T.C.
DOKUZ EYLÜL ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ
KAMU HUKUKU ANABİLİM DALI
KAMU HUKUKU YÜKSEK LİSANS PROGRAMI
YÜKSEK LİSANS TEZİ

ULUSLARARASI HUKUKTA MÜDAHALE VE KUVVET KULLANIMININ YASAKLANMASI İLKELERİ BAĞLAMINDA SİBER SALDIRILAR

Merve Leman BULUT MİŞE

Danışman
Dr. Öğretim Üyesi Uğur SAMANCI

2024

T.C.
DOKUZ EYLÜL ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ
KAMU HUKUKU ANABİLİM DALI
KAMU HUKUKU YÜKSEK LİSANS PROGRAMI
YÜKSEK LİSANS TEZİ

ULUSLARARASI HUKUKTA MÜDAHALE VE KUVVET KULLANIMININ YASAKLANMASI İLKELERİ BAĞLAMINDA SİBER SALDIRILAR

Merve Leman BULUT MİŞE

Danışman
Dr. Öğretim Üyesi Uğur SAMANCI

İZMİR – 2024

TEZ ONAY SAYFASI

YEMİN METNİ

Yüksek Lisans Tezi olarak sunduğum "Uluslararası Hukukta Müdahale ve Kuvvet Kullanımının Yasaklanması İlkeleri Bağlamında Siber Saldırılar" adlı çalışmanın, tarafımdan, akademik kurallara ve etik değerlere uygun olarak yazıldığını ve yararlandığım eserlerin kaynakçada gösterilenlerden oluştuğunu, bunlara atıf yapılarak yararlanılmış olduğunu belirtir ve bunu onurumla doğrularım.

Tarih

..../..../.....

Merve Leman BULUT MİŞE

İmza

ÖZET

Yüksek Lisans Tezi

Uluslararası Hukukta Müdahale ve Kuvvet Kullanımının Yasaklanması İlkeleri Bağlamında Siber Saldırılar

Merve Leman BULUT MİŞE

Dokuz Eylül Üniversitesi
Sosyal Bilimler Enstitüsü
Kamu Hukuku Anabilim Dalı
Kamu Hukuku Programı

Uluslararası hukukta devletlerin egemen eşitliği, müdahale ve kuvvet kullanma yasakları hakkındaki düzenlemeler; uluslararası toplumun huzur ve güvenliği bakımından kritik öneme sahip, emredici temel ilkelerdir. Siber uzay ve siber saldırılar ise, teknolojinin gelişmesiyle birlikte devletler için diğer ülkesel alanlardan farklı ve yeni bir zemin oluşturan, birçok açıdan hukuki yoruma açık ve güncel bir mesele olarak karşımıza çıkmaktadır.

Siber uzayın anonim ve sınır aşan yapısı, kendisine özgü yeni kurallar oluşturulması gerektiğini göstermektedir. Bunun üzerine çeşitli kodifikasyon çalışmaları yürütülürken, mevcut düzenlemelerin koruyucu gücünden faydalanılmaktadır. Nitekim devletlerin gerçekleştirdiği ve ulusal ve uluslararası çalışmalar da bu hususu desteklemekte, temel uluslararası hukuk ilkelerine bağlı kalınarak hareket edilmektedir. Kodifikasyon çalışmalarında ise bağlayıcı niteliği bulunmamasına rağmen, Tallinn Kılavuzu çerçevesindeki küresel uzlaşı önem arz etmektedir.

Çalışmamızda siber uzay ve siber saldırılar teknik bilgiler, egemenlik, müdahale, kuvvet kullanma, meşru müdafaa ve uluslararası sorumluluk kavramları eşliğinde değerlendirilmiştir. Devletler tarafından gerçekleştirilen yahut devletlere isnat edilebilen siber saldırılar, örnekler üzerinden incelenerek devletlerin sorumluluğu irdelenmiştir. Nihayetinde çalışmamızın amacı, devletleri etkileyen siber saldırıların uluslararası hukuka uygunluğunu

incelemek ve ihlal durumunda devletlerin başvurabileceği yolları ortaya koymaktır.

Çalışmamız üç bölümden oluşmaktadır. İlk bölümde siber uzayın gelişimi ve teknik özellikleri üzerine temel açıklamalar yapılmış, siber saldırı yöntemleri ve siber aktörler hakkında bilgi verilmiştir.

Çalışmamızın ikinci bölümünde siber saldırılara uygulanacak temel uluslararası hukuk kuralları açıklanmış, yeni çalışmaların gelişimi aktarılarak düzenlemelerin uygulanabilirliği değerlendirilmiştir.

Çalışmamızın üçüncü bölümünde devletler tarafından gerçekleştirildiği iddia edilen muhtelif siber saldırı örnekleri incelenmiş, somut olaylar üzerinden hukuk kurallarının uygulaması tartışılmıştır.

Anahtar Kelimeler: Uluslararası Hukuk, Egemenlik, Müdahale Yasağı, Kuvvet Kullanma Yasağı, Meşru Müdafaa, Uluslararası Sorumluluk, İsnadiyet, Siber Uzay, Siber Saldırı, Siber Güvenlik, Tallinn Kılavuzu, Teknoloji.

ABSTRACT

Master's Thesis

Cyber Attacks in the context of the Principles of Prohibition of Intervention and the Use of Force in International Law

Merve Leman BULUT MİŞE

Dokuz Eylül University

Graduate School of Social Sciences

Department of Public Law

Public Law Program

Regulations on the sovereign equality of states in international law and prohibitions on intervention and the use of force; they are essential fundamental principles that are of critical importance for the peace and security of the international community. Cyberspace and cyber attacks, on the other hand, emerge as a current issue that is open to legal interpretation in many respects, creating a new and different ground for states from other national areas, with the development of technology.

The anonymous and transboundary structure of cyberspace shows that new rules must be created. While various codification studies are carried out, the protective power of existing regulations is utilized. As a matter of fact, national and international studies carried out by states also support this issue, and action is taken in accordance with the basic principles of international law. In codification studies, although it is not binding, the global consensus within the framework of the Tallinn Manual is important.

In our study, cyberspace and cyber attacks were evaluated together with technical information, sovereignty, intervention, use of force, self-defense and international responsibility concepts. Cyber attacks carried out by states or attributable to states are examined through examples and the responsibilities of states are examined. Ultimately, the aim of our study is to examine the compliance of cyber attacks affecting states with international law and to reveal the remedies that states can apply in case of violation.

Our study consists of three parts. In the first part, basic explanations were made on the development and technical features of cyberspace, and information was given about cyber attack methods and cyber actors.

In the second part of our study, the basic international law rules to be applied to cyber attacks are explained, the development of new studies is explained and the applicability of the regulations is evaluated.

In the third part of our study, various examples of cyber attacks allegedly carried out by states were examined and the application of legal rules was discussed through concrete events.

Keywords: International Law, Sovereignty, Prohibition of Intervention, Prohibition of Use of Force, Self-Defense, International Responsibility, Attribution, Cyberspace, Cyber Attack, Cyber Security, Tallinn Manual, Technology.

ULUSLARARASI HUKUKTA MÜDAHALE VE KUVVET KULLANIMININ YASAKLANMASI İLKELERİ BAĞLAMINDA SİBER SALDIRILAR

İÇİNDEKİLER

TEZ ONAY SAYFASI ii
YEMİN METNİ iii
ÖZET iv
ABSTRACT vi
İÇİNDEKİLER viii
KISALTMALAR xi
ŞEKİLLER LİSTESİ xii
TABLOLAR LİSTESİ xiii

