkisini azaltmaktadır[294]. Netice itibarıyla devletlerin taraf oldukları anlaşma veya rejimlere uyup uymadıklarına ilişkin denetim şekli, gerçek durumu ortaya koymakta yetersiz kalmaktadır[295].

Espiyonaj ise gerçek durumu ortaya çıkaran araçların en etkilisidir. Bu kapsamda devletlerin taraf oldukları uluslararası rejimler veya anlaşmalar ile üstlendikleri yükümlülük ve sorumluluklara uyulup uyulmadığının tespitinin espiyonaj yoluyla mümkün olması, devletleri uluslararası barış ve güvenlik için iş birliğine ve diyaloğa teşvik edeceği savunulmuştur[296]. Buna göre uluslararası güvenlik konusunda devletlerin yükümlülüklerinden kaçınmasının sonuçlarının öngörülemez oluşu, devletlerin yükümlülüklerine uyumunu izlemede espiyonaj dahil olmak üzere tüm araçların kullanılmasını gerekli kılmaktadır[297].

Siber espiyonaj da geleneksel espiyonaj gibi uluslararası denetim aracı olarak kullanılmakta ve bir takas dengesi barındırmaktadır[298]. Geleneksel espiyonajda bilginin bedeli, insan veya maddi kaynaklar ya da dostane ilişkinin kaybıdır. Siber espiyonajda da benzer yönde bir takas mevcut olsa dahi insan ve maddi kaynaklara yönelik risklerden kaçınılabilmektedir[299]. Dahası teknik imkân ve kabiliyetlerle sofistike hale getirilen siber espiyonaj, soruşturma ve ilişkilendirmeye yönelik girişimleri de başarısız kılabilmektedir.

Geleneksel espiyonajın sadece espiyonaj olarak kalmayıp saldırı ihtimaline dönüşme durumu siber espiyonaj için de geçerlidir. Keşif uçaklarının silahlar ile donatılarak saldırıda bulunabileceği gibi siber espiyonaj sızmış olduğu sisteme zarar vererek saldırı gerçekleştirebilmektedir. Bu bağlamda siber espiyonajın geleneksel espiyonajdan farklı bir değerlendirmeye tabi tutulmaması gerektiği belirtilmiştir[300]. Buna göre siber espiyonajın saldırıya dönüşme ihtimali bulunduğu sürece ulusların

[293] Buchan, a.g.m., 2015, 176.
[294] Baker, a.g.m., 2003, 1103.
[295] Stone, J. (1962). "Legal Problems of Espionage in Conditions of Modern Conflict*", Essays on Espionage and International Law*, 41.
[296] Baker, a.g.m., 2003, 1112.
[297] Stone, a.g.m., 1962, 41-42.; Baker, a.g.m., 2003, 1113.
[298] Pelican, a.g.m., 2012, 382.
[299] Ziolkowski, a.g.e., 2013, 447.
[300] Pelican, a.g.m., 2012, 385.

birbirilerinin niyetlerini ve faaliyetlerini tespit etmekte yüksek menfaatleri bulunmaktadır. Bu cihetle siber espiyonaj, uluslararası güvenlik ve istikrar yönünden geleneksel espiyonajda olduğu gibi tolere edilmeye devam edilebilir.

Diğer taraftan, veriye yetkisiz erişimin devletlerin egemenlik haklarını ihlal etmekle birlikte uluslararası güven ve barış ortamına zarar vereceği savunulmuştur[301]. Buna göre, devletlerin birbirlerine güven duymadığı bir ortamda iş birliğinde bulunmaları beklenemeyeceği gibi uluslararası barış ve güvenliğe ilişkin konularda uzlaşı sağlanması da beklenemeyecektir. Bu halde espiyonaj, uluslararası barış ve güvenlik için tehdittir[302]. Bu sonuca, espiyonajın devletlerin kritik altyapılarını[303] veya kritik altyapı sektörlerini[304] hedef aldığı senaryoda daha kolay ulaşılacaktır.

Devletler, fiziksel olmayan siber alana egemenliklerini tatbik etmektedir[305]. Dolayısıyla siber alanda yer alan devlete ait varlıklara yönelik siber espiyonaj, devletler nazarında egemenlik haklarının ihlali olarak değerlendirilecektir. Bu itibarla, uluslararası güven ve barış ortamı için geleneksel espiyonajın tehdit olarak değerlendirilmesi siber espiyonaj için geçerli olacaktır. Edward Snowden tarafından sızdırılan NSA belgelerinde ABD'nin Brezilya başkanının ve Brezilya büyükelçiliklerinin telefon görüşmelerini izlediğinin ifşa olması üzerine Brezilya devlet başkanı, ABD'yi protesto etmek için Washington'a planladığı ziyareti iptal etmiş ve BM Genel Kurulunda ABD'yi hedef alarak, siber espiyonaj eylemlerinin diplomatik krize neden olduğunu ifade etmiştir[306].

Geleneksel espiyonaj ve siber espiyonajın uluslararası barış, güvenlik ve iş birliği ortamına yönelik oluşturduğu tehdidin boyutlarının farklı olduğu, siber

---

[301] Buchan, a.g.m., 2015, 177.

[302] 1960 yılında ABD keşif uçağı U-2'nin Sovyetler tarafından düşürülmesi sonrasında doğu ve batı bloklarının yakınlaşması maksadı ile aynı yıl düzenlenmesi planlanan barış zirvesi, ABD'nin istihbarat faaliyeti nedeniyle geçekleşmemiştir. BBC News. '1960: east-west summit in tatters after spy plane row'. http://news.bbc.co.uk/onthisday/hi/dates/stories/may/17/newsid_2512000/2512335.stm.

[303] Ulusal Siber Güvenlik Stratejisi ve Eylem Planında kritik altyapı, *"İşlediği bilginin/verinin gizliliği, bütünlüğü veya erişilebilirliği bozulduğunda can kaybına, büyük ölçekli ekonomik zarara, ulusal güvenlik açıklarına veya kamu düzeninin bozulmasına yol açabilecek bilişim sistemlerini barındıran altyapılar"* şeklinde tanımlanmıştır. Bkz. dipnot 71.

[304] Ulusal Siber Güvenlik Stratejisi ve Eylem Planında kritik altyapı sektörleri, *"kritik altyapıları barındırmakta olan "Elektronik Haberleşme", "Enerji", "Finans", "Ulaştırma", "Su Yönetimi" ve "Kritik Kamu Hizmetleri" sektörleri"* olarak tanımlanmıştır. Bkz. dipnot 71.

[305] Buchan, a.g.m., 2015, 177.

[306] Julian Borger. (2013). "Brazilian president: US surveillance a 'breach of international law'", The Guardian. https://www.theguardian.com/world/2013/sep/24/brazil-president-un-speech-nsa-surveillance.

espiyonajın tehdidin boyutunu artırdığı değerlendirilmektedir[307]. Siber alan daha önce hiç görülmemiş bir ölçekte, hızda, yoğunlukta ve derinlikte espiyonaj için teknolojik bir platform ve hedef bakımından zengin bir ortam sağlar[308]. İnternet ile altın çağını yaşayan siber espiyonaj, uluslararası barış ve güvenlik için tasavvurlardaki halinden daha tehlikeli olup[309] geleneksel espiyonaja gösterilen tolerans siber espiyonaj için azalmaktadır[310].

### 3.2.2. Siber Espiyonaj ve Kuvvet Kullanma Yasağı

Uluslararası teamül hukukunun temel bir ilkesi olan ve bu hukukun yansıması olarak[311] BM Antlaşması ikinci maddesi dördüncü paragrafında yer alan düzenleme, *"Tüm üyeler, uluslararası ilişkilerinde gerek herhangi bir başka devletin toprak bütünlüğüne ya da siyasal bağımsızlığa karşı, gerek Birleşmiş Milletler'in Amaçları ile bağdaşmayacak herhangi bir biçimde kuvvet kullanma tehdidine ya da kuvvet kullanılmasına başvurmaktan kaçınırlar"* hükmünü havidir.

Bağlayıcı nitelikte olmasa dahi yol gösterici olan 1970 tarihli Birleşmiş Milletler Antlaşması uyarınca Devletler Arasında Dostane İlişkiler ve İşbirliğine İlişkin Uluslararası Hukuk İlkeleri Bildirgesi[312] ile mezkûr düzenleme tahlil edilmiştir. Bu tahlilde tespit edilen bir kısım hususlar şunlardır: devletler, barışa karşı işlenen bir suç olan saldırı faaliyetlerinden uluslararası hukuka göre sorumludurlar; saldırı propagandasında bulunmamalıdır; mevcut sınırları değiştirmek için veya uluslararası uyuşmazlıkları çözmek için kuvvet kullanmamalı ya da tehditte bulunmamalıdır; halkları kendi kaderlerine karar verme hakkından yoksun bırakmak amacıyla güç kullanmamalıdır; başka bir devlette iç çatışmaya veya teröre yönelik eylemleri organize etmek, kışkırtmak, desteklemek veya başka bir devletin topraklarını ele geçirmeye yönelik silahlı milislerin oluşumunu teşvik etmekten kaçınmalıdırlar.

---

[307] Ziolkowski, a.g.e., 2013, 463; Buchan, a.g.m., 2015, 178.
[308] Fidler, D. P. (2012). Tinker, Tailor, Soldier, Duqu: Why cyberespionage is more dangerous than you think. International Journal of Critical Infrastructure Protection, 1(5), 29.
[309] Buchan, a.g.m., 2015, 179.
[310] Ziolkowski, a.g.e., 2013, 450.
[311] Judgment; Case Concernıng Military And Paramilitary Activities in and Against Nicaragua, 100.
[312] UN. General Assembly (25th sess. : 1970). "Declaration on Principles of International Law concerning Friendly Relations and Cooperation among States in accordance with the Charter of the United Nations", A/RES/2625(XXV).

BM Antlaşmasının ikinci maddesi dördüncü paragrafı, cana veya mala zarar veren fiziksel eylemler[313] organize bir unsur tarafından gerçekleştirilen silahlı saldırılar olarak anlaşılmış ancak pratikte daha geniş tatbik edilmiştir[314]. Anılan düzenlemenin kapsamı üzerine tartışmalar son bulmamış, günümüzde de devam etmektedir. Örneğin, bir devletin politikalarında değişiklik sağlamak amacıyla açıkça ekonomik baskı kurulması BM Antlaşmasının ikinci maddesi dördüncü paragrafı bağlamında tartışılırken[315] günümüzde siber faaliyetlerin kuvvet kullanma teşkil edip etmediği bu tartışmalara eklenmiştir[316].

Günümüzde devletlerin bilişim sistemlerine ve ağlarına büyük ölçüde bağımlı olduğu malumdur. Dolayısıyla fiziksel zararla sonuçlanmayan bir siber saldırı önemli miktarda hasara veya aksamaya neden olabilecek potansiyeli haizdir[317]. Nitekim sofistike siber saldırıların, konvansiyonel veya kinetik saldırılar ile aynı neticeyi oluşturabilecek kabiliyette olduğu bilinmektedir[318]. Bu itibarla BM Antlaşmasının ikinci maddesi dördüncü paragrafının fiziksel hasar temelli değerlendirilmesi eleştirilmiş ve söz konusu düzenlemenin siber saldırıları da kapsama alacak şekilde yorumlanması gerektiği vurgulanmıştır[319].

NATO Siber Savunma Mükemmeliyet Merkezi tarafından hazırlanan Tallinn Kılavuzu'nda siber operasyonlar kuvvet kullanımı bağlamında incelenmiştir[320]. Buna göre, operasyonda kullanılan aracın geleneksel ya da siber olmasının kuvvet kullanımı

---

313 Brownlie, I. (1963). *International law and the use of force by states*, Oxford University Press, 362.
314 Brownlie, a.g.e., 1963, 361.
315 1973 yılında yaşanan petrol krizinde petrolün bir silah olarak kullanılıp kullanılmadığı ve bunun kuvvet kullanımı oluşturup oluşturmadığına ilişkin olarak bkz. Paust, J. J., & Blaustein, A. P. (1974). "The Arab Oil Weapon--A Threat to International Peace", *The American Journal of International Law*, 68(3).
316 Roscini, M. (2021). "Chapter 14: Cyber operations as a use of force". *In Research Handbook on International Law and Cyberspace*, Edward Elgar Publishing, 233.
317 Siber faaliyetlerin BM Antlaşması çerçevesinden değerlendirilmesi hakkında genel olarak bkz. Schmitt, M. N. (1999). "Computer network attack and the use of force in international law: thoughts on normative framework", *Columbia Journal of Transnational Law*, 37(3).
318 Melnitzky, a.g.m., 2012, 542; ABD ve İsrail ortaklığında gerçekleştirilen Stuxnet adlı siber saldırı, İran'ın nükleer çalışmalarını akamete uğratmak maksadıyla fiziksel saldırı yerine nükleer tesis ağına yerleştirilen solucan yazılımı ile netice alması vakası olarak siber operasyonların kabiliyetini ortaya koyan meşhur bir örnektir. William J. Broad, John Markoff and David E. Sanger. (2011). "Israeli Test on Worm Called Crucial in Iran Nuclear Delay", *The New York Times*. https://www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html#:~:text=They%20say%20Dimona%20tested%20the,make%20its%20first%20nuclear%20arms.
319 Buchan, a.g.m., 2015, 187; Schmitt, a.g.m., 1999, 934-935.
320 Schmitt, a.g.e., 2017, 328 vd.

değerlendirmesi üzerinde rolü yoktur. Kuvvet kullanma eşiğinin aşılıp aşılmadığını belirleyen kullanılan araçtan ziyade operasyonun boyutu/ölçüsü ve etkisidir.

BM Antlaşması, bir operasyonun hangi koşullarda kuvvet kullanma anlamına geldiğinin tespitine ilişkin ölçüt belirlememiştir. Divan, hangi eylemlerin silahlı saldırı olarak değerlendirilebileceğine yönelik etki ve ölçü kriterlerini ortaya koymuştur[321]. Ölçü ve etki kriterleri, bir siber operasyonun kuvvet kullanımı anlamına gelip gelmediğini tespit ederken analiz edilmesi gereken nicel ve nitel kıstasları kapsamaktadır[322]. Bu itibarla siber operasyonların ölçüsü ve etkileri, kuvvet kullanımı niteliğinde olan ve siber olmayan operasyonların ölçü ve etkileri ile mukayese edilerek söz konusu siber operasyonun kuvvet kullanımı anlamına gelip gelmediği tespit edilebilecektir. Diğer bir ifade ile siber operasyonun; konvansiyonel, biyolojik ya da kimyasal silahlar ile yürütülen faaliyetlerin genel olarak neden olduğu etkilerle kıyaslanabilir etkilere neden olması halinde BM Antlaşmasının ikinci maddesi dördüncü paragrafının ihlal edildiği söylenebilecektir[323].

BM Antlaşmasının ikinci maddesi dördüncü paragrafı etki ve ölçü kriterleri ile yorumlandığında hassas ve gizli bilgilere yetkisiz erişim, kuvvet kullanımı olarak değerlendirilebilecektir[324]. Siber espiyonaj ile verilecek zararın boyutunun, fiziksel olarak verilecek zarardan çok daha fazla olabileceği[325] ve hatta işgal düzeyinde olduğu savunulmuş ve siber espiyonajın kuvvet kullanımı olarak değerlendirilmesine imkân sağlayan etki ve ölçü temelli analiz sisteminin uluslararası ihtiyacı karşıladığı belirtilmiştir[326].

Diğer taraftan fiziksel zarara neden olmayan siber espiyonajı kuvvet kullanımı olarak değerlendiren bu görüşe karşı olarak siber espiyonajın kendi başına kuvvet kullanma eşiğini aşamayacağı, dolayısıyla BM Antlaşması sisteminde kuvvet

[321] Judgment; Case Concernıng Military And Paramilitary Activities in and Against Nicaragua, 103-104.
[322] Schmitt, a.g.e., 2017, 331.
[323] Ziolkowski, a.g.e., 2013, 451.
[324] Melnitzky, a.g.m., 2012, 566; Huntley, T. C. (2010). "Controlling the use of force in cyber space: the application of the law of armed conflict during a time of fundamental change in the nature of warfare". *Naval L. Rev*., 60, 39-40; Goldsmith, a.g.m., 2013, 135.
[325] Huntley, a.g.m.,2010, 39.
[326] Melnitzky, a.g.m., 2012, 566.

kullanımı oluşturmayacağı savunulmuştur[327]. Nitekim yetkisiz erişilen verilerin kopyalanması ile konvansiyonel, biyolojik ve kimyasal silahların kullanılmasından doğan etkiler mukayese edilemeyecek mahiyettedir. Tek başına siber espiyonaj kuvvet kullanımı olarak değerlendirilmediğinde doğal olarak silahlı saldırı niteliğini de haiz olmayacaktır[328].

Siber espiyonajın kuvvet kullanımı olarak değerlendirilmesinde hedefin niteliği tartışılmıştır. Devletin ulusal güvenliği için hayati öneme sahip verinin hedef alınması halinde söz konusu operasyonun kuvvet kullanımı oluşturacağı belirtilmiştir[329]. Ötesinde ulusal güvenliğe hizmet eden unsurların hedef alınması halinde verinin niteliği fark etmeksizin kuvvet kullanımı olarak değerlendirilebileceği savunulmuştur[330]. Hedefin niteliği temel alınarak yapılan değerlendirme ile ticari sırlar, fikri mülkiyete ilişkin veriler veya ilgilisince hayati önemde olduğu değerlendirilen tüm verilere yönelik siber espiyonaj, kuvvet kullanımı olarak değerlendirilerek akabinde silahlı çatışmayı veya meşru müdafaa hakkını gündeme getirecektir. Bu bağlamda hedef odaklı yaklaşım siber espiyonaj için kabul edilemez[331]. Aksi halde silahlı çatışma eşiği düşecek ve uluslararası barış ve güvenlik sistemine öznel bir boyut ekleyecektir[332].

Siber espiyonajın kuvvet kullanma tehdidi olarak değerlendirilmesinde, operasyon niyetinin düşmanca olup olmadığı kriter olarak ele alınmıştır[333]. Kuvvet kullanma durumundan daha düşük bir eşiğe sahip olan kuvvet kullanma tehdidi, fiziksel zarar veya açık bir tahribat olmaksızın oluşabilir[334]. Bu yaklaşım özellikle devletin savunma kabiliyetlerine yönelik siber espiyonajın düşmanca niyet içerdiğini kabul etmektedir. Örneğin askeri komuta ve kontrol sistemleri, erken uyarı sistemleri, füze savunma veya nükleer unsurlara ilişkin sistemlere yönelik siber espiyonaj düşmanca niyet ihtiva etmektedir.