GİRİŞ 1

BİRİNCİ BÖLÜM
NİTELİĞİ İTİBARİYLE İNTERNET VE SİBER UZAY

I. BİR ÇAĞA DAMGASINI VURAN TEKNOLOJİ: İNTERNET 2
II. KAVRAM VE TERİMLERLE SİBER UZAY 4
A. Siber ve Siber Uzayın Kökeni 4
B. Siber Uzaya İlişkin Temel Özellikler 6
C. Ulusal ve Uluslararası Sahada Siber Uzay Kavramları 7
1. Türkiye'de Siber Uzaya İlişkin Temel Kavramlar 8
2. ABD'de Siber Uzaya İlişkin Temel Kavramlar 9
3. Kuzey Atlantik Antlaşması Örgütü'nde (NATO) Siber Uzaya İlişkin Temel Kavramlar 10
4. Şanhay İşbirliği Örgütü'nde Siber Uzaya İlişkin Temel Kavramlar 11
III. SİBER SALDIRI ARAÇ VE YÖNTEMLERİ 13
A. Siber Saldırı Araçları 13
1. Başka Bir Programa Bağımlı Siber Saldırı Yazılımları 14
a. Virüs (Virus) 14

b. Truva Atı (Trojan Horse) 15
c. Mantık Bombası (Logic Bomb) 16
d. Arka Kapı (Backdoor/Trapdoor) 17
2. Diğer Programlardan Bağımsız Siber Saldırı Yazılımları 17
a. Bakteri (Bacterium) 17
b. Solucan (Worm) 18
B. Başlıca Siber Saldırı Yöntemleri 19
1. Hizmet Engelleme (Denial of Service - DoS/DDoS) 19
2. Zombi/Köle Bilgisayar (Botnet) 19
3. Yetki Artırımı (Privilege Escalation) 20
4. Sosyal Mühendislik (Social Engineering) 20
5. Gelişmiş Sürekli Tehditler (Advanced Persistent Threats) 21
IV. SİBER AKTÖRLER 22
A. Devletler 23
B. Uluslararası Kurumlar ve Devlet Dışı Aktörler 24
1. Bilgisayar Eylemcileri (Hacktivists) 26
2. Bilgisayar Korsanları (Hackers) 26
3. Siber Teröristler 28
4. Organize Siber Suçlular 28
5. Şirketler 29
6. Siber Casusluk Ajanları 29
7. Siber Savaşçılar/Milisler 30

İKİNCİ BÖLÜM
ULUSLARARASI HUKUKUN İLGİLİ TEMEL KURALLARI VE SİBER SALDIRILAR

I. DEVLETLERİN EGEMENLİĞİ 32
A. Egemenliğin Mahiyeti 32
B. Devletlerin Egemen Eşitliği İlkesi 34
C. Siber Uzayda Egemenlik 38
II. İÇ İŞLERE KARIŞMAMA İLKESİ VE MÜDAHALE YASAĞI 40

A. İç İşlere Karışmama İlkesi ve Müdahale Yasağının Mahiyeti 40
B. Siber Uzayda İç İşlere Karışmama İlkesi ve Müdahale Yasağı 43
III. KUVVET KULLANMA YASAĞI VE MEŞRU MÜDAFAA 46
A. Kuvvet Kullanma Yasağı ve Meşru Müdafaanın Mahiyeti 46
B. Siber Uzayda Kuvvet Kullanma Yasağı ve Meşru Müdafaa 55
IV. DEVLETLERİN ULUSLARARASI SORUMLULUĞU VE İSNADİYET 59
A. Devletlerin Uluslararası Sorumluluğu ve İsnadiyetin Mahiyeti 59
B. Siber Uzayda Devletlerin Uluslararası Sorumluluğu ve İsnadiyet 62
1. Devlet Organları Tarafından veya Özen Yükümlülüğünün İhlali Sonucu Gerçekleştirilen Siber Saldırılar 65
2. Devlet Dışı Aktörler Tarafından Gerçekleştirilen Siber Saldırılar 66

ÜÇÜNCÜ BÖLÜM
SİBER UZAYDA DEVLET UYGULAMALARINA DAİR BAŞLICA ÖRNEKLER

I. EGEMENLİK, İÇ İŞLERE KARIŞMAMA İLKESİ VE MÜDAHALE YASAĞINA İLİŞKİN ÖRNEKLER 70
A. İlk Siber Saldırı ve Uluslararası Hukuk Tartışmaları: Estonya (2007) 70
B. Siber Saldırıların Hibrit Niteliği: Gürcistan-Rusya Sorunları (2008) 75
C. Baskı Amaçlı Siber Saldırılar: Abd-Sony-Kuzey Kore Üçgeni (2014) 81
II. KUVVET KULLANMA YASAĞI VE MEŞRU MÜDAFAAYA İLİŞKİN ÖRNEKLER 87
A. Siber Saldırıların Desteği: Suriye-İsrail Orchard Operasyonu (2007) 87
B. Siber Saldırılarda Fiziksel Zarar Tartışmaları: Stuxnet (2014) 89
C. Süregelen Siber Saldırılar: Ukrayna-Rusya Gerilimi (2014-Günümüz) 95

SONUÇ 104
KAYNAKÇA 107

KISALTMALAR

ABD	Amerika Birleşik Devletleri
ARPA	Advanced Research Projects Agency
bkz.	Bakınız
BM	Birleşmiş Milletler
CCDCOE	Cooperative Cyber Defense Center of Excellence
CIA	Central Intelligence Agency
Çev.	Çeviren
DoS/DDoS	Distributed Denial of Service
Ed.	Editör
FBI	Federal Bureau of Investigation
GoP	Guardians of Peace
IP	Internet Protocol
m.	Madde
NATO	Kuzey Atlantik Antlaşması Örgütü
NSA	National Security Agency
OSCE	Organization for Security and Cooperation in Europe
prg.	Paragraf
RG	Resmî Gazete
s.	Sayfa
SCADA	Supervisory Control and Data Acquisition
ss.	Sayfa Aralığı
SSCB	Sovyet Sosyalist Cumhuriyetler Birliği
ŞİÖ	Şanhay İşbirliği Örgütü
T.C.	Türkiye Cumhuriyeti
TCP	Transmission Control Protocol
UAD/ICJ	Uluslararası Adalet Divanı
USAD/PCIJ	Uluslararası Sürekli Adalet Divanı
Y.	Yıl

ŞEKİLLER LİSTESİ

Şekil 1: Siber Saldırı Yazılımlarının Türleri s. 13

TABLOLAR LİSTESİ

Tablo 1: Devlet Dışı Siber Aktörler s. 25
Tablo 2: Silahlı Saldırının Belirlenmesinde Genişletilmiş UAD Çerçevesi s. 53

GİRİŞ

Uluslararası hukuk, uluslararası ilişkilerin en önemli yapıtaşlarından biridir. Devletler 20. yüzyılın başından itibaren, uluslararası barış ve güvenliğin sağlanması yolunda sorun oluşturabilecek hususlarla ilgili mesai harcayarak, attıkları her adımı hukuka uygun hale getirme çabasında olmuştur. Bu noktada uluslararası hukuk, dünyadaki değişim ve gelişimlerden etkilenerek şekillenip günümüzdeki halini almıştır. Temel kuralların yeni sorunlarla baş edebilecek şekilde varlığını sürdürmesi için; yaşanan ve yaşanması muhtemel hadiseler göz önüne alınarak kuralların güncellenmesi, her zaman önemini korumuştur.

Uluslararası hukukta devletlerin egemen eşitliği, müdahale ve kuvvet kullanma yasağı gibi temel kavramlar, uluslararası toplumun huzuru açısından savunmasız bırakılamayacak kadar önemlidir. Bu hususa ilişkin farklı soru ve sorunlar ortaya çıktığında, olumsuz sonuçlardan kaçınabilmek adına hızlı çözüm önerileri getirilebilmelidir. Siber saldırılar, uluslararası güvenliği tehdit edebilecek ve devletleri etkileyebilecek olgular arasında gündemdeki yerini koruyan ve çözüme muhtaç konulardan biri olarak, ifade ettiğimiz sorunlar arasında yerini almaktadır.

Siber uzay ve siber saldırılarla bağlantılı kavramların içeriği, ulusal ve uluslararası hukukta kapsamı henüz netleşmemiş, teknoloji ile ilişkili, yeni ve dinamik konulardan oluşmaktadır. 21. yüzyılda devletler, fiziki varlıklarının yanında, teknolojik olarak varlıklarını korumak ve güçlerini geliştirmek isterken, bir yandan da siber tehditlerin geri dönüşü olmayan yıkımlarını engellemek amacıyla hareket etmekte ve uluslararası çalışmalar yürütmektedir. Siber faaliyetlerin gerçekleştiği siber uzayın yeni bir operasyon alanı olması sebebiyle, uluslararası hukukta uzlaşı sağlanıp yeni düzenlemeler oluşturulması zaman almaktadır. Bu nedenle var olan uluslararası kuralların mevcut koşullar ölçüsünde değerlendirilmesi gereği ortaya çıkmaktadır.

Çalışmamızda; siber güvenlik süreci, uluslararası hukukun siber saldırılara karşı gösterdiği tutum ve siber saldırılara uygulanabilecek uluslararası hukuk kurallarına ilişkin hususlar ele alınacaktır. Siber uzay ve siber saldırılara ilişkin teknik bilgiler, egemenlik, müdahale, kuvvet kullanma yasağı ve siber uzaya özgü hazırlanmış uluslararası metinler hakkında bilgi aktarılacaktır. Somut olaylarla siber saldırılarda devletlerin rolü, saldırıların uluslararası hukuka etkisi değerlendirilecektir.

BİRİNCİ BÖLÜM
NİTELİĞİ İTİBARİYLE İNTERNET VE SİBER UZAY

I. BİR ÇAĞA DAMGASINI VURAN TEKNOLOJİ: İNTERNET

İnternet, tarih sahnesinde görece kısa bir geçmişe sahip, dünya üzerinde yaygın kullanımı olan bir kitle iletişim teknolojisidir. En temel anlatımla, *'ağların ağı'* anlamına gelmekte ve altyapısıyla dünya üzerindeki bilgisayarları birbirine bağlayan bir sistem olarak tanımlanmaktadır.[1] Gün geçtikçe kullanım alanı genişleyen internet, zamanla hayatımızın vazgeçilmez bir parçası haline gelerek, bilişim teknolojisinin en temel ürünlerinden biri olan bilgisayarla birlikte bilgi toplumunun gelişimine önderlik etmektedir.

İnternet, esasen Amerika Birleşik Devletleri (ABD) ve Sovyet Sosyalist Cumhuriyetler Birliği (SSCB) arasında yaşanan Soğuk Savaş döneminin ürünüdür.[2] 1957 yılında SSCB'nin Sputnik projesini başarıyla tamamlayıp ilk yapay uyduyu uzaya göndermesi üzerine ABD, bilim ve teknoloji alanındaki yarışta bir adım atmış ve 1958 yılında Savunma Bakanlığı uhdesinde Gelişmiş Araştırma Projeleri Teşkilatı'nı (Advanced Research Projects Agency – ARPA) kurmuştur.

ARPA'nın temel amacı, olası bir nükleer saldırıya karşı dünyanın farklı yerlerinde bulunan ABD üslerinin iletişiminin devamını sağlamaktır. Bunun için, kullanılacak iletişim yolunun tek bir merkeze bağlı olmaması, birden çok bağlantıya aynı anda erişimi mümkün kılması, bağlantılardan birinin hasara uğraması halinde diğerlerinin iletişime devam edebilmesi gerekmektedir. Tüm bu özellikleri bünyesinde barındıracak iletişim yolu için birçok proje yapılmış ve nihayetinde bir bilgisayar ağı tasarlanarak ARPANET ismini almıştır. 1969 yılında ARPANET'in fiziksel temellerinin California'da atılmasının ardından, internete ilişkin ilk faaliyetler somutlaştırılmış ve günümüze değin gelişimini sürdüren birçok çalışmanın önü açılmıştır.[3]

ABD Savunma Bakanlığı'nın askeri iletişim yolu şeklinde kullanmayı amaçlayarak başlattığı bir proje olan ARPANET, internet teknolojisinin oluşması

[1] Haluk Geray, **İletişim ve Teknoloji**, Ütopya Yayınları, Ankara, 2002, s. 24.
[2] Mustafa Emre Civelek, **İnternet Çağı Dinamikleri**, Beta Yayıncılık, İstanbul, 2009, s. 6.
[3] Civelek, ss. 7-8.

sürecinde karşımıza çıkan ilk aşamadır. 1970'lerde, 38 ana bilgisayara bağlanan ağ yapısına İngiltere ve Norveç entegre edilmiş, iletişim trafiğinin genişlemesiyle birlikte yeni ağ protokolleri geliştirilmiştir. İletişim Kontrol Protokolü (Transmission Control Protocol - TCP) ve İnternet Protokolü (Internet Protocol - IP) olarak adlandırılan bu protokoller, sunucudan istenen verilerin paketler halinde düzenlenip varış noktasına doğru sıralamayla ve hatasız bir şekilde ulaşması amacına hizmet etmektedir.[4] Söz konusu protokollerin kullanılmaya başlanmasının ardından, Vinton G. Cerf ve Robert E. Kahn'ın TCP hakkında yazmış oldukları bir makalede *'internet'* terimi kullanılarak bağımsız ve halka açık olacak bir ağ sisteminin sinyalleri verilmiştir.[5] 1983 yılına gelindiğinde, ARPANET'e bağlı tüm ağlar TCP ve IP'yi kullanmaya başlamış, ARPANET'in eski ağ protokolü tamamen değiştirilmiştir. Böylece, birbirine bağlı ve herkesin erişimine açık ağların bütünü *'internet'* adını almıştır.[6]

İnternet, günümüzde muhtelif hizmet ve işlemlerin birçoğunun kısa sürede gerçekleştirilebildiği bir platform haline gelmiştir.[7] Hızla yaygınlaşan ve popülerlik kazanmaya devam eden internet teknolojisinin temel niteliklerini şu şekilde açıklamak mümkündür:[8]

- Merkezsiz: İnternetin kullanılmasını yöneten belirli ve ana bir bilgisayar bulunmamaktadır. İnternet, herhangi bir makine kapatılarak kullanılmaz hale getirilemez.
- Özgür: İnternet üzerine çeşitli yasaklamalar getirilse de bu yasakları yine internet aracılığıyla delmek mümkündür.
- Küresel: İnternet kullanımı belirli bir coğrafi bölge ile sınırlı değildir. Dünyanın herhangi bir bölgesinden yayına açılan bir veriye, başka bir bölgeden erişilebilir.
- Dinamik: Kişiler internetteki verilere katkı sağlayıp bizzat kendileri veri oluşturabilir, var olan veriler hakkında görüş bildirebilir.

---

[4] Raphael Cohen-Almagor, "Internet History", **International Journal of Technoethics**, Cilt:2, Sayı:2, 2011, s. 50.

[5] Vinton G. Cerf ve Robert E. Kahn, "A Protocol for Packet Network Intercommunication", **IEEE Transactions on Communications**, Cilt:22, Sayı:5, 1974, ss. 637-648.

[6] James Slevin, **The Internet and Society**, Polity Press, Oxford, 2000'den aktaran Cohen-Almagor, s. 50.

[7] Abdullah Tokdaş, **Siber Güvenlik ve Uluslararası İlişkiler**, (Yayınlanmamış Yüksek Lisans Tezi), Selçuk Üniversitesi Sosyal Bilimler Enstitüsü, Konya, 2018, s. 31.

[8] Civelek, ss. 12-15.

- Sınırsız: İnternet kullanımı ülke sınırlarıyla paralel değildir. İnternet altyapısının bulunduğu her yere internet üzerinden ulaşılabilir.
- Asenkron: Radyo ve televizyon yayınlarının aksine, internet yayınlarının belirli bir zaman içinde tüketilmesi zorunluluğu yoktur. İnternet üzerinde kayıtlı her veriye, zaman sınırlaması olmaksızın ulaşılabilir.

Açıkladığımız özelliklerin dünyaya olumlu ve olumsuz birçok etkisinin olduğu aşikârdır. Yine de belirtmek gerekir ki; internet kullanımı, bilgi toplumuna yararları ve zararlarıyla elzem bir ihtiyaç haline gelmiştir.