---

[327] Wortham, A. (2011). "Should Cyber Exploitation Ever Constitute a Demonstration of Hostile Intent That May Violate UN Charter Provisions Prohibiting the Threat or Use of Force", *Fed. Comm. LJ*, 64, 655; Schmitt, a.g.e., 2017, 335; Buchan, a.g.m., 2015, 188; Ziolkowski, a.g.e., 2013, 452.
[328] Ziolkowski, a.g.e., 2013, 456.
[329] Joyner, C. C., & Lotrionte, C. (2001). "Information warfare as international coercion: Elements of a legal framework", *European Journal of International Law*, 12(5), 855.
[330] Joyner ve Lotrionte, a.g.m., 2001, 856.
[331] Schmitt, a.g.e., 2017, 328, 330, Kural 69; Ziolkowski, a.g.e., 2013, 454.
[332] Ziolkowski, a.g.e., 2013, 454.
[333] Kilovaty, a.g.m., 2016, 69.
[334] Wortham, a.g.m., 2011, 655.

Diğer taraftan tek başına siber espiyonaj, kuvvet kullanma tehdidine işaret etmez[335]. Nitekim siber espiyonaj, gizlilik ve yanıltıcılık ile siber alanın sağladığı kolaylık içerisinde yürütülmektedir. Yine siber espiyonaj, farklı amaçlar ile icra edilebilmektedir. Bu bakımdan siber espiyonajın düşmanca niyet barındırıp barındırmadığına ilişkin yapılacak değerlendirme isabetli olmayacaktır. Yine bu değerlendirme, BM Antlaşmasının ikinci maddesi dördüncü paragrafının ihlal edildiğini tespit edecek ve BM sistemi kapsamında harekete geçilmesine izin verecek ölçüde doğru olmayacaktır. Ancak saldırı hazırlığı kapsamında ulusal savunma veya güvenlik unsurlarına yönelik siber espiyonaj, kuvvet kullanma tehdidi olarak değerlendirilecektir[336].

### 3.2.3. Siber Espiyonaj ve Ülkesel Egemenlik

Fiziksel ve fiziksel olmayan parçalardan oluşan ve fiziki olmayan bir alan olan siber alanda sınırlı olarak ülkesel egemenlik tesis edilmesi mümkündür. Tüm ulusal alanları kapsayan ülkesel egemenlik, başka bir devletin topraklarında fiziksel etkilere neden olan herhangi bir eylemle ihlal edilebilmektedir[337]. Siber alanda ise ülkesel egemenlik, kötü amaçlı faaliyetler ile fiziksel etki oluşturmaksızın ihlal edilebilmektedir[338].

Devletler egemenlik hakları gereği siber alanı hukuki düzenlemeler ile kurala tabi tutmakta ve bu kurallara aykırılık durumunda yargılama yetkisini kullanmaktadır[339]. Bununla birlikte siber alanın fiziksel bileşenleri, devletlerin egemenlik sahalarında yer almaktadır. Fiziksel bileşenler devletler tarafından veya şirketler tarafından üretilmekte ve ayrıca mülkiyete konu olmaktadır. Yine fiziksel bileşenlerin faal olabilmesi ve istikrarlı çalışabilmesi için gerekli olan altyapı devletler veya şirketler tarafından karşılanmaktadır. Her ne kadar siber alanın mimarisi egemenliğin tatbikini zorlaştırsa da, fiziksel ve teknik imkânlar üzerindeki hâkimiyet ve genel olarak siber altyapının bağımlılığı egemenliğin uygulanmasına mani değildir[340].

---

[335] Wortham, a.g.m., 2011, 656; Ziolkowski, a.g.e., 2013, 454.
[336] Kilovaty, a.g.m., 2016, 69-70.
[337] Joyner ve Lotrionte, a.g.m., 2001, 843.
[338] US White House. (2011). International Strategy for Cyberspace. Prosperity, Security and Openness in a Networked Wold, 12; Ziolkowski, a.g.e., 2013, 163.
[339] von Heinegg, a.g.m., 2012, 10.
[340] von Heinegg, a.g.m., 2012, 11.

Bir devletin egemenlik bölgesinde, başka bir devletin egemenliğini kullanması uluslararası hukuk tarafından yasaklanmıştır[341]. Devletin egemenlik bölgesine yetkisiz giriş ve bu bölgenin yetkisiz kullanımı da söz konusu yasak kapsamındadır[342]. Bu bağlamda siber espiyonaj, siber altyapı sistemlerine fiziksel olarak erişimi gerektiriyorsa bu halde devletin ülkesel egemenliği ihlal edilecektir. Örneğin, İngiltere ve ABD'nin iki yüzden fazla transatlantik fiber optik kabloları dinleyerek veri topladığı Tempora adlı siber operasyonda[343] kabloya müdahalenin gerçekleştiği yer bir ülkenin karasuları içerisinde olması durumunda ülkesel egemenliğin ihlalinden bahsedilebilecektir. Fakat müdahale açık denizde gerçekleşmişse ülkesel egemenliğin ihlalinden ilk bakışta bahsedilemeyecektir. Uzaktan yürütülen yani fiziksel olarak bulunma gerektirmeyen ancak fiziksel etkiye neden olan operasyonların ülkesel egemenliği ihlal ettiği kabul edilebilir[344].

Siber espiyonajın gizlilik ve yanıltıcılık ile icra edilmesi esastır. Tabii olarak gizliliğini ortadan kaldıracak fiziksel etkiye neden olması beklenmez. Esasında siber espiyonaj, veriye yetkisiz erişerek veriyi kopyalama ve gizlilik için gerekli önlemlerden oluşur[345]. Bunları yerine getirirken; hedef sistem bırakılan izlerin silinmesi, saklanması, veriye erişim için hedef sistem üzerinde yapılan değişiklikler ve genel olarak verinin modifikasyonu, hedef üzerinde fiziksel bir etkiye neden olmamaktadır[346]. Bu noktada hedef sistemde bulunan verilerin siber espiyonaj kapsamında değiştirilmesi, ülkesel egemenliğin ihlali olarak değerlendirilemeyecektir[347].

Diğer taraftan sistem veya ağa yetkisiz girişin ilgili devletin ülkesel egemenliğini ihlal edebileceği[348] ve hatta izinsiz fiziksel giriş ile izinsiz sanal girişin eş değer olduğu savunulmuştur[349]. Nitekim siber espiyonaj, hedef devletin güvenlik duvarı gibi aldığı önlemler aşılarak ve hedef devletin bilgi teknolojisi altyapısı

[341] The Lotus Case, 18.
[342] Chesterman, a.g.m., 2005, 1082.
[343] Ewen MacAskill, Julian Borger, Nick Hopkins, Nick Davies and James Ball. (2013). "GCHQ taps fibre-optic cables for secret access to world's communications", The Guardian. https://www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa.
[344] von Heinegg, a.g.m., 2012, 16.
[345] Ziolkowski, a.g.e., 2013, 458-459.
[346] Ziolkowski, a.g.e., 2013, 459.
[347] von Heinegg, a.g.m., 2012, 11.
[348] Forcese, a.g.m., 2011, 208; von Heinegg, a.g.m., 2012, 11.
[349] Department of Defense General Counsel. (1999). "An Assessment of International Legal Issues in Information Operations", Washington DC. https://apps.dtic.mil/sti/pdfs/ADB257057.pdf.

kullanılarak gerçekleştirilmektedir. Siber espiyonaj ile bir devlet, hedef devletin siber altyapısı üzerinde egemenlikten kaynaklanan yetkisini tatbik etmektedir. Bu bağlamda fiziksel etkiden bağımsız olarak ülkesel egemenlik ilkesinin koruması kapsamında olan siber altyapı üzerinde başka bir devletin siber espiyonaj yoluyla egemenlik yetkisini icra etmesi hedef devletin ülkesel egemenliğini ihlal edecektir[350].

[350] von Heinegg, a.g.m., 2012, 12.

# 4. SİBER ALANDA MÜDAHALE ETMEME İLKESİ VE SİBER ESPİYONAJ

## 4.1. Genel Olarak Müdahale Etmeme İlkesi

Müdahale kavramı[351], on dokuzuncu yüzyıl başlarına kadar günümüz teknik anlamında kullanılmamış ancak önceki kullanımlarının bugünkü kullanımının kaynağı olduğu değerlendirilmiştir[352]. Hukuki niteliği tartışmalı da olsa ABD'nin 1823 yılında ortaya koyduğu Monroe Doktrini[353] müdahale kavramına yer vermiştir. Buna göre bağımsızlıklarını ilan etmiş devletlere baskı uygulamak veya kaderlerini etkilemeye yönelik müdahalelerin düşmanca bir tutum olarak değerlendirileceği vurgulanmıştır. Monroe Doktrini, sömürgeci devletlerin Amerika Kıtası'nda bağımsızlıklarını yeni kazanan devletlere yönelik faaliyetlerini engellemek bağlamında müdahale kavramına doğrudan temas etmektedir. Ancak müdahale kavramı yalnızca bu bağlam ile sınırlı değildir.

Uluslararası hukukun muğlak konularından bir olan müdahale[354] hakkında; hak olduğu, ihlal olduğu, istisna olduğu veya uluslararası hukuk tarafından izin verilmeyen bir durum olduğu gibi farklı değerlendirmeler yapılmıştır[355]. Nihayetinde müdahalenin uluslararası hukuk tarafından yasaklanmış olduğu ve devletlerin egemen eşitliği ilkesinin bir sonucu olarak[356] müdahale etmemenin kural olduğu kabul edilmiştir[357].

İmparatorluklar, feodal ve dinsel yapılar egemenliği reddetmiş ve dolayısıyla müdahaleyi hak olarak görmüşlerdir. Devletlerin egemen eşitliği ilkesi, 1648 Westfalya Barış Anlaşması akabinde, imparatorluk ve kilise otoritesini egemen devletlerin üzerinde konumlayan sistemin, yerini ülkesel egemenliğin eşit olduğu ve

---

[351] Literatürde sıklıkla *intervention* veya *interference* ve az sayıda eserde *interposition ve meddling* ifadelerinin kullanıldığı görülmüştür. Bu ifadelere karşılık olarak mevcut çalışmada müdahale kelimesi kullanılmaktadır. Diğer taraftan *interference* ifadesi, müdahale etmeme ilkesinin konusunu oluşturmayan diğer bir ifade ile *intervention* boyutuna varmayan karışmalar için kullanan eserler mevcuttur. Jennings R. ve Watts A. (Eds.). (2011), *Oppenheim's International Law. Volume I: Peace* (9th edn), Oxford University Press, 432.

[352] Emerich de Vattel tarafından 1758'de yayımlanan *Le droit des gens* adlı eserde kavramın açık ve kesin kullanılmış ancak müdahale fikrinin daha eski döneme ait olduğu belirtilmektedir. Winfield, P. P. (1922-1923), "The History of Intervention in International Law", British Year Book of International Law, 3, 130; Jamnejad, M., ve Wood, M. (2009), "The principle of non-intervention", Leiden Journal of International Law, 22(2), 349.

[353] Monroe Doctrine. (1823), The U.S. National Archives and Records Administration, https://www.archives.gov/milestone-documents/monroe-doctrine.

[354] Hodges, H. G. (1915), *The doctrine of intervention*, Banner Press, 5.

[355] Winfield, (1922-1923), A.g.m., 134.

[356] Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America), 106.

[357] Jennings ve Watts, a.g.e., 2011, 428.

bu egemenliğin dışsal otoritelerden ari olduğu sisteme bırakmasıyla ortaya çıkmıştır[358]. Dünyada yaşanan gelişmeler, devletlerin egemen eşitliği ilkesini ve dolayısıyla müdahale etmeme ilkesini kaçınılmaz olarak etkilemiştir. Nitekim savaş ve barış arasında bir durumun kabul edilmediği[359] dönemde gerçekleşen müdahaleler savaş olarak değerlendirilirken günümüzde bu şekilde değerlendirilmemektedir. İmparatorluk ve kilise otoritesinin üstün konumu müdahaleyi kural kabul ederken, devletlerin egemen eşitliği ilkesi müdahaleyi istisna kabul etmektedir.

Müdahale, bir devletin iç veya dış işlerine, başka bir devlet veya devletler tarafından karışılmasıdır[360]. Bu bağlamda müdahalenin iç işlere ve dış işlere olmak üzere ikiye ayrılabileceği söylenebilir. Ayrıca bir müdahale çeşidi olarak cezai müdahale de sayılmıştır[361]. Buna göre devletlerin iç işlerine dair aldıkları kararların başka bir devleti etkilemesi sonucunda, etkilenen devletin bu etkiye mukabil hareketi cezai müdahale olarak değerlendirilmiştir. Mevcut durumda cezai müdahale iç işlerine müdahale kapsamındadır. Cezai müdahaleye bir devletin iç işlerine dair aldığı karar neden olmakta ve bu müdahale ile iç işlerine ilişkin alınan karara müdahalede bulunmak amaçlanmaktadır. Diğer taraftan müdahaleyi politik olan ve olmayan olarak tasnif eden çalışmalar da bulunmaktadır[362]. Buna göre politik müdahale, bir devletin itibarına ya da güvenliğine yönelik eylem ve politikalara karşı anlaşmazlıkların bir sonucuyken; politik olmayan müdahale, müdahalede bulunan devletin müdahale edilen devletin egemenliği altında yer alan vatandaşlarını korumaya yöneliktir. Bugünkü durumda akademik çalışmalarda müdahalenin tasnifi yapılmamaktadır. Müdahale etmeme ilkesi, unsurları üzerinden incelenmektedir.

### 4.2. Müdahale Etmeme İlkesinin Kaynakları

Uluslararası teamül hukuku, uluslararası antlaşmalar hukuku ve Divan kararları kapsamında müdahale etmeme ilkesinin kaynakları incelenecektir. Müdahale etmeme ilkesi, çok taraflı ve bölgesel anıtlaşmalarda net olarak ifade edilse de içeriğe ilişkin

[358] Gross, L. (1948), "The Peace of Westphalia, 1648-1948", *The American Journal of International Law*, 42(1), 28; Jamnejad, M., ve Wood, M. (2009), a.g.m., 349.
[359] Grotius savaşı, "uyuşmazlıklarını zorlama yollarına başvurarak çözmeğe çalışanların karşılıklı durumudur" şeklinde tanımlamaktadır. Grotius, H. (1967), *Savaş ve barış hukuku* (Çev. S. L. Meray), Ankara Üniversitesi Siyasal Bilgiler Fakültesi Yayınları No.222-224, 17.
[360] Hodges, a.g.e., 1915, 1.
[361] Winfield, a.g.m., 1922-1923, 143-146.
[362] Hodges, a.g.e., 1915, 19.

aynı netliğe sahip düzenlemeler mevcut değildir. Müdahale etmeme ilkesinin içeriği, uluslararası teamül hukuku ve Divan kararları ile gelişmeye devam etmektedir.

### 4.2.1. Uluslararası Antlaşmalar Hukuku

Müdahale etmeme ilkesi birçok antlaşmaya konu olmuştur. Bölgesel, ikili veya çok taraflı olan bu antlaşmalar müdahale etmeme ilkesine genel ve yüzeysel olarak temas etmiştir.

7'nci Amerikan Devletleri Uluslararası Konferansı'nda kabul edilen 1933 Montevideo Konvansiyonu[363] sekizinci maddesi ile hiçbir devletin başka bir devletin iş veya dış işlerine müdahale hakkına sahip olmadığı düzenlenmiştir. 1948 yılında düzenlenen dokuzuncu Amerikan Devletleri Uluslararası Konferansında kabul edilen Amerika Devletleri Organizasyonu Tüzüğünde (ADOT) de müdahale etmeme ilkesi düzenlenmiştir. Buna göre; ADOT'un hiçbir hükmü katılımcı devletlerin iç işlerine müdahale yetkisi vermemektedir. Ayrıca temsili demokrasinin pekiştirilmesi ve desteklenmesi müdahale etmeme ilkesi gözetilerek sağlanacak, her devlet herhangi bir müdahale olmaksızın dilediği ekonomik, sosyal ve politik sistemi seçebilecektir. Ek olarak hiçbir devlet başka bir devletin iç veya dış işlerine doğrudan veya dolaylı olarak müdahale etme hakkına sahip değildir.

Afrika Birliği Kurucu Anlaşması[364], iç işlerine müdahale edilmemesini bir ilke olarak belirtmiştir. Diğer taraftan Afrika Birliği'nin, üye ülkelerde gerçekleşen savaş suçları, soykırım ve insanlığa karşı suçlar nedeniyle müdahale etme hakkının bulunduğunu belirtmiştir.

BM Antlaşmasının ikinci maddesinin dördüncü ve yedinci fıkraları müdahale etmeme ilkesi bağlamında değerlendirilmektedir. Dördüncü fıkra ile devletlerin, başka bir devletin toprak bütünlüğüne ya da siyasal bağımsızlığına karşı kuvvet kullanma tehdidine ya da kuvvet kullanılmasına başvurmaktan[365] kaçınması gerektiği tanzim

[363] League of Natıons, Treaty Series. (1936), Volume CLXV, No. 3802.
[364] Constitutive Act of African Union, https://au.int/sites/default/files/pages/34873-file-constitutive-act_en.pdf.
[365] Brezilya'nın "örgütün amaçlarına aykırı ekonomik önlem tehdidi veya kullanımının" maddeye eklenmesine dair teklifi reddedilmiştir. Belçika delegesi Brezilya'nın bu teklifine mukabil madde metninde bulunan "başka herhangi bir şekilde" ifadesini işaret etmiştir. Documents of the United Nations Conference on International Organization, San Francisco, 1945, Volume VI, 334-335. https://digitallibrary.un.org/record/1300969.

edilmiştir[366]. Yedinci fıkra ile bu antlaşmanın hiçbir hükmünün üye devletlerin iç işlerine müdahale yetkisini BM'ye vermediği düzenlenmiştir[367]. Ancak BM Antlaşmasının yedinci bölümü kapsamında alınan önlemlerin uygulanmasında anılan ilkenin engel oluşturmayacağı belirtilmiştir[368].

Güneydoğu Asya Ülkeleri Birliği Antlaşması[369], Güneydoğu Asya Ülkeleri Birliği'nin ve üye devletlerin, iç işlerine müdahale etmeme ilkesini ve üye devletlerin ulusal varlığını dış müdahale, yıkıcılık ve zorlayıcılıktan bağımsız şekilde idare hakkına sahip olduğunu düzenlemiştir.

Arap Devletleri Birliği Paktı[370], üye devletlerin hükümet sistemlerini değiştirmeye yönelik eylemlerden kaçınılması gerektiğini ve hükümet sistemlerinin ilgili devletin münhasır meselesi olduğunu belirtmiştir.