Bilgisayar ve cep telefonu teknolojilerinin hızla gelişmesiyle internet yoluyla işlem yapabilecek araç skalası hayli genişlemiştir. Böylece, ulusal ve uluslararası hukukta internetin sebep olabileceği güvenlik açıklarına ilişkin tartışmalar gündeme gelmiştir. 20. yüzyılın sonu ve 21. yüzyılın başlarında devletler, ulusal siber güvenlik politikalarını geliştirmeye başlamış ve *'siber uzay (cyberspace)'*, hayatımıza dahil olmuştur.[9]

II. KAVRAM VE TERİMLERLE SİBER UZAY

A. Siber ve Siber Uzayın Kökeni

İnternet ve bilgisayar teknolojileri, icat edilmelerinden bu yana birçok ilerleme kaydetmiş; atıl teknolojiler olarak kalmayıp, yeni kavramların ortaya çıkması ve mevcut kavramların gelişmesinde rol oynamıştır. Siber uzay da bu kavramlardan biridir. *'Siber'* kelimesi, köken olarak eski Yunanca *'gemiyi yöneten, dümenci'* anlamlarına gelen *'kübernetes'* ; Latince *'yönetim, sevk, idare'* anlamlarına gelen *'gobernare'* kelimelerinden türetilmiş *'sibernetik'* kavramına ve sibernetik bilimine dayandırılmaktadır.[10]

Sibernetik biliminin ortaya çıkışı, Orta Çağ'da birçok makine ve buluşa imza atarak diğer bilim insanlarına da ilham olan Ebû'l İz İsmail İbni Rezzaz El-Cezerî'ye dayanmaktadır. El-Cezerî, fen ve teknik, robotlar, saatler, su makineleri, termoslar,

[9] Mahruze Kara, **Siber Saldırılar – Siber Savaşlar ve Etkileri**, (Yayınlanmamış Yüksek Lisans Tezi), İstanbul Bilgi Üniversitesi Sosyal Bilimler Enstitüsü, İstanbul, 2013, s. 3.

[10] Bekir Çırak ve Abdülkadir Yörük, "Mekatronik Biliminin Öncüsü İsmail El - Cezeri", **Siirt Üniversitesi Sosyal Bilimler Enstitüsü Dergisi**, Sayı:4, 2015, s. 178.

otomatik çocuk oyuncakları, şifreli kilitler ve kasalar gibi 60 ayrı makinenin mucididir. Önemli bir İslam bilim insanı olan El Cezeri, bilgisayarın temelini atan ve sibernetik biliminin öncülüğünü yapan kişi olarak bilinmektedir.[11] Ancak sibernetik bilimi, isim olarak çok daha sonra; 1900'lü yıllarda anılmaya başlanmıştır.

Sibernetik, ilk kez 1948 yılında matematikçi Norbert Wiener tarafından *'Sibernetik ya da Hayvanlarda ve Makinelerde Kontrol ve İletişim (Cybernetics or Control and Communication in the Animal and Machine)'*[12] başlıklı kitapta, *'hayvanlar ve makineler arası iletişim-kontrol bilimi'* anlamında kullanılmıştır. Türk Dil Kurumu'nda *'güdüm bilimi'* olarak ifade edilen sibernetik; teknolojik, biyolojik, sosyolojik ve ekonomik sistemlerde kumanda uç iletişimini inceleme amacına hizmet eden etki bilimi olarak tanımlanmaktadır.[13] Özetle, canlılar ve makineler arasındaki soyut bağın kontrolü üzerinde çalışan bilim sibernetiktir ve birçok bilim dalı ile etkileşim halindedir. Sibernetik biliminin temeli olan siber kavramı ise; canlılar ve makinelerin aynı düzlemde eyleme geçebildiği sanal oluşumu ifade etmektedir.

Siber uzay, bilim insanları tarafından yaratılmış teknik bir terim değildir. 1982 yılında, ilk olarak bilim-kurgu edebiyatı yazarlarından William Gibson'ın *'Burning Chrome'*[14] adlı eserinde kullanılmış bir kavramdır. 1984 yılında yayınladığı *'Neuromancer'*[15] eserinde ise siber uzayı detaylı bir şekilde tasvir etmiştir. Eserdeki siber uzay tanımı şu şekildedir:[16]

> *Siber uzay. Her ulustaki milyarlarca yasal kullanıcının, matematiksel kavramların öğretildiği çocukların her gün deneyimlediği rızaya dayalı bir halüsinasyon... İnsan sistemindeki her bilgisayarın bankalarından soyutlanmış verilerin grafik bir temsili. Düşünülemez karmaşıklık. Işığın çizgileri, zihnin uzaysızlığında, kümelerde ve veri takımyıldızlarında uzanmakta. Şehir ışıkları gibi, uzaklaşan...*

1990'lı yıllarda siber uzaya ilişkin tanımlamalar bilimsel bir hal alıp genişleyerek dünyadaki gelişmelere ayak uydurmuştur. *Benedikt,* siber uzayı

---

[11] Abdullah Yaşın, "Ebul-İz'in Bilime Katkıları", **Bilim Düşünce ve Sanatta Cizre (Uluslararası Bilim Düşünce ve Sanatta Cizre Sempozyumu Bildirileri)**, 2012, s. 201.
[12] Norbert Wiener, **Cybernetics or Control and Communication in the Animal and Machine**, 2. Baskı, MIT Press, London, 2019.
[13] Toygar Akman, **Sibernetik "Dünü Bugünü Yarını"**, Kaknüs Yayınları, İstanbul, 2003, s. 21.
[14] William Gibson, **Burning Chrome**, Yeniden Baskı, HarperCollins Publishers, Scotland, 2003.
[15] William Gibson, **Neuromancer**, Elektronik Baskı, ACE Books by ACE Publishing Group – Penguin Putnam Inc., Newyork, 2003.
[16] Gibson, **Neuromancer**, s. 51.

"bilgisayar kullanılarak sürdürülen, erişim imkânı sunan, veri üretilen küresel ağ temelli sanal ve yapay iletişim alanı" şeklinde açıklamıştır.[17]

Görüldüğü üzere, siber uzayın ortaya çıkış sürecinde kurgusal yanından farklı bir anlamı yoktur. Ancak zamanla, kademeli bir yükselişle, siber uzay birçok alanda önemli hale gelmiştir. Bu alanlardan biri de uluslararası hukuktur. 2009'da *Libicki*, siber uzayı *"kara, deniz, hava ve uzay alanlarına benzeyen ancak bunlardan bağımsız, iletişim altyapılarını kullanan, daha az somut, katmanlı bir sanal ortam"* olarak ifade etmiştir.[18] Söz konusu tanım, siber uzayın yapısını ve uluslararası hukuktaki yerini açıklama yolunda farklı ve ayrıntılı bir anlatım olarak literatürdeki yerini almıştır.

Bu tanımlardan hareketle söylenebilir ki; siber uzay, fiziki altyapısı nedeniyle somut, gerçek dünyadan bağımsız ve sanal bir mekân anlayışıyla soyut iki ayağı olan bir bilgi havuzudur. Öte yandan sahip olduğu dinamik yapı sayesinde sürekli gelişme halindedir. Doğası gereği her yerden ulaşılabilen siber uzay, kapsamı ve etki ölçeğiyle yeni bir gerçeklik yaratmıştır.

Tüm bu sebeplerle, devletler arasındaki dengeyi değiştirebilecek her husus gibi, siber uzayın politik önemi yadsınamayacak kadar büyüktür. Hükümetler, ordular, özel şirketler ve sivil ağlar tarafından yoğun bir şekilde üzerinde çalışılan siber uzay, yeni özellik ve kavramları da beraberinde getirerek birçok tartışmanın odak noktası haline gelmiştir.[19]

B. Siber Uzaya İlişkin Temel Özellikler

Bir alanın siber uzay olarak kabul edilmesi için belli başlı özellikleri bünyesinde barındırması gerekmektedir. Söz konusu özelliklerin tamamını içermeyen bir alan, yalnızca siber uzayı oluşturan parçalardan biri olabilir. Siber uzay, siber deneyime katılan kullanıcılar, sanal ortamda bulunan veriler, hizmetleri oluşturup platform yapısını destekleyen mantıksal yapı taşları ve fiziksel temeller olmak üzere

[17] Michael Benedikt, "Cyberspace: Some Proposals", **Cyberspace: First Steps**, (Ed. Michael Benedikt), 3. Baskı, MIT Press, London, 1992, s. 119.
[18] Martin C. Libicki, **Cyberdeterrence and Cyberwar**, RAND Corporation, Santa Monica, 2009, ss. 11-12.
[19] Ayrıntılı bilgi için bkz. Nazli Choucri, **Cyberpolitics in International Relations**, MIT Press, London, 2012, ss. 3-8.

dört katmandan oluşmaktadır.[20] Bununla birlikte, münhasır özellikleri de şu şekilde özetlenmektedir:[21]

- Zamansallık: Siber uzay, geleneksel zaman algısını neredeyse yakın anlı durumlara çevirir.
- Fiziksellik: Siber uzay, coğrafi ve fiziksel konum kısıtlamalarını görmezden gelir.
- Geçirgenlik: Siber uzay, sınırlara ve yetki alanlarına nüfuz edecek güçtedir.
- Akışkanlık: Siber uzay, sürekli değişim ve yeniden yapılanma halindedir.
- Katılım: Siber uzay, eyleme geçme ve politik olarak kendini ifade edebilme karşısındaki engelleri azaltır.
- Atıf: Siber uzaydaki aktörler ve eylem bağlantıları gizlenir.
- Hesap Verebilirlik: Siber uzayda sorumluluk mekanizmaları rahatlıkla delinebilir.

Siber uzayın, tüm bu özellikleri göz önüne alındığında, ne denli önemli olaylara sebebiyet verebileceği net bir şekilde anlaşılmaktadır. Fiziksel dünyada meydana gelen değişim ve gelişimler siber uzayı etkilerken, siber uzayda meydana gelen eylemler de aynı şekilde fiziksel dünyada yankılarını gösterebilme gücüne sahiptir. Gün geçtikçe gerçek dünya ve siber uzay ayrımı ortadan kalkmakta, siber uzay hayatımızın her alanına dahil olabilmektedir.[22] Bu sebeple, ulusal ve uluslararası faaliyetlerde siber uzaya ilişkin savunma ve güvenlik çalışmaları artarak devam etmektedir.

C. Ulusal ve Uluslararası Sahada Siber Uzay Kavramları

Teknoloji ve bilişim sistemlerinin gelişmesiyle birlikte, devletlerin egemenliğine ilişkin tartışma konularına bir yenisi daha eklenmiş; siber uzay uluslararası hukuktaki soru işaretlerinden biri olarak yerini almıştır. Siber uzayın hayatımızın farklı noktalarına ani etkide bulunabilecek potansiyele ulaşmasıyla;

[20] David Clark, "Characterizing Cyberspace: Past, Present and Future", **MIT CSAIL**, Version 1.2, 2010, s. 1.
[21] Choucri, s. 4.
[22] Buğrahan Emir, **Uluslararası İlişkilerin Kuramsal Çerçevesi ve Siber Güvenlik Kavramının Analizi**, (Yayınlanmamış Yüksek Lisans Tezi), Karadeniz Teknik Üniversitesi Sosyal Bilimler Enstitüsü, Trabzon, 2020, s. 8.

uluslararası hukukta mekânsal olarak kabul edilip kurallara tabi tutulan kara, deniz, hava ve uzay alanlarının yanı sıra, askeri faaliyetler için beşinci bir alan olarak kabul edilip edilmeyeceğine yönelik halen güncelliğini koruyan tartışmalar ortaya çıkmıştır. Benzer şekilde; siber uzayın, devletlerin egemenlik alanları dışında kalan ve insanlık için müşterek kullanım alanı olarak görülebilecek *'küresel ortaklık'*[23] niteliğinde bir yapısının olup olmadığı tartışmaları da sürmektedir.[24] Bu kapsamda devletler, kendi varlıklarını korumak adına, iç hukuk ve politikalarında görüşlerini açıklamaktadır.

1. Türkiye'de Siber Uzaya İlişkin Temel Kavramlar

Türkiye, siber güvenlik konusunda 2013 yılından bu yana *'Ulusal Siber Güvenlik Stratejisi ve Eylem Planı'* adı altında çalışmalar yürütmekte; söz konusu çalışmalar kapsamında kavram ve tanımlara önem atfetmektedir. Bu çerçevede siber uzay, *"doğrudan ya da dolaylı olarak internete, elektronik haberleşme ve bilgisayar ağlarına bağlı olan tüm sistem ve hizmetler"* olarak tanımlanmaktadır.[25] Söz konusu tanımdan yola çıkarak belirtmek gerekir ki; esasında siber uzayın ve siber uzaya dair tüm kavramların gelişimi, internet hizmetleriyle ilişkilidir.

Siber güvenlik, tanım olarak şu şekilde ifade edilmiştir:[26]

> *Siber güvenlik; siber uzayı oluşturan bilişim sistemlerinin saldırılardan korunmasını, bu ortamda işlenen bilginin/verinin gizliliği, bütünlüğü ve erişilebilirliğinin güvence altına alınmasını, saldırıların ve siber olayların tespit edilmesini, bu tespitlere karşı tepki mekanizmalarının devreye alınmasını ve sonrasında ise sistemlerin yaşanan siber olay öncesi durumlarına geri döndürülmesini kapsayan faaliyetler bütünüdür.*

---

[23] Küresel ortalık, uluslararası hukukta kabul edilen *'İnsanlığın Ortak Mirası (Common Heritage of Mankind)'* ilkesiyle yakından ilişkilidir. İnsanlığın ortak mirası kapsamında kabul edilen bir husus; hiçbir kişi, kurum ya da devlete tahsis edilmemiş, ortak bir idare ile uluslararası toplumun çıkarlarına uygun ve barışçıl amaçlarla kullanılan, askeri ve silahlı çatışmalardan uzak tutulan, toplum yararına elde edilen faydanın adil bir şekilde paylaşıldığı ve bu mirasın gelecek nesillere ulaşması amacıyla korunduğu olguları ifade etmektedir. Bu kapsamda ülkesel sınırları aşan belirli ortak alanlar ve bu alanlardaki doğal kaynaklar, insanlığın ortak mirası olarak görülmektedir. Ayrıntılı bilgi için bkz. Kudirat Magaji W. Owolabi, "The Principle of The Common Heritage of Mankind", **Nnamdi Azikiwe University Journal of International Law and Jurisprudence**, Cilt:4, 2013, ss. 51-56.

[24] François Delerue, **Cyber Operations and International Law**, Cambridge University Press, United Kingdom, 2020, s. 10.

[25] T.C. Ulaştırma ve Altyapı Bakanlığı, **Ulusal Siber Güvenlik Stratejisi ve Eylem Planı 2020-2023**, Ankara, 2020, s. 10.

[26] Ulusal Siber Güvenlik Stratejisi ve Eylem Planı 2020-2023, s. 10.

Siber güvenliğin ihlali sonucunu doğuracak siber saldırıların tanımı şu şekilde yapılmıştır:[27]

> *Siber saldırılar, uzaydaki bilişim ve endüstriyel kontrol sistemlerinin veya bu sistemler tarafından işlenen bilginin/verinin gizliliği, bütünlüğü veya erişilebilirliğini ortadan kaldırmak amacıyla, siber uzayın herhangi bir yerindeki kişi ve/veya bilişim sistemleri tarafından kasıtlı olarak yapılan işlemlerdir.*

Siber olaylar ise, *"Bilişim ve endüstriyel kontrol sistemlerinin veya bu sistemler tarafından işlenen bilginin/verinin gizliliği, bütünlüğü veya erişilebilirliğinin ihlal edilmesi"* olarak tanımlanmıştır.[28] Bu çerçevede, siber saldırı ve siber olayların arasındaki temel farkların zarar verme amacı ve kasıtlı hareket olduğu görülmektedir. Ayrıca, siber olayların siber saldırılara göre yıkım gücünün daha düşük bir seviyede olduğu da net bir şekilde söylenebilecektir.

2. ABD'de Siber Uzaya İlişkin Temel Kavramlar

Birçok teknolojik gelişmeye öncülük eden ABD'de siber uzay oldukça önemlidir. Savunma Bakanlığı Sözlüğü'ndeki tanıma göre, siber uzay, *"internet, telekomünikasyon ağları, bilgisayar sistemleri, gömülü işlemciler ve denetleyiciler dahil olmak üzere; birbirine bağlı bilgi teknolojisi altyapıları ve yerleşik veri ağlarından oluşan bilgi ortamında küresel bir alan"* şeklinde ifade edilmiştir.[29] Bununla birlikte ABD Ordusu'nun 2016-2028 yılları için hazırlamış olduğu *'Siber Uzay Operasyonları Kavram Yetenek Planı'* kitapçığında siber uzayın mevcut durumu için *"hava, kara, deniz ve uzay alanlarının yanındaki beşinci alan"* açıklaması yapılmış, bu beş alanın birbirine bağlı olduğu da ayrıca vurgulanmıştır.[30]

ABD Savunma Bakanlığı tarafından hazırlanan Sözlükteki diğer önemli hususlar ise siber uzay güvenliği ve saldırıların tanımlanması hakkındadır. Siber uzay güvenliği, şu şekilde kaleme alınmıştır:[31]

> *Siber uzayın kullanılabilirliğini, bütünlüğünü sağlamak için; bilgisayarlara, elektronik iletişim sistemlerine ve platform bilgi teknolojisi de dahil olmak üzere diğer bilgi teknolojilerine ve mevcut bilgilere yetkisiz erişimi, bunlardan*

[27] Ulusal Siber Güvenlik Stratejisi ve Eylem Planı 2020-2023, s. 10.
[28] Ulusal Siber Güvenlik Stratejisi ve Eylem Planı 2020-2023, s. 10.
[29] DOD Dictionary of Military and Associated Terms, s. 55.
[30] The United States Army's, **Cyberspace Operations Concept Capability Plan 2016-2028**, United States, 2010, s. 8.
[31] DOD Dictionary of Military and Associated Terms, s. 55.

yararlanılmasını veya tüm bu hususların zarar görmesini önlemek ve korumak amacıyla siber alanda gerçekleştirilen kimlik doğrulama, gizlilik ve inkar edilemezlik şeklindeki eylemler, siber uzay güvenliğini kapsamaktadır.