DİHVS kırk birinci maddesi, diplomatik ajanları kabul eden devletin iç işlerine müdahale etmeme ile yükümlü kılmıştır[371]. KİHVS elli beşinci maddesi, ÖMDS kırk yedinci maddesi ve 1975 Devletlerin Evrensel Nitelikteki Uluslararası Örgütlerle

[366] Bu tez kapsamında müdahale etmeme ilkesi, siber espiyonajın kuvvet kullanma tehdidi veya kuvvet kullanma boyutunda olmadığının kabulüne paralel olarak, kuvvet kullanma tehdidi veya kuvvet kullanma cihetiyle incelenmemiştir. Bununla birlikte kuvvet kullanma tehdidi veya kuvvet kullanma, müdahale etmeme ilkesini ihlal edecektir. Diğer taraftan kuvvet kullanma tehdidi veya kuvvet kullanmaya ilişkin sistemin bağımsızlaşarak müdahale etmeme ilkesi bağlamında değil, kendi müstakil sistemi içerisinde değerlendirilmesi gerektiği ifade edilmektedir. Buchan, R. and Tsagourias, N. (2017), "The Crisis in Crimea and the Principle of Non-Intervention", *International Community Law Review,* 19 (2-3), 13.

[367] Milletler Cemiyeti Sözleşmesi 15'inci maddesinin sekizinci fıkrasıyla bir uyuşmazlığın ilgili devletin iç işleri kapsamında olduğunun tespit edilmesi durumunda Milletler Cemiyeti Konseyi tarafından tavsiyede bulunamayacağını düzenlemiştir. Covenant Of The League Of Natıons. (1919). https://www.ungeneva.org/en/about/league-of-nations/covenant.

[368] Devlet uygulamaları ışığında anlaşma hükmünün öneminin azaldığı değerlendirilmektedir. Higgins, R. (1965), "The Development Of Internatıonal Law By The Polıtıcal Organs Of The Unıted Natıons". *Proceedings of the American Society of International Law at Its Annual Meeting (1921-1969),* 59; Watson, J. S. (1977), "Autointerpretation, Competence, and the Continuing Validity of Article 2(7) of the UN Charter", *The American Journal of International Law,* 71(1); Jamnejad, M., ve Wood, M. (2009), a.g.m., 362.

[369] Charter of the Association of Southeast Asian Nations. https://asean.org/wp-content/uploads/images/archive/publications/ASEAN-Charter.pdf.

[370] Unıted Nations Treaty Series. (1950), Volume 70, No.241.

[371] Uluslararası Hukuk Komisyonu özel raportörü bu yükümlülüğü, kabul eden devletin hukuku, diplomatik ajanların görevlerinin ifasını engellediği durumlarda diplomatik ajanın kendi inisiyatifi ile kabul eden devletin iç işlerine müdahale etmemesi için düzenlediği yorumunda bulunmuştur. Yearbook of The International Law Commisson. (1957), Volume 1, 143. https://www.un-ilibrary.org/content/books/9789213624487/read.

İlişkilerinde Temsil Edilmesine Dair Viyana Sözleşmesi[372] yetmiş yedinci maddesinde aynı yöndeki düzenlemeye yer verilmiştir.

1949 tarihli Cenevre Sözleşmelerinin iki numaralı ek protokolünün[373] müdahale etmeme kenar başlıklı üçüncü maddesinde, protokolün hiçbir hükmünün bir devletin egemenliğini veya hükümetin sorumluluğunu etkileyecek şekilde kullanılmasına cevaz verilmediği belirtilmektedir. Bu kapsamda topraklarında çatışma meydan gelen devletin, doğrudan ya da dolaylı olarak ve her ne sebeple olursa olsun, iç veya dış işlerine ya da silahlı çatışmasına müdahale edilmesinde iki numaralı ek protokolünün hükümleri gerekçe olarak kabul edilmeyecektir. Aynı hükme; Belirli Silahlara İlişkin Sözleşme'nin iki numaralı ek protokolünün[374] birinci maddesinin beşinci fıkrası ve Silahlı Çatışma Durumunda Kültür Varlıklarının Korunmasına İlişkin 1954 Lahey Sözleşmesi'nin ek iki numaralı protokolünün[375] yirmi ikinci maddesinin beşinci fıkrası yer vermiştir.

Uluslararası Ceza Mahkemesi Roma Statüsü (Roma Statüsü)[376], önsözünde, bu statünün hiçbir hükmünün bir devletin iç işlerine müdahale yetkisi vermediği belirtilmiştir.

İkili antlaşmalar çerçevesinde müdahale etmeme ilkesi dostluk ve iş birliği esaslı antlaşmaların bir ilkesi olarak ortaya konulmaktadır[377]. Bir kısım antlaşmalarda da BM Antlaşması ilkelerinin benimsenmesi nedeniyle[378] dolaylı şekilde müdahale etmeme ilkesinin kabul edildiği varsayılabilecektir.

---

[372] Vienna Convention on the Representation of States in their Relations with International Organizations of a Universal Character (1975). https://legal.un.org/ilc/texts/instruments/english/conventions/5_1_1975.pdf.

[373] Protocol Additional to The Geneva Conventions of 12 August 1949, And Relating To The Protection of Victims of Non-International Armed Conflicts (Protocol II), of 8 June 1977. https://ihl-databases.icrc.org/assets/treaties/475-AP-II-EN.pdf.

[374] Protocol on Prohibitions or Restrictions on the Use of Mines, Booby-Traps and Other Devices as amended on 3 May 1996 (Protocol II to the 1980 CCW Convention as amended on 3 May 1996). https://ihl-databases.icrc.org/assets/treaties/575-IHL-92-EN.pdf.

[375] Unıted Nations Treaty Series. (2005), Volume 2253, A-3511.

[376] Unıted Nations Treaty Series. (2004), Volume 2187, I-38544.

[377] Treaty Of Peace, Frıendshıp And Cooperatıon Between The Government Of Indıa And The Government Of The Unıon Of Sovıet Socıalıst Republıcs, madde 1; Treaty of Friendship, Co-operation and Mutual Assistance Between the Soviet Union and Certain East European Communist Governments, Signed at Warsaw, May 14, 1955.

[378] Basic Treaty of Friendship and Co-operation between Australia and Japan. Madde 2. https://www.dfat.gov.au/geo/japan/basic-treaty-of-friendship-and-co-operation-between-australia-and-japan

### 4.2.2. Uluslararası Teamül Hukuku

Müdahale etmeme ilkesi bağlamında *opinio iuris* ve devlet eylemlerini tam olarak ayrıştırmak mümkün değildir. Sömürgeci devletlerin eski sömürgelerine yönelik müdahaleleri ve aynı zaman sömürgeleriyle mücadele içerisinde olan devletlere yardımları, müdahale etmeme ilkesinin gerekleri ile devlet eylemleri arasında büyük bir fark oluşturmaktadır[379]. Devletler müdahale etmeme ilkesinin ihlalini protesto etse de aynı ihlalde bulunmaları ve ihlallere karşı yaptırım taleplerinin zayıf kalması devlet eylemlerinin tutarsızlığını sürdürmektedir. Bu itibarla, müdahale etmeme ilkesi bağlamında devlet eylemlerinin araştırılması sonuç vermeyecektir[380].

Diğer taraftan müdahale etmeme ilkesine ilişkin olarak BM nezdinde yürütülen faaliyetlerde ortaya konulan görüşlerin ve BM sistemi haricinde olan Helsinki Nihai Senedi'nin *opinio iuris* bağlamında değerlendirilmesi mümkündür.

BM, yirminci yüzyılın ortalarından itibaren müdahale etmeme ilkesine doğrudan veya dolaylı olarak birçok kez temas etmiştir[381]. 1957 öncesinde BM nezdinde yapılan görüşmelerde bir kısım devletler uluslararası hukuk çerçevesinde

---

[379] Devlet eylemleri ile müdahale etmeme ilkesi arasındaki çelişkilerin değerlendirilmesi için bkz. Damrosch, L. (1989), "Politics across borders: nonintervention and nonforcible influence over domestic affairs", *American Journal of International Law*, 83(1).

[380] Jamnejad ve Wood, a.g.m., 2009, 352.

[381] Peaceful and neighbourly relations among States. (1957). A/RES/1236(XII). https://digitallibrary.un.org/record/207248; Declaration on the Inadmissibility of Intervention in the Domestic Affairs of States and the Protection of Their Independence and Sovereignty. (1965). A/RES/2131(XX). https://digitallibrary.un.org/record/203886?ln=en; Status of the implementation of of the Declaration on the Inadmissibility of Intervention in the Domestic Affairs of States and the Protection of Their Independence and Sovereignty. (1966). A/RES/2225(XXI). https://digitallibrary.un.org/record/203172?ln=en; Declaration on Principles of International Law concerning Friendly Relations and Cooperation among States in accordance with the Charter of the United Nations. (1970). A/RES/2625(XXV). https://digitallibrary.un.org/record/202170?ln=en; Charter of Economic Rights and Duties of States. (1970). A/RES/3281(XXIX). https://digitallibrary.un.org/record/190150?ln=en; Non-interference in the internal affairs of States. (1976). A/RES/31/91. https://digitallibrary.un.org/record/187959?ln=en; Non-interference in the internal affairs of States. (1977). A/RES/32/153. https://digitallibrary.un.org/record/187959?ln=en; Economic measures as a means of political and economic coercion against developing countries : resolution / adopted by the General Assembly.(1984). A/RES/39/210. https://digitallibrary.un.org/record/74906?ln=en; Solemn appeal to States in conflict to cease armed action forthwith and to settle disputes between them through negotiations, and to States Members of the United Nations to undertake to solve situations of tension and conflict and existing disputes by political means and to refrain from the threat or use of force and from any intervention in the internal affairs of other States. (1985). A/RES/40/9. https://digitallibrary.un.org/record/106220?ln=en; Respect for the principles of national sovereignty and non-interference in the internal affairs of States in their electoral processes : resolution / adopted by the General Assembly. (1989). A/RES/44/147. https://digitallibrary.un.org/record/82467?ln=en; Necessity of ending the economic, commercial and financial embargo imposed by the United States of America against Cuba: resolution / adopted by the General Assembly. (2007). A/RES/62/3. https://digitallibrary.un.org/record/610595?ln=en.

müdahale etmeme ilkesinin önemine vurgu yapmıştır[382]. Müdahale etmeme ilkesinin BM Genel Kurulunun kararına konu olması ise 1957 tarihli Devletler Arasında Barışçıl ve Komşuluk İlişkileri[383] başlıklı karar ile gerçekleşmiştir. Buna göre BM Antlaşmasının amaçları kapsamında uluslararası barış ve güvenliğin sürdürülebilmesi için devletlerin birbirlerinin iç işlerine müdahale etmemesi gerektiği vurgulanmıştır. 1965 yılında Devletlerin İç İşlerine Müdahalenin Kabul Edilemezliği ve Bağımsızlıklarının ve Egemenliklerinin Korunmasına Dair Bildiri[384] ile devletlerin iç işleri ile dış işlerine de müdahale edilmemesinin gerekliliği teyit edilmiştir[385]. BM Genel Kurulunun sonrasında aldığı kararlar 1957 ve 1965 tarihli kararlarını teyit eder nitelikte olmuştur[386].

BM Genel Kurulunun 1970 yılında aldığı Devletlerarası Dostça İlişkiler ve İşbirliğine Dair Uluslararası Hukuk İlkeleri Hakkındaki Deklarasyon[387] başlıklı kararda, bu deklarasyon ile şekillendirilen BM Antlaşması ilkelerinin uluslararası hukukun temel ilkelerini oluşturduğu belirtilmiştir. Deklarasyon müdahale etmeme ilkesi ile ilgili olarak; ulusların birlikte barış içerisinde yaşayabilmesinin temel şartının devletlerin birbirlerinin işlerine müdahale etmeme yükümlülüğüne uygun eylemlerde bulunması, devletlerin uluslararası ilişkilerinde diğer devletlerin politik bağımsızlığına ya da toprak bütünlüğüne yönelik olarak askeri, siyasi, ekonomik veya başka bir yöntem ile zorlayıcılıktan kaçınılması gerektiği belirtilmiştir.

Yine 1971 Devletlerin Ekonomik Haklar ve Görevleri Bildirgesi[388], devletler arası ilişkilerde ekonomiyle birlikte siyasi ve diğer ilişkilerin yürütülmesinde diğer unsurlarla birlikte müdahale etmeme ilkesinin de gözetileceğini; devletlerin dış müdahale, zorlama veya tehdit olmaksızın siyasal, sosyal veya kültürel sistemlerini belirlemede egemen olduklarını; hiçbir devletin ekonomik, siyasi veya başka bir tür

[382] Twenty-sixth plenary meeting, Saturday, 9 February 1946. A/PV.26. https://digitallibrary.un.org/record/482356?ln=en.
[383] A/RES/1236(XII).
[384] A/RES/2131(XX). Bildirinin Genel Kurul görüşmeleri sırasında ABD, Japonya ve İsrail dahil olmak üzere bir kısım devletler, bu bildiriye dair kararın politik bir niyet beyanı olduğu, hukuksal olmadığı ve devletlere ilişkilerinde yol göstermesi amaçlandığını belirtmiştir. Summary record of the 1423rd meeting : 1st Committee, held at Headquarters, New York, Monday, 20 December 1965, General Assembly, 20th session. 436. https://digitallibrary.un.org/record/800368.
[385] ABD, Divanda görülen Nikaragua davasında 1965 tarihli bildiri ve bu bildiriyi genişleterek teyit eden diğer BM Genel Kurulu kararlarının uluslararası teamül hukukunu ortaya koymadığını savunmuştur. Counter-Memorial of the United States of America. (1984), 94.
[386] A/RES/2225(XXI); A/RES/32/153.
[387] A/RES/2625(XXV).
[388] A/RES/3281(XXIX).

zorlayıcılık ile başka bir devletin egemenlikten kaynaklanan hakların kullanımının sınırlanamayacağını belirtmiştir.

1976[389] ve 1981[390] müdahalenin kabul edilmezliğine dair bildiriler, müdahale etmeme ilkesini tanımlamamakla birlikte kapsama ilişkin tespitlerde bulunmaktadır. 1976 bildirisi gerek ulusların gerekse de sömürülen halkların kendi kaderini tayin hakkından bahsederek müdahale etmeme ilkesine istisna getirmiştir. 1981 bildirisi ise müdahale etmeme ilkesinin kapsamında yer alan yirmi üç tane görev ve yükümlülükleri sıralamıştır. Bu yükümlülük ve görevler arasında belirtilenlerden birkaçı şu şekildedir: devletlerin ve bireylerin bilgiye özgürce erişimine müdahale edilmemesi, devletlerin düşmanca kampanya ve propagandadan kaçınması ve devletlerin müdahale etmeme ilkesinin ihlali ile oluşan durumları tanımama hakkı ve görevi. Bu doğrultuda 1981 bildirisi, müdahale etmeme ilkesinin kapsamını oldukça geniş değerlendirmiştir.

BM sistemi dışında yer alan ancak müdahale etmeme ilkesini konu edinen Helsinki Nihai Senedi[391] katılımcı devletlerin ilişkilerinde gözetilecek ilkeler arasında müdahale etmeme ilkesini saymıştır. Buna göre devletler başka bir devlete yönelik olarak kendi çıkarlarını sağlamak maksadıyla askeri, ekonomik, siyasi veya başka şekilde zorlayıcılıktan kaçınacaktır.

### 4.2.3. Uluslararası Adalet Divanı Kararları

Divan, Korfu Boğazı davası ile müdahale etmeme ilkesini değerlendirme imkânı bulmuştur. İngiltere; kendi kendine yardımda bulunduğunu, iddia olunan suçun maddi unsurunun kaybolmaması ve muhtemel yargılama sürecine delil olarak sunulabilmesi için Korfu Boğazı'ndan mayınları topladığını ve bu durumun müdahaleyi haklı kıldığını savunmuştur. Divan bu savunmaya itibar etmeyerek İngiltere'nin müdahalesini uluslararası hukukta yeri olmayan bir kuvvet politikasının tezahürü olarak değerlendirmiştir[392].

[389] A/RES/31/91.
[390] A/RES/36/103.
[391] Conference On Securıty And Co-Operatıon In Europe Fınal Act, (1975). https://www.osce.org/files/f/documents/5/c/39501.pdf.
[392] Corfu Channel case, Judgment of April 9th, 1949: I.C.J. Reports 1949, P. 4, 34,35.

Nikaragua davası ile müdahale etmeme ilkesi Korfu Boğazı davasına nazaran daha detaylı ele alınmıştır[393]. Divan, müdahale etmeme ilkesinin uluslararası teamül hukukunun bir parçası olduğunu belirtmiş ve egemen devletlerin işlerini müdahaleye uğramadan yönetebilmesi müdahale etmeme ilkesinin kapsamında olduğunu tespit etmiştir. Devletlerin egemen eşitliği ilkesinin doğal sonucu olmasıyla birlikte müdahale etmeme ilkesi, *opinio iuris* ile desteklenmektedir. Divan *opinio iuris* bağlamında BM nezdinde yürütülen çalışmaları kanıt olarak göstermiştir[394].

Müdahale etmeme ilkesinin içeriğine ilişkin tanımlama ihtiyacını belirleyen Divan, Nikaragua davasında bu tanımlamayı yalnızca dava konusu ile ilgili yönleriyle yapmıştır. Her ne kadar Divan müdahale etmeme ilkesinin içeriğine tüm yönleriyle değinmese de ortaya koyduğu esas ile müdahale etmeme ilkesinin özünü belirlemiştir. Buna göre, egemen devletlerin serbestçe karar verebileceği konulara ilişkin doğrudan veya dolaylı zorlayıcılık içeren yöntemler ile müdahale yasaklanmıştır. Zorlayıcılık unsuruna ilişkin olarak Divan dava konusu eylemler yönüyle değerlendirme yapmıştır. Bu bağlamda bölücü ve tahrip edici gruplara veya terörist unsurlara yönelik desteğin ya da doğrudan askeri girişimin, kuvvet kullanma yönü olan bir müdahale olması nedeniyle, zorlayıcılık unsurunun varlığının kuşkusuz olduğu Divan tarafından tespit edilmiştir.

Nikaragua davasında müdahale etmeme ilkesinin kapsamına dair tespitte bulunulan diğer husus ise hükümet karşıtlarının (*internal opposition*) desteklenmesi durumudur. Silahlı güç kullanarak veya kullanmayarak dolaylı veya doğrudan hükümet karşıtlarını destekleyen devlet eylemlerinin sıklığı, bunun müdahaleyi mümkün kılan genel bir hak oluşturup oluşturmadığının değerlendirilmesine neden olmuştur. Divan, hükümet karşıtlarının desteklenmesi amacıyla müdahale hakkının bulunmadığını tespit etmiştir. Müdahale etmeme ilkesinin ihlalinin çeşitli gerekçelerle müdahale hakkı olarak savunulması uluslararası hukuk ile ilgili olmayıp uluslararası politika beyanları olarak değerlendirilmiştir.