Siber uzay saldırıları ise, *"siber uzayda fark edilebilir inkâr etkileri (bozulma, aksama veya yıkım) yaratan ve yine siber uzayda gerçekleştirilen eylemler ya da fiziksel bir alanda görünen ve bir tür yangın olarak kabul edilip inkârla sonuçlanan manipülasyonlar"* şeklinde tanımlanmıştır.[32] Kısaca açıklayacak olursak; siber uzayda gerçekleşen ve hem siber uzayda hem de fiziksel bir alanda bozulma, aksama, yıkıma neden olabilecek eylemler siber uzay saldırıları olarak kabul edilmiştir.

3. Kuzey Atlantik Antlaşması Örgütü'nde (NATO) Siber Uzaya İlişkin Temel Kavramlar

II. Dünya Savaşı'nın sona ermesinin ardından güç dengesini ve Batı Bloku'ndaki devletlerin egemenliğini korumak amacıyla, SSCB tehdidine karşı olarak kurulan ve Türkiye'nin de üye bulunduğu NATO, siyasi tarihin en önemli uluslararası kuruluşlarından biridir. 1990'lı yıllardan bu yana siber uzayın karmaşık yapısıyla karşı karşıya olan NATO, siber saldırıları önleyici tedbirler üretebilmek için sıkı bir şekilde çalışmakta, çeşitli yöntem ve stratejiler geliştirmektedir.[33]

1999 yılında gerçekleşen Kosova Müdahalesi'nin ardından üye devletlere yapılan siber saldırılar sonucunda NATO, sahip olduğu gücün devamını sağlamak amacıyla siber savunmayı gündemine almış, konu hakkında çalışacak alt oluşumlar kurmuş ve birçok uluslararası metnin öncülüğünü yapmıştır. NATO Zirvelerinde siber güvenliğin yeni bir askeri alan olarak görüldüğü ve buna yönelik savunma politikalarının izlendiği de açıkça anlaşılmaktadır.[34] Nihayetinde NATO bünyesinde geliştirilen *"Siber Operasyonlara Uygulanacak Uluslararası Hukuk Üzerine Tallinn Kılavuzu"*[35] çerçevesinde siber uzay, *"bilgisayar ağlarını kullanarak veri depolamak,*

[32] DOD Dictionary of Military and Associated Terms, s. 55.

[33] Mehmet Ada ve Hüseyin Çakır, "Kuzey Atlantik Antlaşma Örgütü'nün (NATO) Siber Güvenlik Stratejisinin İncelenmesi", **Düzce Üniversitesi Bilim ve Teknoloji Dergisi**, Cilt:5, Sayı:2, 2017, s. 638.

[34] Ayrıntılı bilgi için bkz. Doğan Şafak Polat, "Nato'nun Yeni Operasyon Alanı: Siber Uzay", **Güvenlik Bilimleri Dergisi**, UGK Özel Sayısı, 2020, ss. 142-150.

[35] The International Group of Experts at the Invitation of The NATO Cooperative Cyber Defence Centre of Excellence, **Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations**,

değiştirmek ve iletmek için fiziksel ve fiziksel olmayan bileşenlerin oluşturduğu ortam" şeklinde tanımlanmaktadır.[36]

Tallinn Kılavuzu; Michael N. Schmitt öncülüğünde 2009 ila 2012 yılları arasında hazırlanmış, 2013 yılında yayınlanmış ve 2017 yılında güncellenmiştir. Siber saldırıların güçlü etkilerinin farkına varıldığı bu dönemde, Tallinn Kılavuzu'nun hazırlanmasında NATO Müşterek Siber Savunma Mükemmeliyet Merkeziyle (Cooperative Cyber Defense Center of Excellence - CCDCOE) birlikte çalışan Uluslararası Uzmanlar Grubu da görev almıştır.[37] Kılavuz, esasında barış zamanında devletlerin siber faaliyetlerine uluslararası hukukun uygulanmasına ilişkin uzun ve önemli bir tartışmanın başlangıcıdır.[38] Bağlayıcı bir nitelik taşımayan, ancak günümüze değin konuyla ilgili olarak hazırlanmış en kapsamlı uluslararası alan çalışması olan Tallinn Kılavuzu, birçok devletin bakış açısını yansıtan ve uluslararası mahiyette önem arz eden bir raporlama niteliği taşımaktadır. Söz konusu metin, çalışmamızın ilerleyen kısımlarında daha ayrıntılı bir şekilde ele alınacaktır.

4. Şanhay İşbirliği Örgütü'nde Siber Uzaya İlişkin Temel Kavramlar

Rusya ve Çin'in öncülük ettiği, söz konusu iki devletle birlikte Kırgızistan, Tacikistan, Kazakistan, Özbekistan, Hindistan ve Pakistan devletlerinden oluşan, Türkiye'nin *'diyalog ortağı'*[39] konumunda bulunduğu Şanghay İşbirliği Örgütü'nün çalışmalarında siber uzay ve siber saldırı için araç temelli bir bakış açısı geliştirilmiştir.[40] Bilgi ve iletişim teknolojilerinin gelişimiyle birlikte, "Şanghay İşbirliği Örgütü Üye Devletleri Arasında Uluslararası Bilgi Güvenliğinin

(Ed. Michael N. Schmitt ve Liis Vihul), 2. Baskı, Cambridge University Press, 2017, (Tallinn Kılavuzu).

[36] Tallinn Kılavuzu, s. 564.

[37] Şener Çelik, "Stuxnet Saldırısı ve ABD'nin Siber Savaş Stratejisi: Uluslararası Hukukta Kuvvet Kullanmaktan Kaçınma İlkesi Çerçevesinde Bir Değerlendirme, **Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi**, Cilt:15, Sayı:1, 2013, s. 163.

[38] Eric Talbot Jensen, "The Tallinn Manual 2.0: Highlights and Insights", **Georgetown Journal of International Law**, Cilt:48, 2017, s. 778.

[39] Diyalog ortaklığı, Şanhay İşbirliği Örgütü'nün 2008 yılında gerçekleştirdiği Duşanbe Zirvesi'nde örgütle irtibat kurmak isteyen ancak gözlemci konumunda olmayan devletler ve uluslararası kurumlar için ihdas edilmiş, örgüte özgü yeni bir kurumsal statüdür. T. C. Dışişleri Bakanlığı, **Şanhay İşbirliği Örgütü (ŞİÖ),** https://www.mfa.gov.tr/sanghay-isbirligi-orgutu.tr.mfa, (02.12.2021).

[40] Mehmet Yayla, "Siber Savaş ve Siber Ortamdaki Kötü Niyetli Hareketlerden Farkı", **Hacettepe Hukuk Fakültesi Dergisi**, Cilt:4, Sayı:2, 2014, s. 191.