[393] Judgment; Case Concerning Military And Paramilitary Activities in and Against Nicaragua, 96-100.
[394] Divan, BM görüşmeleri sırasında 1965 tarihli bildirinin hukuk olarak formüle edilmemesi gerektiğine dair görüş bildiren ABD'li temsilcinin, aynı görüşü 1965 tarihli bildirinin teyidi olan 1970 tarihli bildiriye yönelik olarak bildirmemesine vurgu yapmıştır.

Divan, Kongo Topraklarında Silahlı Faaliyetler davasında[395] Uganda'nın Kongo Demokratik Cumhuriyeti'nin topraklarında bulunan düzensiz unsurlara ekonomik, askeri, mali ve lojistik desteğinin müdahale etmeme ilkesini ihlal ettiğine karar vermiştir.

### 4.3. Müdahale Etmeme İlkesinin Mahiyeti

Uluslararası toplumun ve ilişkilerin temelinde devletlerin egemen eşitliği ilkesi bulunmaktadır[396]. Eşit egemenliğin korunması, egemenliğin farklı yönlerine[397] yönelen müdahalelerden korunması ile mümkündür. Ülkesel egemenlik ilkesi, devletin toprakları üzerindeki egemenliği müdahalelerden korurken[398]; müdahale etmeme ilkesi, devletin iç ve dış işlerinin yönetimine yönelik müdahalelerden korumaktadır[399]. Kuvvet kullanma tehdidi ya da kuvvet kullanma yasağı ile devletlerin toprak bütünlüğü ve siyasal bağımsızlığı korunmaktadır[400].

Uluslararası teamül hukukunun özerk bir ilkesi olan[401] müdahale etmeme ilkesi, her devletin egemenlik, ülkesel bütünlük ve politik bağımsızlık hakkının doğal sonucudur[402]. Gerek BM nezdinde yürütülen çalışmalar gerekse Divan kararları müdahale etmeme ilkesinin uluslararası teamül hukukunun bir parçası olduğunu müteaddit şekillerde ortaya koymuştur[403].

Uluslararası Hukuk Komisyonu müdahale etmeme ilkesinin ihlalinin suç oluşturup oluşturmayacağını değerlendirmiştir. İnsanlığın Barış ve Güvenliğine Karşı Suçlar Kodu Tasarısının ilk sürümünde[404], silahlı kuvvet kullanılmasını suç olarak düzenleyen birinci maddenin görüşmeleri sırasında, silahlı kuvvetin bir devlet üzerinde zorlayıcılık oluşturmak için kullanılması durumunda uluslararası hukuku ihlal edileceği vurgulanarak, daha tehlikeli zorlayıcılık içeren yöntemlerin de madde

[395] Armed Activities on the Territory of the Congo (Democratic Republic of the Congo v. Uganda), Judgment, I.C.J. Reports 2005, p. 168.
[396] BM Antlaşması madde 2(1).
[397] Jennings ve Watts, a.g.e., 2015, 382.
[398] Judgment, Corfu Channel case, 35.
[399] Judgment, Case Concerning Military And Paramilitary Activities in and Against Nicaragua, 106.
[400] BM Antlaşması madde 2(5).
[401] Dissenting Opinion of Judge Sir Robert Jennings, Merits; Case Concerning Military And Paramilitary Activities in and Against Nicaragua, 519.
[402] Jennings ve Watts, a.g.e., 2015, 428.
[403] Müdahale etmeme ilkesinin Viyana Antlaşmalar Hukuku Sözleşmesinin 53'üncü maddesi bağlamında *jus cogens* niteliğinde bir norm olabileceği ileri sürülmüştür. Separate Opınıon Of Judge Sette-Camara, , Merits; Case Concerning Military And Paramilitary Activities in and Against Nicaragua, 189.
[404] Yearbook of The International Law Commisson. (1950), Volume 2, 261 vd.

kapsamına dâhil olması gerektiği teklif edilmiştir[405]. Ancak söz konusu tasarının suçları düzenleyen bir metin olması nedeniyle muğlak ifadelerin yer almaması gerektiği ve zorlayıcılık içeren yöntemlerin sayılması durumunda hariçte kalan yöntemlerin suç oluşturmaması durumunun oluşacağından bahisle teklif reddedilmiştir. Keza Roma Statüsü görüşmeleri sırasında müdahale etmeme ilkesinin ihlalinin suç olarak düzenlenmesi önerilmemiş olup mevcut durumda bu ihlalin uluslararası cezai sorumluluğu olabileceğine dair emare bulunmamaktadır[406].

Müdahale etmeme ilkesinin içeriğine dair uluslararası bir rehber yoktur. Dolayısıyla neyin ya da hangi eylemin müdahale etmeme ilkesini ihlal ettiği birçok unsurları ile değişkendir. Devletler müdahale kavramını, başka devletlerin eylemlerini eleştirmek için özensiz şekilde kullanırken uluslararası hukuk daha katı şekilde değerlendirmektedir[407].

Uluslararası hukuk bir devletin başka bir devletin işlerine yönelik hesaplanan sonuçları elde etmek veya eylemleri dayatmak için zorlayıcılık içeren müdahale ile ilgilenmektedir[408]. Bu itibarla müdahalenin egemenlik ve zorlayıcılık olarak iki unsurdan oluştuğu sonucuna ulaşılabilir[409]. Zorlayıcılık müdahalenin şiddetini tanımlarken egemenlik ise zorlayıcılığın uygulandığı alanı diğer bir ifade ile devletin iç ve dış işlerini tanımlamaktadır.

Zorlayıcılık devletin çıkarlarını sağlama almak veya genişletmek ya da başka bir devletin çıkarlarına zarar vermek gayesini[410] gerçekleştirmeye elverişli yoğunluğa sahip olmalıdır[411]. Devletin iradesinden taviz vermesini sağlayacak dolaylı veya dolaysız birçok yöntem olabilir[412]. İstenen zorlayıcılık seviyesine bağlı olarak askeri,

[405] Yearbook of The International Law Commisson. (1950), Volume 1, 110. Daha tehlikeli zorlayıcılık içeren yöntem olarak ekonomik baskı ifade edilmiştir. Silahlı güç yöntemine başvurulduğunda BM yaptırımlarına maruz kalınırken diğer yöntemlerde ise yaptırım riski bulunmamaktadır.
[406] Jamnejadve Wood, a.g.m., 2009, 359.
[407] Jennings ve Watts, a.g.e., 2015, 432.
[408] Jennings ve Watts, a.g.e., 2015, 430.
[409] Buchan ve Tsagourias, a.g.m., 2017, 171.
[410] McDougal, M. S., & Feliciano, F. P. (1958), "International Coercion and World Public Order: The General Principles of the Law of War", *The Yale Law Journal*, 67(5), 781.
[411] Kunig, P. (2008), "Intervention, prohibition of". *Max Planck Encyclopedia of Public International Law*, 16, 3.
[412] Judgment; Case Concerning Military And Paramilitary Activities in and Against Nicaragua, 108.

ekonomik, diplomatik, ideolojik veya siber[413] yöntemler tek başına veya birlikte kullanılabilir[414].

Müdahale etmeme ilkesine konu müdahale, Divanın Nikaragua davasında belirttiği üzere, devletlerin bağımsız olarak karar vereceği meseleler hakkında olmalıdır. Devletlerin iç ve dış meselelerinde bağımsız karar verebilmesi egemenliğinin bir sonucudur. Egemenlik alanının kapsamı, uluslararası ilişkilerde yaşanan gelişmeler ekseninde hareket etmektedir[415]. Dolayısıyla egemenlikten kaynaklanan imtiyazların tamamıyla belirlenmesi mümkün değildir. Bununla birlikte, müdahale etmeme ilkesine ilişkin kaynaklarda, devletlerin serbestçe karar alabileceği alanlara örnek olarak ekonomik, sosyal, kültürel veya dış politika sayılmıştır.

Müdahale etmeme ilkesi, devletler arasındaki güç dengesinin, güçlünün görece daha güçsüz olana karşı zorlayıcılık içeren yöntemlerle müdahalesi sonucu bozulmamasını; ikna süreçleri veya devletlerin halkları tarafından oluşturulan baskı yoluyla güç değişikliklerinin sağlanmasını teşvik etmektedir[416]. Devletlerin irade çatışmalarında güç dengesine tatbik ettiği zorlayıcılığın yoğunluğu, bu müdahalenin uluslararası hukuka göre değerlendirilmesinde önemlidir. Zorlayıcılığın yoğunluğu, müdahalenin silahlı çatışma, savaş, kuvvet kullanma veya müdahale etmeme ilkesinin ihlali olarak değerlendirilmesine ve buna bağlı sonuçların, meşru müdafaa gibi, oluşmasına neden olacaktır.

### 4.4. Dijital Dönüşümün Müdahale Etmeme İlkesine Etkisi

Dijital dönüşüm öncesi müdahalenin güçlü devletlere mahsus olduğu varsayılırken[417], dijital dönüşüm ile bu varsayım geçerliliğini yitirmektedir. Dijital dönüşüm ile değeri ve önemi her geçen gün artan siber alanda operasyon gerçekleştirmek, fiziksel alana kıyasla daha az kaynak gerektirmektedir[418]. ABD'nin

[413] Buchan ve Tsagourias, a.g.m., 2017, 172
[414] McDougal ve Feliciano, a.g.m., 1958, 792.
[415] Permanent Court Of International Justice, Advisory Opinion No. 4.. (1923), 24. https://www.icj-cij.org/sites/default/files/permanent-court-of-international-justice/serie_B/B_04/Decrets_de_nationalite_promulgues_en_Tunisie_et_au_Maroc_Avis_consultatif_1.pdf.
[416] McDougal ve Feliciano, a.g.m., 1958, 802.
[417] Judgment, Corfu Channel case, 35.
[418] On the Application of International Law in Cyberspace. (2021), The German Federal Government, 1.

2022 yılında yapmış olduğu tehdit değerlendirmesinde[419], siber alanda güçlü olduğu düşünülen Çin ve Rusya ile birlikte İran İslam Cumhuriyeti (İran) ve Kore Demokratik Halk Cumhuriyeti'ne (Kuzey Kore) yer verilmiştir. Buna göre; İran'ın siber operasyonlar yürütme konusundaki artan uzmanlığı ve istekliliği, Kuzey Kore'nin mevcut siber programının karmaşık siber operasyonları içermesinin ABD ve müttefikleri için tehlike oluşturduğu tespit edilmiştir.

Dekolonizasyon sürecinde bağımsızlıklarını yeni kazanan görece güçsüz devletlerin egemenliklerini koruma ve pekiştirme gayretleriyle birlikte egemenlik kavramı önemini artırmıştır. Soğuk savaş sonrası uluslararası hukukun ve özellikle insan hakları hukukunun genişleyerek topluluk çıkarlarını öncelikli olarak destekleyen yapıya dönüşmesi, devlet egemenliğinden kaynaklanan münhasır yetki alanının (*domaine reserve*) ve müdahale etmeme ilkesinin kapsamını ve önemini azaltmıştır[420].

Müdahale etmeme ilkesinin önemini yitirmesinin diğer bir nedeni olarak "popülist hükümetlerin[421]" istismarı gösterilmiştir. Buna göre popülist hükümetler, demokratik hukuk devletinin koşulları olan sivil toplum kuruluşları ve diğer toplumsal hareketlerin yanı sıra özgür medya ve düşünce, toplanma, örgütlenme ve ifade özgürlüğünün ulus ötesi kurumlarca desteklenerek küresel normların sivil toplum aracılığı ile yayılmasını engellemek maksadıyla müdahale etmeme ilkesini kullanmaktadır. Müdahale etmeme ilkesinin popülist devlet imajı taşıması nedeniyle devletlerin bu ilkeye başvurmaktan kaçındığı ve dolayısıyla ilkenin öneminin azalmasına neden olduğu belirtilmiştir[422].

Siber alanın genişlemesi ve bu alandan kaynaklanan tehdit ve tehlikelerin boyutu ve çeşitliliği, müdahale etmeme ilkesini yeniden devletlerin gündemine getirmiştir. Dezenformasyon kampanyaları, seçimlere siber müdahaleler, siber alanda toplum mühendisliği ve istikrarsızlaştırma faaliyetleri dikkatleri müdahale etmeme ilkesinin üzerine çekmiştir[423]. Nitekim 1960 ile 1980 yılları arasında, BM nezdinde

---

[419] 2022 Annual Threat Assessment of the U.S. Intelligence Community, Office of the Director of National Intelligence. https://www.dni.gov/files/ODNI/documents/assessments/ATA-2022-Unclassified-Report.pdf.

[420] Willmer, L. (2023), "Does digitalization reshape the principle of non-intervention?". *German Law Journal*, 24(3), 508.

[421] Popülist hükümet; uzlaşmaz düzen karşıtı tutum, çoğulculuk karşıtı duruş ve dışlayıcı kimlik siyasetinin benimsendiği hükümetler olarak açıklanmıştır. Krieger, H. (2019), "Populist governments and international law". *European Journal of International Law*, 30(3), 975.

[422] Willmer, a.g.m., 2023, 510.

[423] Willmer, a.g.m., 2023, 511.

yürütülen çalışmalarda, müdahale etmeme ilkesine gösterilen ilgi, dijital dönüşümün ivme kazanmaya başladığı 2005 sonrasında da BM'de yapılan çalışmalarda görülmektedir.

### 4.4.1. Siber Alanda Müdahale Etmeme İlkesinin Kabulü

Siber alandaki devlet eylemlerine ilişkin Rusya'nın 1998 yılındaki çağrısı[424] ile başlayan siber alanın regülasyonu tartışmaları, günümüzde mevcut uluslararası kuralların siber alana uygulanması ve ne şekilde uygulanacağı ekseninde yürütülmektedir[425]. Siber alanın regülasyonu ve bu alandaki devlet faaliyetlerine ilişkin ilgi, 2007 yılında Estonya'nın uğradığı siber saldırı ile artmıştır. Uluslararası hukukun ve BM Antlaşmasının siber alan için kabul edilebilir olduğuna dair 2013 tarihli uzmanlar grubu raporu[426] ile oluşan ortak anlayış genişleyerek 2015 tarihli raporda, siber alandaki devlet faaliyetlerinde müdahale etmeme ilkesinin önemine vurgu yapılmıştır[427]. Aynı doğrultuda değerlendirmelere 2021 tarihli raporda[428], BM Genel Kurulunun muhtelif kararlarında[429] ve Açık Uçlu Çalışma Grubunun (Çalışma Grubu)[430] faaliyetlerinde yer verilmiştir.

Kuvvet kullanma eşiğinin altındaki ihlallerin genellikle müdahale etmeme ilkesinin ihlali kapsamında olması sebebiyle devletlerin siber alanın regülasyonuna dair görüşlerinde müdahale etmeme ilkesi esas bağlam olmuştur[431]. Bu itibarla

---

[424] Letter dated 23 September 1998 from the Permanent Representative of the Russian Federation to the United Nations addressed to the Secretary-General. (1998), Russian Federation. A/C.1/53/3.
[425] Adamson, L. (2020), "International Law and International Cyber Norms: A Continuum?", *In Governing Cuberspace: Behavior, Power, and Diplomacy*, edited by Dennis Broeders and Bibi van den Berg, London: Rowman&Littlefield International, 19-43.
[426] Bkz. dipnot 114.
[427] A/70/174, 12.
[428] UN. Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security. A/76/135. https://digitallibrary.un.org/record/3906105?ln=en.
[429] Advancing responsible State behaviour in cyberspace in the context of international security : resolution / adopted by the General Assembly. (2019). UN. General Assembly (73rd sess. : 2018-2019). A/RES/73/266. https://digitallibrary.un.org/record/1658328; Developments in the field of information and telecommunications in the context of international security : resolution / adopted by the General Assembly. (2020). UN. General Assembly (75th sess. : 2020-2021). A/RES/75/240. https://digitallibrary.un.org/record/3896458; Situation of human rights in the Autonomous Republic of Crimea and the city of Sevastopol, Ukraine : resolution / adopted by the General Assembly. (2021). UN. General Assembly (75th sess. : 2020-2021). A/RES/75/192. https://digitallibrary.un.org/record/3896447.
[430]Report of the open-ended working group on security of and in the use of information and communications technologies 2021–2025. (2022). A/77/275. https://documents-dds-ny.un.org/doc/UNDOC/GEN/N22/454/03/PDF/N2245403.pdf?OpenElement.
[431] Willmer, a.g.m., 2023, 510.

uluslararası teamül hukukunun bir parçası olan müdahale etmeme ilkesi, siber alan için kabul edilmiştir ancak uygulanabilirliği belirsizliğini korumaktadır.

### 4.4.2. Siber Alanda Müdahale Etmeme İlkesinin Uygulanabilirliği

Dijital dönüşüm ile müdahale etmeme ilkesinin önemi artmış ve devletler siber alanda ilkenin nasıl uygulanacağına dair görüş birliğine varmaksızın kabulüne dair görüş birliğine varmışlardır. Dijital dönüşüm öncesinde müdahale etmeme ilkesinin muğlak unsurları üzerinde fikir birliği oluşmamıştır. Zorlayıcılık skalasında yasaklı müdahaleye neden olan eşiklerin ne olduğu, hangi meselelere uygulanan zorlayıcılığın devletlerin egemenliğine ilişkin olduğu belirsizliğini sürdürmektedir. Örneğin siyasi ve ekonomik zorlayıcılık olarak tek taraflı ekonomik önlemleri müdahale etmeme ilkesinin ihlali olarak değerlendiren devletler olduğu gibi aksi yönde kanaate sahip devletler de mevcuttur[432].

Müdahale etmeme ilkesinin siber alanda uygulanabilirliğine dair standartların tespitinde, uzmanlar ve çalışma grubunun faaliyetleri kapsamında yapılan tartışmalarda ortaya konulan devlet görüşleri rehberlik edebilir.

#### 4.4.2.1. Tallinn Kılavuzunda müdahale etmeme ilkesinin uygulanabilirliği

Uzmanlar grubu tarafından hazırlanan uluslararası hukuk açısından muteber Tallinn Kılavuzu, mevcut uluslararası kuralların yorumlanarak siber alana tatbikine[433] yönelik rehber niteliğindedir. Tallinn Kılavuzu müdahale etmeme ilkesini, devletlerin iç veya dış işlerine siber araçlarla da müdahale edilemeyeceği şeklinde düzenlemiş ve ilkeyi siber bağlamda detaylı olarak incelemiştir[434].