Sağlanmasına İlişkin İşbirliği Andlaşması"[41] yapılmıştır. Andlaşma ekinde[42]; bilgi alanı, bilgi güvenliği, bilgi silahları ve bilgi savaşı gibi siber uzayla ilişkili kavramlar için birçok tanım yapılmıştır.[43]

Andlaşma ekine göre bilgi alanı, *"diğer hususların yanı sıra bireysel ve toplumsal bilinç, bilgi altyapısı ve bilginin kendisi üzerinde etkisi olan bilgilerin oluşumu, üretilmesi, dönüştürülmesi, iletilmesi, kullanılması, depolanması ile ilgili faaliyet alanı"* olarak tanımlanmaktadır. Bilgi güvenliği, *"bireylerin, toplumun ve devletin bilgi alanındaki tehditlerden, yıkıcı ve diğer olumsuz etkilerden korundukları durumdaki hal ve çıkarları"* şeklinde ifade edilmektedir. Bilgi silahları, *"bilgi savaşı amacıyla kullanılan bilgi teknolojileri, araçları ve yöntemleri"* anlamına gelmektedir.[44]

Son olarak, Şangay İşbirliği Örgütü tarafından siber saldırı sürecinin tamamını ele alan bilgi savaşı kavramı, şu şekilde açıklanmıştır:[45]

> *Bilgi savaşı, bilgi sistemlerine, süreçlere ve kaynaklara, kritik öneme sahip yapılara ve diğer yapılara zarar vermek, siyasi, ekonomik ve sosyal sistemleri baltalamak, nüfus kitlelerini istikrarsızlaştırmak için psikolojik olarak manipüle etmek amacıyla bilgi alanındaki iki veya daha fazla devlet arasında bir çatışmadır.*

Görüldüğü üzere, devletlerin ulusal sınırlar içerisinde siber güvenliği sağlama ihtiyacı uluslararası ilişkilerde de benzer şekilde kendini göstermiştir. Böylece siber

---

[41] Shanghai Cooperation Organization, **Agreement on Cooperation in Ensuring International Information Security between the Member States of the Shanghai Cooperation Organization**, 2009.

[42] Andlaşma eklerinin hukuki niteliğinin belirlenmesinde 1969 tarihli Viyana Andlaşmalar Hukuku Sözleşmesi hükümleri dikkate alınmaktadır. Türkiye, Viyana Sözleşmesi'ne taraf değildir. Ancak sözleşmenin genel olarak örf ve âdet taşıyan kurallardan oluşması sebebiyle söz konusu kurallara geçmişten beri uymaktadır. Bu çerçevede, Viyana Sözleşmesi'nin andlaşmaların yorumuna ilişkin 31, 32 ve 33. maddeleri incelenmelidir. 31. madde uyarınca andlaşmalar, başlangıç hükümleri ve andlaşma ekleri de dahil olmak üzere bir bütün olarak, andlaşmanın konu ve amacıyla bağlantılı ve iyi niyetli bir şekilde ele alınmalıdır. Bu bütünlük, genel bir bağlam olarak kabul edilmektedir. Ayrıca, ana ana andlaşmayla bağlantılı olduğu takdirde taraflar arasında yapılan diğer andlaşmalar ve belgelerle birlikte yorum yapılmaktadır. Ayrıntılı bilgi için bkz. Oliver Dörr ve Kirsten Schmalenbach (Ed.), **Vienna Convention on the Law of Treaties: A Commentary**, 2. Baskı, Springer, Germany, 2018, ss. 559-582 ve Melda Sur, **Uluslararası Hukukun Esasları**, 15. Baskı, Beta Yayıncılık, İstanbul, 2021, ss. 22, 74.

[43] Shanghai Cooperation Organization, **Agreement on Cooperation in Ensuring International Information Security between the Member States of the Shanghai Cooperation Organization, ANNEX 1 to the Agreement on Cooperation in the Field of Ensuring International Information Security among the Member States of the Shanghai Cooperation Organization**, ss. 9-10, 2009. (ANNEX 1).

[44] Shanghai Cooperation Organization, ANNEX 1, s. 9.

[45] Shanghai Cooperation Organization, ANNEX 1, s. 9.

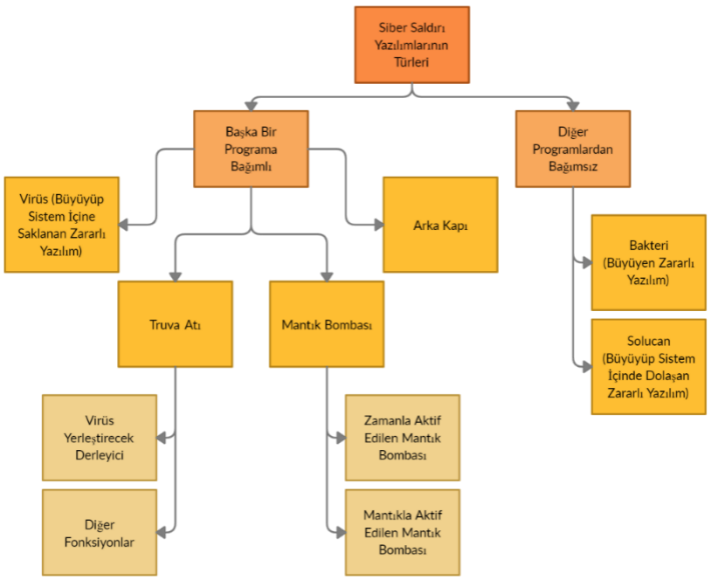
uzayın ve siber uzayla ilgili terimlerin tanımlaması önemli hale gelmiştir. Teknolojinin gelişimi, söz konusu çalışmaları hızlandırmaya devam etmektedir.

III. SİBER SALDIRI ARAÇ VE YÖNTEMLERİ

A. Siber Saldırı Araçları

Siber uzayda bireyleri ve devletleri olumlu olarak etkileyecek faaliyetler gerçekleşebileceği gibi, potansiyel tehdit oluşturacak olumsuz faaliyetler ve siber saldırılar karşımıza çıkabilmektedir. Siber saldırıların birçok türü bulunmaktadır. Bu kapsamda bazı özellikler dikkate alınarak siber saldırı yazılımlarının gruplandırılması yoluna gidilmiştir. Söz konusu gruplandırma, siber eylemlerdeki işleyişi anlamaya yardımcı olmaktadır. Teknik yönü ağır basan bu hususta, temel başlıklar hakkında bilgi vermekle yetineceğiz. Açıklamalarımızın hemen ardından, söz konusu yazılımların araç olarak kullanıldığı temel siber saldırı yöntemlerine de değineceğiz.

Şekil 1: Siber Saldırı Yazılımlarının Türleri



Kaynak: Hasan Çifci, **Her Yönüyle Siber Savaş**, 2. Basım, TÜBİTAK Yayınları, Ankara, 2017, s. 168.

1. Başka Bir Programa Bağımlı Siber Saldırı Yazılımları

a. Virüs (Virus)

Virüsler, kendini daha geniş yapılı programların içine kopya edebilen ve bu programa müdahale etme yetisine sahip olan parçalı kodlardan oluşmaktadır. Bir virüsün aktif hale gelebilmesi için, içinde bulunduğu programın çalışması gerekir. Söz konusu program çalıştığı sürece, virüs kendini tekrarlayarak diğer programların içine de yayılır.[46] Esasen virüsler, çalışma şekli bakımından biyolojik virüslerle benzerlik göstermektedir ve siber eylemlerde sıklıkla kullanılan bir yazılım türüdür.

Virüsler, ekseriyetle uygulama dosyaları olarak karşımıza çıkmaktadır. Bazı virüsler kendini kopyalamak için internet ve yerel ağlara ihtiyaç duyarken, bazıları hard disk, USB disk, CD ve DVD gibi depolama araçlarını kullanabilmektedir. Virüsün etkileriyle birlikte programlardaki birtakım veriler değiştirilir yahut silinir. Bu hususta tehlikenin boyutu; virüsü meydana getiren, programa sızılmasını sağlayan kişinin amacına ve bilgisine göre değişiklik göstermektedir.[47]

David L. Smith tarafından oluşturulan ve 1999 yılında ortaya çıkan Melissa virüsü, e-posta sistemi üzerinden yayılmayı başarmış ilk virüstür. Microsoft Outlook'u kullanan kişiler önemli nitelikteki e-postaların içeriğini merak edip açtıklarında, adres defterindeki kişilerden bir dosya gönderildiğini görüp bilgisayarlarına indirmiştir. Söz konusu dosya açıldıktan sonra, Melissa virüsünün talimatı gereği, kullanıcının adres defterindeki ilk 50 kişiye aynı türde bir e-posta gönderilmiştir. Ayrıca virüs, Microsoft Word şablonuyla oluşturulmuş belgeleri de yok etmiş, yeni oluşturulan belgelere de bulaşmaya devam etmiştir. Melissa virüsü, yaklaşık olarak 1,2 milyon bilgisayara ve 53 bin sunucuya bulaşmış, sorunun düzeltilmesinin ise 249 ila 561 milyon dolar arasında bir rakama mal olacağı hesap edilmiştir.[48]

Günümüz koşullarında bilgisayar sistemlerini kullanılamaz hale getirebilecek, muhtelif donanımlara fiziki zararlar verebilecek gelişmiş ve karmaşık yapılı virüsler

---

[46] Mutlu Çölgeçen, **Siber Savaş: Kıyametin İlk Halkası**, Arşiv Kitapları, Ankara, 2002, s. 38.