Uzmanlar grubu müdahale etmeme ilkesinin hatlarının belirsizliğini belirterek ilkenin iki unsuru bulunduğunu kabul etmiştir: Zorlayıcılık ve zorlayıcılığın uygulandığı alan olarak devletin iç ve dış işleri.

İç işlerinin kapsamının, *opinio iuris* ve devlet uygulamalarının tetkiki ile mümkün olduğunu ve zamanla değiştiğini belirtmişlerdir. İç işlerinin kapsamında yalnız devletin kurumları ya da eylemleri değil devletin otoritesinin de bulunduğu

[432] Unilateral economic measures as a means of political and economic coercion against developing countries : resolution / adopted by the General Assembly. (2020), UN. General Assembly (74th sess. : 2019-2020). A/RES/74/200. https://digitallibrary.un.org/record/3847699?ln=zh_CN.
[433] Efrony ve Shany, a.g.m., 2018, 583.
[434] Tallinn Kılavuzu, madde 66, 312-327.

tespit edilmiştir. Devletin otoritesini azaltmaya yönelik müdahaleler de altmış altıncı madde kapsamında olabilecektir. Diğer taraftan siber alana ilişkin devlet eylemlerinin uluslararası hukuka konu edilmesi devletlerin bu alandaki egemenliklerine daraltıcı etki yapacaktır. Müdahale etmeme ilkesinin korumasında bulunan diplomatik ve konsolosluk ilişkilerinin yürütülmesi, devletlerin veya hükümetlerin tanınması, uluslararası kuruluşlara üyelik, antlaşmaların oluşturulması veya katılım sağlanması gibi konular devletin dış işlerine örnek olarak sayılmıştır.

Zorlayıcılık, bir devleti seçme özgürlüğünden yoksun bırakmak amacıyla ve fiziksel güçle sınırlı olmayan eylemdir. Uzmanlar grubu, müdahale etmeme ilkesinin ihlali için zorlayıcılık içeren eylemin yeterli olmadığını, bu eylemin hedef devlet faaliyetlerine veya hedef alınan konuya dair sonuçlara etki edebilecek şekilde tasarlanmış olması gerektiği kanaatindedir. Diğer bir görüşe göre müdahale ile hedeflenen mesele üzerinde ilgili devletin kontrol imkânın azaltılmış olması müdahale etmeme ilkesinin ihlali için yeterlidir.

Siber araçlarla zorlayıcılık içeren müdahaleler ve siber olmayan araçlarla başka bir devletin iç veya dış işleri kapsamında olan siber aktivitelerine müdahale, müdahale etmeme ilkesi kapsamındadır. Müdahale etmeme ilkesinin ihlalinin siber alanda gerçekleşmesi için fiziksel bir sonucun ortaya çıkmasına gerek olmadığı konusunda uzmanlar grubu hemfikirdir. Siber alanda zorlayıcılık içeren ve hedef devletin kararlarını etkilemeyi amaçlayan müdahale eyleminin sonuçlarının siber alan ile sınırlı kalması ihlalin gerçekleşmediği anlamına gelmeyecektir. Örneğin bir devletin siber alanda verdiği hizmetleri kesintiye uğratmaya yönelik siber operasyonlar sonuçlarını siber alanda doğurmaktadır. Bu operasyon hedef devlette eylem değişikliği sağlamak maksadıyla gerçekleştiğinde müdahale etmeme ilkesinin ihlali gündeme gelecektir.

Uzmanlar grubu siber alanda müdahale etmeme ilkesi bağlamında zorlayıcılığı farklı yönleri ile incelemişlerdir. Hedef devletin bir zorlayıcılığa maruz kaldığının farkında olmaması durumunda müdahale etmeme ilkesinin ihlal edilip edilmediği tartışılmış ancak uzlaşı sağlanamamıştır. Yine zorlayıcılık ile ulaşılmak istenen gayenin dolaylı şekilde oluşmasının müdahale etmeme ilkesini ne şekilde etkileyeceği tartışılmıştır.

Zorlayıcılığın yasaklı müdahale oluşturabilmesi için müdahale eden devletin niyetinin zorlama yönünde olması hususunda uzmanlar grubu hemfikirdir. Devletin

eyleminin *de facto* zorlayıcı görünümü *de jure* zorlayıcılık içeren durumlardan ayrıştırılmalıdır. Örneğin bir devletin vatandaşlarının yararına olarak şebekeler üstü hizmetlere[435] yönelik aldığı güvenlik artırıcı kararlar, bu hizmetleri kullanan terörist unsurlar ile mücadele eden devlet perspektifinden terörist unsurlara destek niteliğinde olabilir. Bu halde kendi vatandaşlarının mahremiyetini koruma gayesi ile karar alan devletin zorlayıcılık niyeti bulunmadığından müdahale etmeme ilkesinin ihlalinden bahsedilemeyecektir.

Uzmanlar grubu zorlayıcı siber operasyonun yürütülme amacının ya da ulaşılmak istenen sonucun oluşup oluşmadığının müdahale etmeme ilkesinin ihlali değerlendirilmesinde önemsiz olduğunu belirtmiştir. Diğer bir ifade ile müdahale etmeme ilkesi zorlayıcı siber operasyonun, başarılı olması ile değil tatbik edilmesi ile ihlal edilecektir.

#### 4.4.2.2. Çalışma grubu faaliyetlerinde müdahale etmeme ilkesinin uygulanabilirliği

2020 yılında 5 yıllık süre için kurulan çalışma grubunun görevleri arasında, bilgi ve iletişim teknolojilerinin kullanımında devlet eylemlerine ilişkin normları, ilkeleri veya ek kuralları geliştirmek; bilgi güvenliği ve veri güvenliği alanına uluslararası hukukun nasıl uygulanacağına dair ortak anlayışın oluşmasına katkı sağlamak sayılmıştır[436]. Çalışma grubunun faaliyetleri kapsamında devletler mevcut normlara ve tehditlere ilişkin görüşlerini belirtmişlerdir[437]. Devletler, uluslararası hukuk ilkelerini ve dolaysıyla müdahale etmeme ilkesini siber alan için teyit etmişlerdir.

Diğer taraftan bir kısım devletler genel bir doğrulamanın yanında müdahale etmeme ilkesine dair görüşlerinde detaylı değerlendirme yapmıştır. Ancak bu değerlendirmeler sistematik değil örnek vermek üzerine kurulmuştur. Ukrayna

---

[435] 13.10.2022 tarihli ve 7418 sayılı Kanun ile değişik 5809 sayılı Elektronik Haberleşme Kanununun 3'üncü maddesinin birinci fıkrasının(ççç) bendi şebekeler üstü hizmeti şu şekilde tanımlamıştır: "*şebekeler üstü hizmet: İnternet erişimine sahip abone ve kullanıcılara, işletmecilerden veya sağlanan internet hizmetinden bağımsız olarak kamuya açık bir yazılım vasıtası ile sunulan; sesli, yazılı, görsel iletişim kapsamındaki kişiler arası elektronik haberleşme hizmetlerini,".*

[436] Developments in the field of information and telecommunications in the context of international security : resolution / adopted by the General Assembly. (2020), UN. General Assembly (75th sess. : 2020-2021). A/RES/75/240. https://digitallibrary.un.org/record/3896458.

[437] Report of the Open-ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security. (2021). A/75/816, 24. https://documents-dds-ny.un.org/doc/UNDOC/GEN/N21/068/72/PDF/N2106872.pdf?OpenElement.

seçimlere siber araçlarla müdahalenin uluslararası güvenlik ve politik istikrar için tehdit oluşturduğunu ifade etmiştir[438]. İran, siber alan üzerinden yürütülen dezenformasyon ve algı çalışmaları ile iç işlere müdahale edilerek istikrarsızlaştırma amaçlandığını ve bu durumun sömürgecilik anlayışının farklı bir boyutu olduğunu belirtmiştir[439]. Avustralya devletlerin finansal sistemini istikrarsızlaştıran, seçim sonuçlarını ve parlamento faaliyetlerini manipüle eden siber operasyonların müdahale etmeme ilkesini ihlal ettiğini belirtmiştir[440].

Çalışma grubu faaliyetleri kapsamında ortaya konulan devlet görüşleri, siber alanda müdahale etmeme ilkesinin hatlarını tam olarak ortaya koymamıştır. Ancak müdahale etmeme ilkesinin siber alanda kabul edildiği ve ilkenin daha sık gündeme geleceği anlaşılmıştır.

Uzmanlar grubu ve çalışma grubunun faaliyetleri, müdahale etmeme ilkesinin siber alanda kabul edildiği ancak nasıl uygulanacağına dair belirsizliğin devam ettiğini göstermiştir. Devletler çeşitli vasıtalarla siber alanda müdahale etmeme ilkesinin uygulanabilirliğine dair politikalarını açıklamaya devam etmektedir[441]. Bu politikalar genel olarak uzmanlar ve çalışma grubunun faaliyetleri sonucu oluşan esasların benimseneceğine dairdir. Diğer taraftan Almanya daha somut bir politika ortaya koymuştur. Buna göre siber zorlayıcılığın, etki ve ölçü bakımından fiziksel zorlayıcılık

[438] Statement by the Delegation of Ukraine at the First session of the Open- Ended working group on security of and in the use of ICTs under agenda item 5 (d). https://documents.unoda.org/wp-content/uploads/2021/12/Statement-Ukraine-OEWG-12152021-Threats.pdf.

[439] Statement by Delegation of the Islamic Republic of Iran To the Second Substantive Session of the Open-ended Working Group on Security of and in the Use of information and telecommunications Technologies. https://documents.unoda.org/wp-content/uploads/2022/03/1-Introductory-Remarks-Existing-and-Potential-Threats.pdf.

[440] Australıan Paper – Open Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security, September 2019. https://unoda-web.s3.amazonaws.com/wp-content/uploads/2019/09/fin-australian-oewg-national-paper-Sept-2019.pdf.

[441] International Law applicable in cyberspace. (2022), Government of Canada. https://www.international.gc.ca/world-monde/issues_development-enjeux_developpement/peace_security-paix_securite/cyberspace_law-cyberespace_droit.aspx?lang=eng#a3; International law and cyberspace Finland's national positions. Ministry for Foreign Affairs. https://um.fi/documents/35732/0/KyberkannatPDF_EN.pdf/12bbbbde-623b-9f86-b254-07d5af3c6d85?t=1603097522727; Application of international law to states' conduct in cyberspace: UK statement. (2021), Foreign, Commonwealth & Development Office. https://www.gov.uk/government/publications/application-of-international-law-to-states-conduct-in-cyberspace-uk-statement/application-of-international-law-to-states-conduct-in-cyberspace-uk-statement#contents; On the Application of International Law in Cyberspace. (2021), The German Federal Government.

ile mukayese edilerek, müdahale etmeme ilkesinin ihlalini oluşturacak eşiği geçip geçmediği tespit edilebilecektir.

### 4.5. Siber Espiyonaj ve Müdahale Etmeme İlkesi

Müdahale etmeme ilkesi, egemenlik alanı ve zorlayıcılık olmak üzere iki unsur çerçevesinde değerlendirilmektedir. Siber imkân ve kabiliyetlerle veriye yetkisiz erişimi ve verinin elde edilmesi olarak tanımlanan siber espiyonajın, bu unsurlar bağlamında incelenmesi ile müdahale etmeme ilkesine göre durumu tespit edilebilecektir.

#### 4.5.1. Siber Espiyonaj ve Egemenlik

Müdahale etmeme ilkesinin ihlali için zorlayıcılık, devletin egemenliğinin gereği olarak serbestçe karar verebileceği meselelere ilişkin olmalıdır. Siber espiyonaj bilgiyi hedef almaktadır. Devlet fonksiyonlarının yerine getirilmesinde veri, egemenliğin vazgeçilmez ve ayrılmaz bir parçasıdır[442]. Bu nedenle siber espiyonajın müdahale etmeme ilkesinin unsurlarından olan egemenlik alanına yönelik olduğu kabul edilebilir.

Diğer taraftan bir devlete ait veri, fiziksel olarak başka bir devlet egemenliği altındaki alanda bulunabilir. Nitekim siber alan veri merkezleri ile bilginin saklanmasında ve depolanmasında çeşitli ve geniş imkânlar sunulmaktadır. Başka bir devlet egemenliğindeki alanda bulunan veri üzerinde, bilginin sahibi devletin egemenliğini kullanıp kullanamayacağı önemlidir. Doğu Timor Demokratik Cumhuriyetinin (Doğu Timor) başvurusu üzerine Divan[443], benzer bir duruma ilişkin değerlendirmelerde bulunmuştur. Avustralya'da bulunan ve Doğu Timor için hukuk danışmanlığı hizmeti veren Avusturyalı avukatın ofisinde bulunan Doğu Timor ile Avustralya arasındaki mevcut ve müstakbel müzakereler ile ilgili materyallere, Avustralya Güvenlik İstihbarat Organizasyonu Yasası kapsamında el konulmuştur. Avustralya'nın bu eylemi hakkında Doğu Timor, egemenliğinin ve uluslararası hukuk ve iç hukuk kapsamında mülkiyet ve diğer haklarının ihlal edildiğini belirterek ihtilaf

[442]Buchan, a.g.m., 2016, 76; Irion, K. (2012), "Government cloud computing and national data sovereignty". *Policy & Internet*, 4(3-4), 53. Yazar ayrıca ulusal egemenliğin sağlanabilmesi için veri egemenliğinin sağlanması gerektiği ve hatta kritik bilgileri başka bir devlet tarafından kontrol edilen devletin sömürge olacağını belirtmiştir.

[443] Questions relating to the Seizure and Detention of Certain Documents and Data (Timor-Leste v. Australia). https://www.icj-cij.org/case/156.

hakkında Divana başvurmuştur. Divan, Avustralya'nın eyleminin Doğu Timor'un egemenlik haklarını ihlal ettiği iddiasını makul *(plausible*) bulmuş[444] ve geçici tedbir olarak Avustralya'nın Doğu Timor ve hukuk danışmanları arasındaki iletişime müdahale etmemesine karar vermiştir[445].

Ait olduğu devletten başka bir devletin topraklarında muhafaza edilen veya altyapısı ile aktarılan bilgi, ait olduğu devletin "ulusal veri egemenliğine[446]" sahiptir[447]. Bu veriye yönelik siber espiyonaj, fiziksel olarak kontrolünde olmayan ancak veriye egemen olan devletin egemenliğine müdahale niteliğinde olabilecektir.

### 4.5.2. Siber Espiyonaj ve Zorlayıcılık

Devletin egemenlik alanına uygulanan zorlayıcılığın diktatörce olması durumunda müdahale etmeme ilkesinin ihlalinden bahsedilebilecektir[448]. Zorlayıcılık, bir devletin karar ve seçimlerinde hareket özgürlüğünü kısıtlaması durumunda diktatörce olacaktır[449]. Zorlayıcılığın şiddetine ilişkin bu yorum, siber espiyonajın müdahale etmeme ilkesi bağlamında değerlendirilmesinde sonuca doğrudan katkı sağlamaktadır. Gizlilik içerisinde yürütülmesi esas olan siber espiyonaj, ele geçirilen verinin ne şekilde kullanıldığıyla ya da başka bir eylemin hazırlık hareketi olup olmadığıyla ilgilenmemektedir. Doğal olarak siber espiyonajın zorlayıcılık unsuru barındırmadığı sonucuna ulaşılacaktır[450].

---

[444] Questions relating to the Seizure and Detention of Certain Documents and Data (Timor-Leste v. Australia), Provisional Measures, Order of 3 March 2014, I.C.J. Reports 2014, 153.
[445] Provisional Measures, 161. 2015 yılında Doğu Timor yargılamanın sonlandırılması isteğinde bulunması üzerine Divan davanın listeden kaldırılmasına karar vermiştir. Bu nedenle ihtilafa ilişkin nihai karar verilememiştir.
[446] Irion, a.g.m., 2012, 41.
[447] Heintschel von Heinegg, W. (2013), "Territorial sovereignty and neutrality in cyberspace", *International Law Studies,* 89(1), 130.
[448] Quincy, W., Stone, J., Richard, F. A., & Roland, S. J. (1962), *Essays on Espionage and International Law*. Ohio State University Press, 4.
[449] Jamnejadve Wood, a.g.m., (2009), 347-348; Jennings ve Watts, a.g.e., (2015), 432; Buchan,a.g.m., 2016, 77.
[450] Ziolkowski, a.g.e., 2013, 433; Gill, T. D., & Ziolkowski, K. (2013). "Non-intervention in The Cyber Context", Peacetime Regime for State Activities in Cyberspace International Law, International Relations and Diplomacy. NATO CCDCOE, Tallinn, 8; Peters, A. (2013). "Surveillance without Borders? The Unlawfulness of the NSA-Panopticon", Part II. *Ejil Talk! Blog of the European Journal of International Law*; Talliinn Kılavuzu siber espiyonajın kendi başına uluslararası hukuku ihlal etmeyeceğini belirtmiştir. Tallinn Kılavuzu, madde 32.

Diğer taraftan müdahale etmeme ilkesinin ihlali olabilecek zorlayıcılık eşiğinin daha aşağıda konumlandırılarak geniş yorumlanması gerektiği savunulmuştur[451]. Buna göre nasıl ki devletin fiziksel egemenliğine sıkı bir koruma sağlayan ülkesel egemenlik geniş yorumlanıyorsa, devletin siyasal bütünlüğünü koruyan müdahale etmeme ilkesi de geniş yorumlanmalıdır. Bu bağlamda devletin otoritesini azaltan veya otoriteden taviz verilmesini sağlayan devlet eylemlerinin, müdahale etmeme ilkesini ihlal edecek nitelikte, zorlayıcı olduğunun kabulü gerekir.

Devlet eylemlerinin müdahale niteliği, bir ucunda zorlayıcılığın en yoğun hali olan askeri zorlayıcılık diğer ucunda ise basit müdahale eyleminin bulunduğu spektrum üzerinden değerlendirilmiştir[452]. Spektrumda hangi noktanın müdahale etmeme ilkesinin ihlal eşiği olduğunun tespiti ilk bakışta mümkün değildir. Bu nedenle başka kriterlere başvurulması gerekmektedir. Zorlayıcılığın sonuçları üzerinden yapılan değerlendirme[453] ile yoğunluk temelli zorlayıcılık anlayışının ötesine geçilebilir[454]. Bununla birlikte düşük yoğunluklu zorlayıcılık içeren eylemler, devletin yetki alanını ihlal ediyorsa müdahale etmeme ilkesinin ihlali de gündeme gelecektir[455].

Nikaragua davasında Divanın, müdahale etmeme ilkesini mevcut uyuşmazlık bağlamında değerlendirmesi ve ilkenin kapsamının mezkûr uyuşmazlıkla sınırlı olmadığına yönelik tespiti müdahale etmeme ilkesinin geniş yorumunu desteklemektedir[456]. Bu bağlamda ve Nikaragua davasında ortaya konulan kriterler kapsamında siber espiyonajın müdahale etmeme ilkesinin ihlalini oluşturacak zorlayıcılığa sahip olduğu sonucuna ulaşılacaktır[457]. Nitekim siber espiyonaj ile

[451] Terry, P. C. (2018). "'Don't Do as I Do'—The US Response to Russian and Chinese Cyber Espionage and Public International Law", *German Law Journal*, 19(3), 620 vd.; 1965 Devletlerin İç İşlerine Müdahalenin Kabul Edilemezliği ve Bağımsızlıklarının ve Egemenliklerinin Korunmasına Dair Bildiri ve aynı şekilde 1970 Devletlerarası Dostça İlişkiler ve İşbirliğine Dair Uluslararası Hukuk İlkeleri Hakkındaki Deklarasyon'da yer alan "*Hiçbir Devlet, egemenlik haklarının kullanılmasının başka bir Devlete bırakılmasını sağlamak ve ondan herhangi bir çıkar elde etmek amacıyla, ekonomik, siyasi veya diğer türden tedbirleri kullanamaz veya kullanılmasını teşvik edemez"* ifadesinin, müdahale etmeme ilkesinin geniş yorumlanmasını teşvik ettiği belirtilmiştir. Buchan, a.g.m., 2016, 78.

[452] Higgins, R. (2012). Themes and Theories, Selected Essays, Speeches and Writings in Internati-onal Law, Volume 1, Oxford Academic., 272-283.

[453] Zorlayıcılığın sonuçları, etkilenen devlet çıkar ve menfaatlerin önemi ve sayısı; bu çıkar ve menfaatlerin ne ölçüde etkilendiği ve çıkar ve menfaatleri etkilenen devlet sayısı olmak üzere üç boyut tespit edilmiştir. McDougal ve Feliciano, a.g.m., 1958, 779.

[454] Watts, a.g.m., 2014, 9.

[455] Higgins, a.g.e., 2012, 275.

[456] Beim, J. (2018) "Enforcing a Prohibition on International Espionage,", *Chicago Journal of International Law*, 18(2), 654; Terry, a.g.m., 2018, 620-621.

[457] Terry, P. C. (2020), ""The Riddle of the Sands" Peacetime Espionage and Public International Law", *Georgetown Journal of International Law*, 51(2), 32.

devletler, iç ve dış politikalarını belirleme ya da egemen oldukları bilgilerin kimler tarafından bilinmesine veya açıklanıp açıklanmayacağına karar verme yetkisinden yoksun kalmaktadır[458].

[458] Terry, a.g.m., 2015, 197.

## 5. SONUÇ

Devletlerin politika oluşturma süreçlerinin elzem parçası olan istihbarat, espiyonaj sonucu elde edilen verinin analizidir. Espiyonaj, verinin yetkisiz erişim yoluyla ele geçirilmesidir. Espiyonajın bir bütün olarak gizlilik içerisinde yürütülmesi esastır. Diğer bir ifade ile hedef, espiyonaja maruz kaldığının farkında olmamalıdır. Espiyonaj, verinin gizliliğine yönelik olup verinin bütünlüğü veya yok edilmesiyle ilgilenmemektedir. Aksi halde espiyonaj gizliliğini kaybetmekle birlikte bir araç veya hazırlık hareketi olacaktır. Bu halde espiyonaj müstakil olarak değerlendirilemeyecektir. Nitekim espiyonajın araç veya hazırlık hareketi olarak kullanıldığı durumlarda amaca esas eylemle ayrıştırılarak bağımsız ve isabetli bir değerlendirme yapılması mümkün olmamaktadır.

Siber espiyonaj, siber alanda siber imkân ve kabiliyetler kullanılarak gerçekleştirilen espiyonajdır. Siber alanda yığılan verinin boyutu siber espiyonajın cazibesini artırmaktadır. Geleneksel espiyonaj siber espiyonaja göre daha maliyetli ve sonuçları yönünden daha az tercih edilebilirdir. Bu durum, espiyonaj faaliyetlerinin siber alana kaymasına neden olmaktadır. Ayrıca siber alanın sağladığı kolay ve ucuz imkânlar siber espiyonaja başvurulma sıklığını da artırmaktadır.

Siber alanda devlet eylemlerinin uluslararası hukuka konu edilmesi talebine olan katılımcı sayısı, devletlerin bu alanda kendileri aleyhine yaşanan gelişmelerin artışına paralel olarak artmıştır. Çok taraflı yeni bir anlaşma ile siber alanda devlet eylemlerinin düzenlenmesi fikri yerini mevcut uluslararası hukukun siber alana tatbik edilmesi fikrine bırakmıştır. Günümüzde devletler mevcut uluslararası hukuk kurallarının siber alana uygulanabilir olduğu konusunda ortak görüşe varmışlardır.

Geleneksel espiyonaj ve daha yeni bir fenomen olan siber espiyonaj hakkında uluslararası hukuk kasıtlı olarak sessizlik içerisindedir. Uluslararası hukuktan daha uzun süredir var olan espiyonaj fenomenine ilişkin bu sessizliği ve belirsizliği giderme amacıyla sunulan çözümler, genel bir uygulamaya dönüşecek düzeyde kabul görmemiştir. Ancak siber espiyonajın geleneksel espiyonaja nazaran daha tehditkâr ve tehlikeli oluşu uluslararası hukuk çerçevesinde siber espiyonajın daha az müsamaha ile değerlendirilmesine neden olmuştur.

Espiyonajın uluslararası hukuka göre meşruiyeti tartışmalıdır. Uluslararası hukukta espiyonaja izin veren veya yasaklayan bir düzenleme bulunmamaktadır. Bu

nedenle uluslararası hukukun kaynakları espiyonaj ve siber espiyonaj bağlamında yorumlanmıştır. Espiyonajın uluslararası hukuka göre meşru olduğu ve olmadığı değerlendirmeleri denge içerisindedir. Dolayısıyla geleneksel ve siber espiyonajın uluslararası hukuka göre meşruluk sorununa net bir cevap verilememektedir.

Uluslararası barış ve güvenliğin sürdürülebilmesi ve uluslararası toplumun bir ihtiyacı olarak uluslararası hukukun espiyonaj konusundaki belirsizliği siber espiyonaj için devam etmemelidir. Siber espiyonaj uluslararası teamül hukukunun bir ilkesi olan müdahale etmeme ilkesi kapsamında değerlendirilerek belirsizliğin giderilmesine katkı sağlanmış olacaktır.

Müdahale etmeme ilkesi, devletlerin meselelerinde irade özgürlüğünü korumaktadır. İlkenin iki unsuru bulunmaktadır: irade özgürlüğünü sınırlayan veya ortadan kaldıran ölçekte zorlayıcılık, devletin karar ve seçim özgürlüğünün bulunduğu egemenlik alanı. Egemenlik alanının kapsamı uluslararası hukuk ve ilişkilerdeki gelişime ve dönüme bağlı olarak değişmektedir. Dolayısıyla egemenlik alanının kapsamı net olarak belirlenememektedir. İlkenin ihlaline neden olacak zorlayıcılık eşiği belirsizdir. Bu noktada uluslararası hukukun belirsizliğinin giderilmesinde içeriği ve sınırları tam olarak belli olmayan müdahale etmeme ilkesi ile katkı sağlama çabasının sonuçsuz kalacağı düşünülebilir. Ancak müdahale etmeme ilkesinin bu durumu ona yeni ihtiyaçlara cevap verebilecek esnekliği sağlamaktadır.

Siber espiyonaj, gizli kalmasına ya da kimlerin erişebileceğine karar verilen veriye erişim sağlayarak onu ele geçirmeyi amaçlamaktadır. Siber espiyonajın bu amacı müdahale etmeme ilkesinin egemenlik unsuru yönünden belirsizlik içermemektedir. Devlet egemen olduğu veri hakkında karar almaktadır. Diğer bir ifade ile veri hakkında karar alınabilmesi devletin egemenlik hakkının bir sonucudur. Bu halde hakkında gizliliğine veya kimlerin erişebileceğine karar verilebilen veri, kararı alan devletin egemenlik alanındadır.

Diğer taraftan veri, ait olduğu devletin haricinde başka bir devletin topraklarında bulunabilir. Bu durumda verinin fiziksel olarak bulunduğu devletin egemenlikten kaynaklanan yetkilerini veriye tatbik etmesi gündeme gelebilecektir. Verinin ait olduğu ve verinin fiziksel olarak bulunduğu devletlerin hangisinin egemenliğine öncelik verileceği belirsizdir. Kanaatimce verinin fiziksel olarak başka bir devletin egemenlik alanına girişinin şekline bakılarak karar verilmelidir. Verinin

başka bir devletin egemenlik alanına fiziksel olarak taşınması verinin sahibi devletin rızası ile olmuşsa aksine bir antlaşma olmadığı sürece kural olarak verinin fiziksel olarak bulunduğu devletin egemenliğinin daha üstün olduğu kabul edilmelidir. Aksi durumda, fiziksel olarak başka devletin egemenlik alanına verinin ait olduğu devletin rızası olmadan taşınması halinde, en başından itibaren verinin sahibi olan devletin egemenliği ihlal edildiğinden veri üzerinde başka bir egemenlik iddiası makbul olmayacaktır.

Siber espiyonajın müdahale etmeme ilkesinin ihlaline neden olacak zorlayıcılık eşiği yönünden durumu egemenlik alanına göre daha belirsizdir. Müdahale etmeme ilkesine konu devlet eylemlerinin icbar niteliği, egemen bir devletin kabul etmeyeceği eylemleri veya almayacağı kararları almasına neden olacak boyutta olması gerektiği kabul edilirse, yani zorlayıcılık dar yorumlanırsa siber espiyonajın zorlayıcılıktan yoksun olduğu sonucuna ulaşılabilir. Diğer taraftan, siyasal bağımsızlığı sınırlandıran veya yok eden devlet eylemleri zorlayıcı olarak kabul edilirse, yani zorlayıcılık geniş yorumlanırsa siber espiyonajın gerekli zorlayıcılığa sahip olduğu sonucuna ulaşılabilir.

Netice olarak siber espiyonajın müdahale etmeme ilkesinin ihlaline neden olacak zorlayıcılığa sahip olmadığına ulaşılmıştır. Elbette siber espiyonajın devletin otoritesini azaltıcı bir etkisi vardır. Ancak bu etki zorlayıcı değildir. Nitekim siber espiyonaj ile bir devleti bir şey yapmaya veya yapmamaya zorlamak amaçlanmamaktadır. Yine siber espiyonaj sonucunda veri gizliliğini yitirmekte ve belki de hedef devlet bunun farkında bile olmamaktadır. Siber espiyonajın gizliliği esas alan doğası zorlayıcılıktan uzaktır. Bu itibarla siber espiyonajın müdahale etmeme ilkesini ihlal etmeyeceği sonucuna ulaşılmıştır. Ancak bu sonuç siber espiyonajın izin verilen bir devlet eylemi olduğu anlamına gelmemektedir. Veriye ilişkin devlet kararlarını ortadan kaldıran siber espiyonajın müdahale etmeme ilkesinin de kaynağı olan devletlerin egemen eşitliği ilkesinin ihlali olarak değerlendirilmesi mümkündür.

## KAYNAKÇA


Adamson, L. (2020). "International Law and International Cyber Norms: A Continuum?", *Governing Cyberspace: Behaviour, Power and Diplomacy*, 19-44.

Baker, C. D. (2004). "Tolerance of International Espionage: Functional Approach". *American University International Law Review*, 19(5), 1091-1114.

Barlow, J. (2019-2020). "Declaration of the Independence of Cyberspace", *Duke Law & Technology Review*, 18, 5-7.

Beim, J. (2018). "Enforcing a Prohibition on International Espionage", *Chicago Journal of International Law*, 18(2), 647-672.

Bendovschi, A. (2015). "Cyber-Attacks – Trends, Patterns and Security Countermeasures", *Procedia Economics and Finance*, 28, 24-31.

Broeders, D., L. Adamson and R. Creemers. (2019). "Coalition of the Unwilling? Chinese and Russian Perspectives on Cyberspace", *The Hague Program For Cyber Norms Policy Brief*, 1-20.

Brownlie, I. (1963). *International Law and the Use of Force by States*, Oxford University Press.

Buchan, R. (2015). "Cyber Espionage and International Law", *In Research Handbook on International Law and Cyberspace*, 168-189.

Buchan, R. (2016), "The International Legal Regulation of State-Sponsored Cyber Espionage", *In International Cyber Norms: Legal, Policy & Industry Perspectives.* Osula, A. M., & Rõigas, H. (Eds.), NATO Cooperative Cyber Defence Centre of Excellence, 65-86.

Buchan, R. and Tsagourias, N. (2017). "The Crisis in Crimea and the Principle of Non-Intervention", *International Community Law Review*, 19 (2-3), 165-193.

Burk, D. L. (1995). "Federalism in Cyberspace", *Conn. L. Rev.*, 28, 1095-1136.

Chesterman, S. (2005). "The Spy Who Came in from the Cold War: Intelligence and International Law", *Mich. J. Int'l L.*, 27, 1071-1130.

Choucri, N., & Clark, D. D. (2013). "Who Controls Cyberspace?", *Bulletin of the Atomic Scientists*, 69(5), 21-31.

Clark, D. D. (2010). "Characterizing Cyberspace: Past, Present and Future", *MIT Political Science Department*, 1-18.

Damrosch, L. (1989). "Politics Across Borders: Nonintervention and Nonforcible İnfluence over Domestic Affairs", *American Journal of International Law*, 83(1), 1-50.

Deibert, R. J., Rohozinski, R., Manchanda, A., Villeneuve, N., ve Walton, G. M. F. (2009). "Tracking GhostNet: Investigating a Cyber Espionage Network", *Munk Centre for International Studies*, 1-53.

Delupis, I. (1984). "Foreign Warships and Immunity for Espionage*", the American Journal of International Law*, 78(1), 53-75.

Demarest, G. B. (1996). "Espionage in International Law", *Denver Journal of International Law and Policy*, 24(2), 321-348.

Efrony, D., & Shany, Y. (2018). "A Rule Book on the Shelf? Tallinn Manual 2.0 on Cyberoperations and Subsequent State Practice", *American Journal of International Law*, 112(4), 583-657.

Egan, B. J. (2017). "International Law and Stability in Cybershpace", *Berkeley J. Int'l L.*, 35, 169-180.

Ensafi, R., Winter, P., Mueen, A., & Crandall, J. R. (2015). "Analyzing the great firewall of china over space and time". *Proc. Priv. Enhancing Technol.*, 2015(1), 61-76.

Evans M.D.(Editör). (2010). *International Law*, Oxford University Press.

Fassbender, B. (1998). "The United Nations Charter as Constitution of the İnternational Community", *Columbia Journal of Transnational Law*, 36(3), 529-619.

Fidler, D. P. (2012). "Tinker, Tailor, Soldier, Duqu: Why Cyberespionage is More Dangerous Than You Think", *International Journal of Critical Infrastructure Protection*, 1(5), 529-619.

Finnemore, M., ve Hollis, D. B. (2020). "Beyond Naming and Shaming: Accusations and International Law in Cybersecurity", *European Journal of International Law*, 31(3), 969-1003.

Forcese, C. (2011). "Spies without Borders: International Law and Intelligence Collection", *Journal of National Security Law & Policy*, 5(1), 179-210.

Garcia-Mora, M. R. (1964). "Treason, Sedition and Espionage as Political Offenses Under the Law of Extradition", *U. Pitt. L. Rev.*, 26, 65-98.

Gill, T. D., & Ziolkowski, K. (2013). "Non-intervention in the Cyber Context", *Peacetime Regime for State Activities in Cyberspace International Law, International Relations and Diplomacy*. NATO CCDCOE, Tallinn, 217-238.

Goldsmith, J. (2013). "How Cyber Changes the Laws of War", *European Journal of International Law*, 24(1), 129-138.

Goldsmith, J. L. (1998). "Against Cyberanarchy", *The University of Chicago Law Review*, 65(4), 1199-1250.

Gross, L. (1948). "The Peace of Westphalia, 1648-1948", *The American Journal of International Law*, 42(1), 20-41.

Grotius, H. (1967). (Çev. S. L. Meray). *Savaş ve Barış Hukuku (De Iure Belli Ac Pacis*). Ankara Üniversitesi Basımevi.

Hardy, I. T. (1993). "The Proper Legal Regime for Cyberspace", *U. Pitt. L. Rev.*, 55, 993-1056.

Hathaway, O. A., Crootof, R., Levitz, P. ve Nix, H. (2012). "The Law of Cyber-attack", *Calif. L. Rev.* 100(4), 817-885.

Heintschel von Heinegg, W. (2013). "Territorial Sovereignty and Neutrality in Cyberspace", *International Law Studies*, 89(1), 123-156.

Herman, M. (1996). *Intelligence Power in Peace and War*. Cambridge University Press.

Higgins, R. (1965). "The Development of International Law by the Political Organs of the United Nations". *In Proceedings of the American Society of International Law at its annual meeting* (1921-1969), 59, 116-124.

Higgins, R. (2012). *Themes and Theories, Selected Essays, Speeches and Writings in International Law, Volume 1*, Oxford Academic.

Hodges, H. G. (1915). *The Doctrine of Intervention*, Banner Press.

Huang, Z., & Mačák, K. (2017). "Towards the International Rule of Law in Cyberspace: Contrasting Chinese and Western Approaches", *Chinese Journal of International Law*, 16(2), 271-310.

Huntley, T. C. (2010). "Controlling the Use of Force in Cyber Space: The Application of the Law of Armed Conflict During Time of Fundamental Change in the Nature of Warfare", *Naval Law Review*, 60(1), 1-40.

Irion, K. (2012). “Government Cloud Computing and National Data Sovereignty”. *Policy & Internet*, 4(3-4), 40-71.
Jamnejad, M., ve Wood, M. (2009). “The Principle of Non-intervention”, *Leiden Journal of International Law*, 22(2), 345-381.
Jennings R. ve Watts A. (Eds.). (2011). *Oppenheim's International Law. Volume I: Peace (9th edn)*, Oxford University Press.
Johnson, D. R., & Post, D. (1996). “Law and Borders: The Rise of Law in Cyberspace”, *Stanford Law Review*, 48(5), 1367-1402.
Joyner, C. C., & Lotrionte, C. (2001). “Information Warfare as International Coercion: Elements of a Legal Framework”, *European Journal of International Law*, 12(5), 825-865.
Jupillat, N. (2016). “From the Cuckoo's Egg to Global Surveillance: Cyber Espionage That Becomes Prohibited Intervention”, *NCJ Int'l L.*, 42, 933-988.
Kara, I. (2022). “Cyber-Espionage Malware Attacks Detection and Analysis: A Case Study”, *Journal of Computer Information Systems*, 62(6), 1253-1270.
Kilovaty, I. (2016). “World Wide Web of Exploitations-The Case of Peacetime Cyber Espionage Operations Under International Law: Towards a Contextual Approach”, *Colum. Sci. & Tech. L. Rev.*, 18(1), 42-78.
Kraska, J. (2015). “Putting Your Head in the Tiger's Mouth: Submarine Espionage in Territorial Waters”, *Colum. J. Transnat'l L.*, 54(1), 164-247.
Krieger, H. (2019). “Populist Governments and International Law”. *European Journal of International Law*, 30(3), 971–996.
Kunig, P. (2008). “Intervention, Prohibition of”. *Max Planck Encyclopedia of Public International Law*, 16.
Lessig, L. (2003). “Law Regulating Code Regulating Law”, *Loyola University Chicago Law Journal*, 35(1), 1-14.
Lin, H. (2011). “Responding to Sub-Threshold Cyber Intrusions: A Fertile Topic for Research and Discussion”, *Georgetown Journal of International Affairs*, 127-135.
Lubin, A. (2020). “The Liberty to Spy”, *Harv. Int'l LJ*, 61(1), 185-244.
Mačák, K. (2017). “From Cyber Norms to Cyber Rules: Re-engaging States as Law-makers”, *Leiden Journal of International Law*, 30(4), 877-899.
McDougal, M. S., & Feliciano, F. P. (1958). “International Coercion and World Public Order: the General Principles of the Law of War”, *The Yale Law Journal*, 67(5), 771-846.
McDougal, M. S., Lasswell, H. D., ve Reisman, W. M. (1972). “The İntelligence Function and World Public Order”, *Temp. LQ*, 46(3), 365-448.
Melnitzky, A. (2012). “Defending America Against Chinese Cyber Espionage through the Use of Active Defenses”, Cardozo Journal of International and Comparative Law, 20(2), 537-570;
Merritt, D., & Mullins, B. (2011). “Identifying Cyber Espionage: Towards a synthesis Approach”. *In the Proceedings of the 6th International Conference on Information Warfare and Security*, 180-187.
Murphy, T. (2010). “Security Challenges in the 21st Century Global Commons”, *Yale Journal of International Affairs*, 5(2), 28-43.
Navarrete, I., ve Buchan, R. (2018). “Out of the Legal Wilderness: Peacetime Espionage, International Law and the Existence of Customary Exceptions”, *Cornell Int'l LJ*, 51(4), 897-953.

Ottis, R. (2008). “Analysis of the 2007 Cyber Attacks Against Estonia from the Information Warfare Perspective”, *In Proceedings of the 7th European Conference on Information Warfare*, 163-174.

Paust, J. J., & Blaustein, A. P. (1974). “The Arab Oil Weapon--A Threat to International Peace”, *The American Journal of International Law*, 68(3), 410–439.

Perina, A. H. (2014). “Black Holes and Open Secrets: the Impact of Covert Action on International Law”, *Colum. J. Transnat'l L.*, 53(3), 507-583.

Peters, A. (2013). “Surveillance without Borders? the Unlawfulness of the NSA-Panopticon”, *Part II. Ejil Talk! Blog of the European Journal of International Law*.

Pfluke, C. (2019). “A History of the Five Eyes Alliance: Possibility for Reform and Additions”, *Comparative Strategy*, 38(4), 302-315.

Pun, D. (2017). “Rethinking Espionage in the Modern Era”, *Chicago Journal of International Law*, 18(1), 353-391.

Quincy, W., Stone, J., Richard, F. A., & Roland, S. J. (1962). *Essays on Espionage and International Law*. Ohio State University Press.

Radsan, A. (2007). “The Unresolved Equation of Espionage and International Law”, *Michigan Journal of International Law*, 28(3), 595-623.

Raymond, D., Cross, T., Conti, G., & Nowatkowski, M. (2014). “Key Terrain in Cyberspace: Seeking the High Ground”, *In 2014 6th International Conference On Cyber Conflict, IEEE*.

Reisman, W. M., Reisman, W. M. R., William Michael, R., ve Baker, J. E. (1992). *Regulating Covert Action: Practices, Contexts, and Policies of Covert Coercion Abroad in İnternational and American Law*. Yale University Press.

Rivera, R., Pazmiño, L., Becerra, F., & Barriga, J. (2022). “An Analysis of Cyber Espionage Process”, *In Developments and Advances in Defense and Security: Proceedings of MICRADS 2021*, 3-14.

Roscini, M. (2014). *Cyber Operations and the Use of Force in İnternational Law*, Oxford University Press.

Roscini, M. (2021). "Cyber Operations as a Use of Force". *In Research Handbook on International Law and Cyberspace*, Edward Elgar Publishing, 297-316.

Sander, B. (2019). “The Sound of Silence: International Law and the Governance of Peacetime Cyber Operations”, *In 2019 11th International Conference on Cyber Conflict (NATO CCD COE Publications)*, 361-381.

Schmitt, M. (2012). “Classification of Cyber Conflict”, *Journal of Conflict and Security Law*, 17(2), 245-260.

Schmitt, M. (2017). *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations (2nd ed.)*, Cambridge University Press.

Schmitt, M. N. (1999). “Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework”, *Columbia Journal of Transnational Law*, 37, 885-937.

Schmitt, M. N., & Vihul, L. (2014). “The Nature Of İnternational Law Cyber Norms”, *Tallinn Papers*, 5.

Scott, R. D. (1999). “Territorially Intrusive Intelligence Collection and International Law”, *Air Force Law Review*, 46, 217-226.

Shull, A. (2013). “Cyber Espionage and International Law”, *In GigaNet: Global Internet Governance Academic Network*, Annual Symposium.

Sloan, L. D. (2001). “ECHELON and the Legal Restraints on Signals Intelligence: A Need for Reevaluation”, *Duke Law Journal,* 50(5), 1467-1510.
Smith, J. H. (2007). “Keynote Address”, *Mich. J. Int'l L*, 28(3), 543-552.
Stone, J. (1962). “Legal Problems of Espionage in Conditions of Modern Conflict”, *Essays on Espionage and International Law*, 29-44.
Sulmasy, G., & Yoo, J. (2006). “Counterintuitive: Intelligence Operations and International Law”, *Mich. J. Int'l L.*, 28, 625-633.
Terry, P. C. (2015). “Absolute Friends: United States Espionage against Germany and Public International Law”, *Revue Quebecoise de Droit International*, 28(2), 173-204.
Terry, P. C. (2018). “‘Don't Do as I Do’—The US Response to Russian and Chinese Cyber Espionage and Public International Law*”, German Law Journal*, 19(3), 613-626.
Terry, P. C. (2020). “"The Riddle of the Sands" Peacetime Espionage and Public International Law”, *Georgetown Journal of International Law*, 51(2), 377-414.
Todd, G. H. (2009). “Armed Attack in Cyberspace: Deterring Asymmetric Warfare with an Asymmetric Definition”, *AFL Rev.,* 64(1), 65-102.
Tondini, M. (2018). “Espionage and International Law in the Age of Permanent Competition”, *Military Law and Law of War Review*, 57(1), 17-58.
Totic, M. (2022). “The Importance and Role of Espionage at the International Level”, *International Journal of Economics and Law*, 12(35), 227-242.
von Heinegg, W. H. (2012). “Legal Implications of Territorial Sovereignty in Cyberspace”, *In 2012 4th International Conference on Cyber Conflict (CYCON 2012)*, 1-13.
Wallace, D. A., McCarthy, A. H., ve Visger, M. (2018). “Peeling Back the Onion of Cyber Espionage after Tallinn 2.0.”, *Md. L. Rev.,* 78(2), 205-246.
Warner, M. (2002). “Wanted: A Definition of Intelligence”, *Studies in Intelligence*, 46(3), 15-22.
Watson, J. S. (1977), “Autointerpretation, Competence, and the Continuing Validity of Article 2(7) of the UN Charter”, *The American Journal of International Law*, 71(1), 60-83.
Watt, E. (2017). *Cyberspace, Surveillance, Law and Privacy*. PhD thesis University of Westminster Law.
Waxman, M. C. (2011). “Cyber-Attacks and the Use of Force: Back to the Future of Article 2(4)”, *Yale J. Int'l L.*, 36(2), 421-460.
Weissbrodt, D. (2013). “Cyber-Conflict, Cyber-Crime, and Cyber-Espionage”, *Minnesota Journal of International Law*, 22(2), 347-387.
Willmer, L. (2023). “Does Digitalization Reshape the Principle of Non-Intervention?”. *German Law Journal*, 24(3), 508-521.
Winfield, P. P. (1922-1923). “The History of Intervention in International Law”, *British Year Book of International Law*, 3, 130-149.
Wolfrum, R. (1983). “The Principle of the Common Heritage of Mankind”, *Heidelberg Journal of International Law*, 43(2), 312-337.
Wolfrum, R. (2011). “Sources of International Law”, *Max Planck Encyclopedia of Public International Law,* 9, 299-313.
Wortham, A. (2011). “Should Cyber Exploitation Ever Constitute a Demonstration of Hostile Intent That May Violate UN Charter Provisions Prohibiting the Threat or Use of Force”, *Fed. Comm. LJ,* 64(3), 643-660.

Wu, T. S. (1997). "Cyberspace Sovereignty--the Internet and the International System", *Harvard Journal of Law & Technology*, 10(3), 647-666.
Ziolkowski, K. (Ed.). (2013). *Peacetime Regime for State Activities in Cyberspace: International Law, İnternational Relations and Diplomacy*. NATO Cooperative Cyber Defence Centre of Excellence, Tallinn.

## İNTERNET KAYNAKLARI

"2022 Annual Threat Assessment of the U.S. Intelligence Community", Office of the Director of National Intelligence. https://www.dni.gov/files/ODNI/documents/assessments/ATA-2022-Unclassified-Report.pdf.
"African Union Convention on Cyber Security and Personal Data Protection". (2014). https://au.int/sites/default/files/treaties/29560-treaty-0048_-_african_union_convention_on_cyber_security_and_personal_data_protection_e.pdf.
"Agreement on Cooperation in Ensuring International Information Security between the Member States of the SCO". (2009). http://eng.sectsco.org/documents/.
"Application of international law to states' conduct in cyberspace: UK statement". (2021), Foreign, Commonwealth & Development Office. https://www.gov.uk/government/publications/application-of-international-law-to-states-conduct-in-cyberspace-uk-statement/application-of-international-law-to-states-conduct-in-cyberspace-uk-statement#contents.
"Basic Treaty of Friendship and Co-operation between Australia and Japan". https://www.dfat.gov.au/geo/japan/basic-treaty-of-friendship-and-co-operation-between-australia-and-japan.
"Birleşmiş Milletler Sözleşmeleri", Adalet Bakanlığı Dış İlişkiler ve Avrupa Birliği Genel Müdürlüğü, https://diabgm.adalet.gov.tr/arsiv/sozlesmeler/coktaraflisoz/bm/bm_26.pdf.
"Constitutive Act of African Union", https://au.int/sites/default/files/pages/34873-file-constitutiveact_en.pdf.
"Convention (IV) respecting the Laws and Customs of War on Land and its annex: Regulations concerning the Laws and Customs of War on Land". The Hague, https://ihl-databases.icrc.org/applic/ihl/ihl.nsf/Article.xsp?action=openDocument&documentId=090BE405E194CECBC12563CD005167C8.
"Covenant Of the League Of Natıons". (1919). https://www.ungeneva.org/en/about/league-of-nations/covenant.
"Declaration of Principles Building the Information Society: a global challenge in the new Millennium". WSIS-03/GENEVA/DOC/4-E. https://www.itu.int/net/wsis/docs/geneva/official/dop.html; Geneva Plan of Action, WSIS-03/GENEVA/DOC/0005. https://www.itu.int/net/wsis/docs/geneva/official/poa.html.
"Declaration on Principles of International Law concerning Friendly Relations and Cooperation among States in accordance with the Charter of the United Nations". (1970). A/RES/2625(XXV). https://digitallibrary.un.org/record/202170?ln=en.

"Declaration on the Inadmissibility of Intervention in the Domestic Affairs of States and the Protection of Their Independence and Sovereignty". (1965). A/RES/2131(XX). https://digitallibrary.un.org/record/203886?ln=en.

"Follow-up to the World Summit on the Information Society and review of the Commission on Science and Technology for Development", UN. Economic and Social Council (2006, substantive sess. : Geneva). E/RES/2006/46. https://www.un.org/en/ecosoc/docs/2006/resolution%202006-46.pdf.

"Intelligence Services Act 1994", https://www.legislation.gov.uk/ukpga/1994/13/section/1.

"International law and cyberspace Finland's national positions", Ministry for Foreign Affairs. https://um.fi/documents/35732/0/KyberkannatPDF_EN.pdf/12bbbbde-623b-9f86-b254-07d5af3c6d85?t=1603097522727.

"International Law applicable in cyberspace". (2022). Government of Canada. https://www.international.gc.ca/world-monde/issues_development-enjeux_developpement/peace_security-paix_securite/cyberspace_law-cyberespace_droit.aspx?lang=eng#a3.

"Memorandum of understanding between the US Department of Commerce and Internet corporation for assigned names and numbers", https://www.icann.org/resources/unthemed-pages/icann-mou-1998-11-25-en.

"Operation Aurora", Council on Foreign Relations. https://www.cfr.org/cyber-operations/operation-aurora.

"Second Report on Identification of Customary International Law, Identıfıcatıon Of Customary Internatıonal Law", U.N. Doc. A/CN.4/672, https://legal.un.org/ilc/documentation/english/a_cn4_672.pdf.

"USC/ICANN Transition Agreement", https://www.icann.org/resources/unthemed-pages/usc-icann-transition-2012-02-25-en

Advancing responsible State behaviour in cyberspace in the context of international security : resolution / adopted by the General Assembly. (2019). UN. General Assembly (73rd sess. : 2018-2019). A/RES/73/266. https://digitallibrary.un.org/record/1658328.

Armed Activities on the Territory of the Congo (Democratic Republic of the Congo v. Uganda), https://www.icj-cij.org/case/116.

Australıan Paper – Open Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security, September 2019. https://unoda-web.s3.amazonaws.com/wp-content/uploads/2019/09/fin-australian-oewg-national-paper-Sept-2019.pdf.

Bangladesh Government's e-Government Computer Incident Response Team. "Sowbug: targets South American and Southeast Asian governments [source: symantec]". https://www.cirt.gov.bd/sowbug-cyber-espionage-group-targets-south-american-and-southeast-asian-governments-source-symantec/.

BBC News. "1960: east-west summit in tatters after spy plane row". http://news.bbc.co.uk/onthisday/hi/dates/stories/may/17/newsid_2512000/2512335.stm.

BBC. (2014). "Edward Snowden: Leaks that exposed US spy programme", https://www.bbc.com/news/world-us-canada-23123964.

Bussell, J. (2013). "Cyberspace". Encyclopedia Britannica. https://www.britannica.com/topic/cyberspace.

Centre for the Protection of National Infrastructure. (2021). "Espionage". https://www.cpni.gov.uk/espionage.

Charter of Economic Rights and Duties of States. (1970). A/RES/3281(XXIX). https://digitallibrary.un.org/record/190150?ln=en; Non-interference in the internal affairs of States. (1976). A/RES/31/91. https://digitallibrary.un.org/record/187959?ln=en.

Charter of the Association of Southeast Asian Nations. https://asean.org/wp-content/uploads/images/archive/publications/ASEAN-Charter.pdf.

Chris McGreal ve Bobbie Johnson. (2010). "Hillary Clinton criticises Beijing over internet censorship", The Guardian, https://www.theguardian.com/world/2010/jan/21/hillary-clinton-china-internet-censorship.

Commıttee On Formatıon Of Customary (General) Internatıonal Law. (2000). "Fınal Report Of the Commıttee Statement Of Prıncıples Applıcable To the Formatıon Of General Customary Internatıonal Law, Internatıonal Law Associatıon", https://www.law.umich.edu/facultyhome/drwcasebook/Documents/Documents/ILA%20Report%20on%20Formation%20of%20Customary%20International%20Law.pdf

Conference On Securıty And Co-Operatıon In Europe Fınal Act, (1975). https://www.osce.org/files/f/documents/5/c/39501.pdf.

Corfu Channel (United Kingdom of Great Britain and Northern Ireland v. Albania), https://www.icj-cij.org/case/1.

Council Of Europe, "The Budapest Convention and its Protocols" https://www.coe.int/en/web/cybercrime/the-budapest-convention.

Cybersecurity Resource Center. "What Happened". https://www.opm.gov/cybersecurity/cybersecurity-incidents/.

David Drummond. (2010). "Statement from Google: A new approach to China", the Washington Post. https://www.washingtonpost.com/wp-dyn/content/article/2010/01/12/AR2010011202903.html?tid=a_inl_manual.

Defense Advanced Research Projects Agency. "ARPANET". https://www.darpa.mil/about-us/timeline/arpanet.

Department of Defense General Counsel. (1999). "An Assessment of International Legal Issues in Information Operations", Washıngton DC. https://apps.dtic.mil/sti/pdfs/ADB257057.pdf.

Department Of Defense, "Dıctıonary Of Mılıtary And Associated Terms". 60. https://apps.dtic.mil/sti/pdfs/AD1029823.pdf.

Developments in the field of information and telecommunications in the context of international security : resolution / adopted by the General Assembly. (2020). UN. General Assembly (75th sess. : 2020-2021). A/RES/75/240. https://digitallibrary.un.org/record/3896458.

Developments in the field of information and telecommunications in the context of international security : resolution / adopted by the General Assembly. (2020), UN. General Assembly (75th sess. : 2020-2021). A/RES/75/240. https://digitallibrary.un.org/record/3896458.

Documents of the United Nations Conference on International Organization, San Francisco, 1945, Volume VI, https://digitallibrary.un.org/record/1300969.

Economic measures as a means of political and economic coercion against developing countries : resolution / adopted by the General Assembly. (1984). A/RES/39/210. https://digitallibrary.un.org/record/74906?ln=en.

European Parliament. "REPORT on the existence of a global system for the interception of private and commercial communications (ECHELON

interception system) (2001/2098(INI))". https://www.europarl.europa.eu/comparl/tempcom/echelon/pdf/rapport_echelon_en.pdf.
Ewen MacAskill, Julian Borger, Nick Hopkins, Nick Davies and James Ball. (2013). "GCHQ taps fibre-optic cables for secret access to world's communications", The Guardian. https://www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa.
Finkle J. (2011). "Q+A: Massive cyber attack dubbed "Operation Shady RAT", Reuters. https://www.reuters.com/article/us-cyberattacks-qa-idUSTRE7720IS20110803.
Frank J. Prial. (1981). "Soviet Sub Spends Sixth Day Grounded On Swedish Coast", the New York Times, https://www.nytimes.com/1981/11/02/world/soviet-sub-spends-sixth-day-grounded-on-swedish-coast.html.
Frontline. (2003). "Interview with James Lewis". https://www.pbs.org/wgbh/pages/frontline/shows/cyberwar/interviews/lewis.html
Gallagher, S. (2022). "Conti and karma actors attack healthcare provider at same time through proxyshell exploits", Sophos News. https://news.sophos.com/en-us/2022/02/28/conti-and-karma-actors-attack-healthcare-provider-at-same-time-through-proxyshell-exploits/.
Goldsmith, J. (2011). "What is the government's strategy for the cyber-exploitation threat?", Lawfare. https://www.lawfareblog.com/what-governments-strategy-cyber-exploitation-threat.
Government Communications Headquarters."A Brief History of the UKUSA agreement". https://www.gchq.gov.uk/information/brief-history-of-ukusa
Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security. (2013). A/68/98. https://digitallibrary.un.org/record/753055.
Hall, C. H. (2011). "Operational Art in the Fifth Domain", Joint Military Operations Department, https://apps.dtic.mil/sti/pdfs/ADA546255.pdf.
IBM. "Cost of a Data Breach Report 2021", https://www.ibm.com/security/data-breach.
Internet Corporation for Assigned Names and Numbers, https://www.icann.org/get-started.
Internet Corporation for Assigned Names and Numbers. (2014). "The IANA Functions in 180 Seconds" .(Video). Youtube. https://www.youtube.com/watch?v=D__mAX-2sXo.
Internet Governance Forum, https://www.intgovforum.org/en.
Julian Borger. (2013). "Brazilian president: US surveillance a 'breach of international law'", The Guardian. https://www.theguardian.com/world/2013/sep/24/brazil-president-un-speech-nsa-surveillance.
K. Thakur, M. L. Ali, N. Jiang and M. Qiu, "Impact of Cyber-Attacks on Critical Infrastructure," 2016 IEEE 2nd International Conference on Big Data Security on Cloud (BigDataSecurity), IEEE International Conference on High Performance and Smart Computing (HPSC), and IEEE International Conference on Intelligent Data and Security (IDS), 2016. https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7502286.
Legality Of the Threat Or Use Of Nuclear Weapons, Advisory Opinion of 8 July 1996, https://www.icj-cij.org/case/95.

Letter dated 12 September 2011 from the Permanent Representatives of China, the Russian Federation, Tajikistan and Uzbekistan to the United Nations addressed to the Secretary-General (2011). A/66/359. https://digitallibrary.un.org/record/710973.

Letter dated 23 September 1998 from the Permanent Representative of the Russian Federation to the United Nations addressed to the Secretary-General. (1998), Russian Federation. A/C.1/53/3, https://digitallibrary.un.org/record/261158.

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 (2015). A/69/723. https://digitallibrary.un.org/record/786846.

Lipton E., Sanger D. E. ve Shane S. (2016). "The Perfect Weapon: How Russian Cyberpower Invaded the U.S.", the New York Times. https://www.nytimes.com/2016/12/13/us/politics/russia-hack-election-dnc.html.

LoGiurato B. (2013). "Former French Foreign Minister Nails It On the Outrage Over US Spying On Foreign Leaders", Insider. https://www.businessinsider.com/nsa-spying-outrage-merkel-germany-obama-france-hollande-2013-10.

Ma Zhaoxu. (2010). "Foreign Ministry Spokesperson Ma Zhaoxu's Remarks on China-related Speech by US Secretary of State on "Internet Freedom", Embassy Of the People's Republıc of Chına In the Kıngdom of Sweden", http://se.china-embassy.gov.cn/eng/fyrth/201001/t20100122_2879230.htm.

Mandiant. (2014). "APT28: A Window into Russia's Cyber Espionage Operations?", https://www.mandiant.com/resources/blog/apt28-a-window-into-russias-cyber-espionage-operations.

Mark Clayton. (2012). "Stealing US business secrets: Experts ID two huge cyber 'gangs' in China", The Christian Science Monitor. https://www.csmonitor.com/USA/2012/0914/Stealing-US-business-secrets-Experts-ID-two-huge-cyber-gangs-in-China;

Martin Bright, Ed Vulliamy ve Peter Beaumont. (2003). "Revealed: US dirty tricks to win vote on Iraq war", the Guardian. https://www.theguardian.com/world/2003/mar/02/usa.iraq.

Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America), https://www.icj-cij.org/case/70.

Monroe Doctrine. (1823), The U.S. National Archives and Records Administration, https://www.archives.gov/milestone-documents/monroe-doctrine.

Montevideo Konvansiyonu. League of Natıons, Treaty Series. (1936), Volume CLXV, No. 3802, https://treaties.un.org/doc/Publication/UNTS/LON/Volume%20165/v165.pdf.

Natıonal Counterıntellıgence And Securıty Center. (2018). "Foreign Economic Espionage in Cyberspace". https://www.dni.gov/files/NCSC/documents/news/20180724-economic-espionage-pub.pdf.

Nationality Decrees Issued in Tunis and Morocco. Permanent Court Of Internatıonal Justıce, Advısory Opınıon No. 4.. (1923), https://www.icj-cij.org/sites/default/files/permanent-court-of-international-justice/serie_B/B_04/Decrets_de_nationalite_promulgues_en_Tunisie_et_au_Maroc_Avis_consultatif_1.pdf.

NATO Standardizasyon Ofisi. (2020). The Official NATO Terminology Database. https://nso.nato.int/natoterm/Web.mvc.

NBC News. (2021). "Former CIA officer says traditional spying is 'dead' due to technology, internet", https://www.nbcnews.com/now/video/former-cia-officer-says-traditional-spying-is-dead-due-to-technology-internet-122990661534.

Necessity of ending the economic, commercial and financial embargo imposed by the United States of America against Cuba: resolution / adopted by the General Assembly. (2007). A/RES/62/3. https://digitallibrary.un.org/record/610595?ln=en.

Non-interference in the internal affairs of States. (1977). A/RES/32/153. https://digitallibrary.un.org/record/187959?ln=en.

North Sea Continental Shelf Cases (Federal Republic of Ger. v. Den.; Federal Republic of Ger. v. Neth.), https://www.icj-cij.org/case/51, https://www.icj-cij.org/case/52.

Office of Personnel Management data breach (2015). "International cyber law: interactive toolkit", https://cyberlaw.ccdcoe.org/w/index.php?title=Office_of_Personnel_Management_data_breach_(2015)&oldid=2417.

Peaceful and neighbourly relations among States. (1957). A/RES/1236(XII). https://digitallibrary.un.org/record/207248.

Protocol Additıonal to the Geneva Conventıons of 12 August 1949, And Relatıng To the Protectıon of Vıctıms of Non-Internatıonal Armed Conflıcts (Protocol II), of 8 June 1977. https://ihl-databases.icrc.org/assets/treaties/475-AP-II-EN.pdf.

Protocol on Prohibitions or Restrictions on the Use of Mines, Booby-Traps and Other Devices as amended on 3 May 1996 (Protocol II to the 1980 CCW Convention as amended on 3 May 1996). https://ihl-databases.icrc.org/assets/treaties/575-IHL-92-EN.pdf.

Public Safety Canada, "National Cyber Security Strategy", https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ntnl-cbr-scrt-strtg/ntnl-cbr-scrt-strtg-en.pdf.

Questions relating to the Seizure and Detention of Certain Documents and Data (Timor-Leste v. Australia). https://www.icj-cij.org/case/156.

Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security. (2015). A/70/174. https://digitallibrary.un.org/record/799853.

Report of the International Law Commission covering the work of its Tenth Session, 28 April 4 July 1958, Official Records of the General Assembly, Thirteenth Session, Supplement No. 9. Extract from the Yearbook of the International Law Commission:1958 ,vol. II. A/CN.4/117. https://legal.un.org/ilc/documentation/english/reports/a_cn4_117.pdf.

Report of the International Law Commission, Seventieth session, U.N. Doc. A/73/10, https://legal.un.org/ilc/reports/2018/english/a_73_10_advance.pdf.

Report of the Open-ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security. (2021). A/75/816, 24. https://documents-dds-ny.un.org/doc/UNDOC/GEN/N21/068/72/PDF/N2106872.pdf?OpenElement.

Report of the open-ended working group on security of and in the use of information and communications technologies 2021–2025. (2022). A/77/275.

https://documents-dds-ny.un.org/doc/UNDOC/GEN/N22/454/03/PDF/N2245403.pdf?OpenElement.
Reports Of Internatıonal Arbıtral Awards, Island of Palmas Case (Netherlands v. USA) 4 April 1928, Reports of International Arbitral Awards, Volume II, https://legal.un.org/riaa/cases/vol_II/829-871.pdf.
Respect for the principles of national sovereignty and non-interference in the internal affairs of States in their electoral processes : resolution / adopted by the General Assembly. (1989). A/RES/44/147. https://digitallibrary.un.org/record/82467?ln=en.
Reuters. (2013). "United Nations says it will contact United States over spying report". https://www.reuters.com/article/us-usa-security-nsa-un-idUSBRE97P0O720130826.
Richard Norton-Taylor. (2007). "Titan Rain - how Chinese hackers targeted Whitehall", The Guardian. https://www.theguardian.com/technology/2007/sep/04/news.internet.
Rodham Clinton, H. (2010). "Remarks on Internet Freedom. US Department of State", https://2009-2017.state.gov/secretary/20092013clinton/rm/2010/01/135519.htm.
Rubin A. J. (2013). "French Condemn Surveillance by N.S.A", The New York Times. https://www.nytimes.com/2013/10/22/world/europe/new-report-of-nsa-spying-angers-france.html.
Security Council official records, 37th year, 2335th meeting, 25 March 1982, New York. S/PV.2335, 12. https://digitallibrary.un.org/record/83326#record-files-collapse-header.
Security Service MI5. "Counter-Espionage". https://www.mi5.gov.uk/counter-espionage.
Senate. (1991). Report. No. 102–85, 43. https://www.intelligence.senate.gov/sites/default/files/publications/10285.pdf.
Situation of human rights in the Autonomous Republic of Crimea and the city of Sevastopol, Ukraine : resolution / adopted by the General Assembly. (2021). UN. General Assembly (75th sess. : 2020-2021). A/RES/75/192. https://digitallibrary.un.org/record/3896447.
Solemn appeal to States in conflict to cease armed action forthwith and to settle disputes between them through negotiations, and to States Members of the United Nations to undertake to solve situations of tension and conflict and existing disputes by political means and to refrain from the threat or use of force and from any intervention in the internal affairs of other States. (1985). A/RES/40/9. https://digitallibrary.un.org/record/106220?ln=en.
Statement by Delegation of the Islamic Republic of Iran To the Second Substantive Session of the Open-ended Working Group on Security of and in the Use of information and telecommunications Technologies. https://documents.unoda.org/wp-content/uploads/2022/03/1-Introductory-Remarks-Existing-and-Potential-Threats.pdf.
Statement by the Delegation of Ukraine at the First session of the Open- Ended working group on security of and in the use of ICTs under agenda item 5 (d). https://documents.unoda.org/wp-content/uploads/2021/12/Statement-Ukraine-OEWG-12152021-Threats.pdf.
Status of the implementation of of the Declaration on the Inadmissibility of Intervention in the Domestic Affairs of States and the Protection of Their

Independence and Sovereignty. (1966). A/RES/2225(XXI). https://digitallibrary.un.org/record/203172?ln=en.
Summary record of the 1423rd meeting : 1st Committee, held at Headquarters, New York, Monday, 20 December 1965, General Assembly, 20th session. 436. https://digitallibrary.un.org/record/800368.
T.C. Ulaştırma ve Altyapı Bakanlığı. "Ulusal Siber Güvenlik Stratejisi ve Eylem Planı (2022-2023)", https://hgm.uab.gov.tr/uploads/pages/siber-guvenlik/ulusal-siber-guvenlik-stratejisi-ep-2020-2023.pdf.
The International Telecommunication Union, https://www.itu.int/
The Lotus Case. (France v Turkey). (1927). No. 10 (PCIJ), https://www.icj-cij.org/public/files/permanent-court-of-international-justice/serie_A/A_10/30_Lotus_Arret.pdf.
The National Security Act of 1947, https://www.dni.gov/index.php/ic-legal-reference-book/national-security-act-of-1947.
The White House Office President Barack Obama. (2014), "Remarks by the President on Review of Signals Intelligence", https://obamawhitehouse.archives.gov/the-press-office/2014/01/17/remarks-president-review-signals-intelligence.
The White House. (2021). "FACT SHEET: Top 10 Programs in the Bipartisan Infrastructure Investment and Jobs Act That You May Not Have Heard About", https://www.whitehouse.gov/briefing-room/statements-releases/2021/08/03/fact-sheet-top-10-programs-in-the-bipartisan-infrastructure-investment-and-jobs-act-that-you-may-not-have-heard-about/.
Treaty of Friendship, Co-operation and Mutual Assistance Between the Soviet Union and Certain East European Communist Governments, https://www.cvce.eu/content/publication/1997/10/13/b1234dbc-f53b-4505-9d86-277e4f5c20d4/publishable_en.pdf.
Treaty Of Peace, Frıendshıp And Cooperatıon Between the Government Of Indıa And the Government Of the Unıon Of Sovıet Socıalıst Republıcs, https://www.mea.gov.in/bilateral-documents.htm?dtl/5139/Treaty+of.
Tunis Commitment. WSIS-05/TUNIS/DOC/7. https://www.itu.int/net/wsis/docs2/tunis/off/7.html.
Twenty-sixth plenary meeting, Saturday, 9 February 1946. A/PV.26. https://digitallibrary.un.org/record/482356?ln=en
U.S. Statutes at Large, Volume 40 (1917-1919), 65th Congress. 217. https://tile.loc.gov/storage-services/service/ll/llsl//llsl-c65/llsl-c65.pdf.
Uluslararası Adalet Divanı Statüsü, https://inhak.adalet.gov.tr/Resimler/Dokuman/2312020093041bm_02.pdf.
UN Secretary-General, "Foreword" , Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, UN Doc A/68/98, https://digitallibrary.un.org/record/753055.
UN. General Assembly (25th sess. : 1970). "Declaration on Principles of International Law concerning Friendly Relations and Cooperation among States in accordance with the Charter of the United Nations", A/RES/2625(XXV), https://treaties.un.org/doc/source/docs/A_RES_2625-Eng.pdf.
UN. Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security. A/76/135. https://digitallibrary.un.org/record/3906105?ln=en.
Unıted Natıons Satellıte Centre, https://unosat.org/.

United Nations Treaty Series. (1950), Volume 70, No.241, https://treaties.un.org/doc/publication/UNTS/Volume%2070/v70.pdf.
United Nations Treaty Series. (2004), Volume 2187, I-38544, https://treaties.un.org/doc/publication/unts/volume%202187/v2187.pdf.
United Nations Treaty Series. (2005), Volume 2253, A-3511, https://treaties.un.org/doc/Publication/UNTS/Volume%202253/v2253.pdf.
Unilateral economic measures as a means of political and economic coercion against developing countries : resolution / adopted by the General Assembly. (2020), UN. General Assembly (74th sess. : 2019-2020). A/RES/74/200. https://digitallibrary.un.org/record/3847699?ln=zh_CN.
US White House. (2011). "International Strategy for Cyberspace. Prosperity, Security and Openness in a Networked Wold". https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf.
Vailshery L. S. (2020). "Iot and non-iot connections worldwide 2010- 2025, https://www.statista.com/statistics/1101442/iot-number-of-connected-devices-worldwide/.
Verizon. (2022a). "2022 Data Breach Investigations Report", https://www.verizon.com/business/en-gb/resources/2022-data-breach-investigations-report-dbir.pdf.
Verizon. (2022b). "2020-2021 Cyber-Espionage Report", https://www.verizon.com/business/resources/T69/reports/2020-2021-cyber-espionage-report.pdf.
Vienna Convention on Diplomatic Relations. (1961). https://treaties.un.org/Pages/ViewDetails.aspx?src=IND&mtdsg_no=III-3&chapter=3&clang=_en.
Vienna Convention on the Representation of States in their Relations with International Organizations of a Universal Character (1975). https://legal.un.org/ilc/texts/instruments/english/conventions/5_1_1975.pdf.
von SPIEGEL Staff. (2013). "The NSA's Secret Spy Hub in Berlin", https://www.spiegel.de/international/germany/cover-story-how-nsa-spied-on-merkel-cell-phone-from-berlin-embassy-a-930205.html;
William J. Broad, John Markoff and David E. Sanger. (2011). "Israeli Test on Worm Called Crucial in Iran Nuclear Delay", The New York Times. https://www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html#:~:text=They%20say%20Dimona%20tested%20the,make%20its%20first%20nuclear%20arms.
World Summit on the Information Society : resolution / adopted by the General Assembly, UN. General Assembly (56th sess.: 2001-2002). A/RES/56/183. https://digitallibrary.un.org/record/455403.
Yearbook of the International Law Commisson. (1950), Volume 1, https://legal.un.org/ilc/publications/yearbooks/english/ilc_1950_v1.pdf.
Yearbook of the International Law Commisson. (1950), Volume 2, https://legal.un.org/ilc/publications/yearbooks/english/ilc_1950_v2.pdf.
Yearbook of the International Law Commisson. (1957), Volume 1, https://www.un-ilibrary.org/content/books/9789213624487/read.
Zetter K. (2012). "Meet 'Flame,' the Massive Spy Malware Infiltrating Iranian Computers", Wired. https://www.wired.com/2012/05/flame/.

# ÖZGEÇMİŞ

**Kişisel Bilgiler**

Soyadı, adı : Uzun, Ali

Uyruğu : T.C.

**Eğitim**

| **Derece** | **Eğitim Birimi** | **Mezuniyet Tarihi** |
|---|---|---|
| Yüksek lisans | Ankara Hacı Bayram Veli Üniversitesi Lisansüstü Eğitim Enstitüsü | 2023 |
| Lisans | İstanbul Üniversitesi Hukuk Fakültesi | 2014 |
| Lise | Ankara Lisesi | 2010 |

**İş Deneyimi**

| **Yıl** | **Yer** | **Görev** |
|---|---|---|
| 2015- | Ankara Barosu | Avukat |

**Yabancı Dil**

İngilizce

ankara HBM

ankara HBM

le.ahbv.edu.tr