[47] Saim Atalay Keleştemur, **Siber İstihbaratın Kamu Güvenliği İçin Rolü ve Önemi**, (Yayınlanmamış Yüksek Lisans Tezi), İstanbul Gedik Üniversitesi Sosyal Bilimler Enstitüsü, İstanbul, 2018, s. 90.

[48] Lee Garber, "Melissa Virus Creates a New Type of Threat", **Computer**, Cilt:32, Sayı:6, 1999, ss. 16-19.

de mevcuttur.[49] Bu sebeple sistemlerin sürekli olarak denetime tabi tutulması, gerekli güvenlik önlemlerinin alınması, bakım ve onarımların aksatılmaması büyük önem arz etmektedir.

b. Truva Atı (Trojan Horse)

Truva atı, yararlı bir programın içine gizlenerek sisteme giren ve gizli bir şekilde sisteme zarar vermeyi hedefleyen parçalı kodlardan oluşmaktadır.[50] Çoğunlukla e-postaların içine yerleştirilerek sisteme sızabilen bu yazılım, içine gizlendiği program çalışana kadar aktifleşmez. Truva atının aktifleşmesi durumunda; korunmasız haldeki ana bilgisayar yazılımı ve sunucular hakkındaki bilgiler ele geçirilerek, Truva atını gizleyen saldırgana gönderilir.[51]

Truva atlarına ilişkin ilginç örneklerden biri, 2005 yılında tespit edilen GPCoder yazılımıdır. GPCoder, Windows sistemlerine bulaşıp belirli uzantılara sahip dosyaları hedef almış, dosyaları bulduktan sonra şifrelemiş ve orijinallerini de sistemden silmiştir. Güçlü bir şifreleme yöntemiyle şifrelenen dosyalara, sistemin sahibi ya da kullanıcıları tarafından erişim sağlanamamıştır. Bununla birlikte, sistemin ana ekranına dosyalara ulaşabilmek için istenen fidye ödemesi ve yapılması gereken diğer şifre kaldırma işlemlerinin ayrıntılarına yönlendiren bir metin dosyası yerleştirilmiştir. Zamanla daha kapsamlı ve karmaşık nitelikteki Archiveus, Krotten, Cryzip ve MayArchive gibi Truva atı yazılımları da ortaya çıkmıştır.[52]

Arka planda sistem yöneticisinin izni ve bilgisi olmadan çeşitli işlemler gerçekleştirebilen Truva atının asıl amacı, mevcut sistemi saldırganın kontrolü altına sokmaktır. Böylece saldırgan, sızdığı sistemde fark edilmeden hareket edip uzaktan saldırılarla daha büyük hasarlara neden olabilmektedir.[53] Zekice oluşturulmuş bir Truva atının kendisini belli etmeden ve iz bırakmadan hareket ettiği göz önüne alınırsa, bu hususta dikkatli olmanın ve sistemi güvende tutmanın ne kadar önemli olduğu aşikârdır.

---

[49] Keleştemur, s. 90 ve Emir, s. 26.
[50] Çifci, s. 171.
[51] Çölgeçen, s. 39.
[52] Soner Çelik ve Barış Çeliktaş, "Güncel Siber Güvenlik Tehditleri: Fidye Yazılımlar", **Cyberpolitik Journal**, Cilt:3, Sayı:5, 2018, s. 113.
[53] Keleştemur, s. 91.

c. Mantık Bombası (Logic Bomb)

Mantık bombası, diğer yazılımlardan farklı olarak, bir programın içine yerleştirilen ve belirli bir zaman yahut tetikleyici koşulun gerçekleşmesine bağlı şekilde aktifleşen bir kötü amaçlı yazılımdır.[54] Kuluçka olarak ifade edilen bekleyişi sırasında zararsız olan mantık bombası, aktifleştikten sonra verileri değiştirme, silme, sistemi kullanılamaz hale getirme, patlatma ve benzeri birçok istenmeyen sonuca sebep olabilir.

Soğuk Savaş döneminin devam ettiği 1982 yılında, bilgisayar teknolojileri ABD Merkezi İstihbarat Teşkilatı (Central Intelligence Agency - CIA) için önemli bir araç haline gelmiştir. Sovyetler Birliği, Kanada'daki bir şirketten doğal gaz boru hatlarını denetleme işlevine sahip bir yazılımı çalmıştır. Ancak bu yazılım esasında CIA tarafından yerleştirilmiş mantık bombasını içeren bir tuzak olduğu anlaşılmıştır. Bilgisayar sistemlerine entegre olarak çalışan bu yazılım, bir süre sonra bozulmuş ve sistemin aklı karışmıştır. Böylece mantık bombası; doğal gaz boru hatlarındaki pompa hızı ve vana ayarlarını sıfırlamış, akışı anormal seviyelere çıkarmış, hat içindeki basıncı yükseltmiştir. Nihayetinde ABD, kontrolden çıkan Sibirya Doğal Gaz Hattı'nı patlatmayı başarmıştır. Sibirya Doğal Gaz Patlaması olarak ABD tarafından üstlenilen bu olay, siber saldırı yazılımlarının ulusal ve uluslararası mahiyette kullanıldığı ilk uygulama niteliğindedir. Ayrıca bu patlama, şimdiye kadar görülmüş en büyük nükleer olmayan patlama olarak ifade edilmiştir.[55]

Mantık bombası, birçok şekilde sisteme sızdırılabilir. Bu sebeple önlenmesi ve tespit edilmesi zordur. Güvenlik yazılımlarıyla sistemin belirli aralıklarla taranması mantık bombalarını ortadan kaldırmakta işe yarayan bir çözüm olsa da anlık saldırılarda bir garanti sunulamamaktadır.[56] Tüm bu sebeplerle anlık ve periyodik kontrollere dikkat edilmesi, güvenlik güncellemelerinin yapılması ve mantık bombaları tespit edilirse imha sürecinin gerçekleştirilmesi önem arz etmektedir.

---

[54] Emir, s. 26.

[55] Alexander Klimburg, "Mobilising Cyber Power", **Survival**, Cilt:53, Sayı:1, 2011, s. 42. ve Miron Lakomy, "The Significance of Cyberspace in Canadian Security Policy", **Central European Journal of International and Security Studies**, Cilt:7, Sayı:2, 2013, s. 104.

[56] Tokdaş, s. 38.

d. Arka Kapı (Backdoor/Trapdoor)

Arka kapı ya da tuzak kapısı, bir sistemin içine yaratıcısı tarafından yahut onun rızasıyla yerleştirilen bir mekanizmadır. Arka kapının amacı, normal seyrinde işleyen sistemin koruyucularının basit bir şekilde aşılmasını ve sistemi kurup arka kapıyı yerleştiren saldırganın rahatça içeri sızabilmesini sağlamaktır.[57]

Belirli aralıklarla gerçekleştirilen incelemelerde dahi tespiti mümkün olmayan arka kapılar sayesinde saldırgan, sisteme giriş yapıp mevcut veri ve bilgileri elde etme, değiştirme, silme olanağına sahiptir.[58] Saldırgan, sistemin kullanıcısı gibi bizzat sistemi kullanabilmektedir.

Arka kapılarla ilgili en ünlü iddialardan biri, Microsoft şirketinin Windows işletim sistemlerini geliştirirken ABD Milli Güvenlik Ajansı'ndan (National Security Agency - NSA) yardım almış olması ve bu yardıma karşılık sistemlere arka kapı eklemesidir.[59] Bu çerçevede, tescilli bir programa dahi tam olarak güvenilmemesi gerektiği rahatlıkla söylenebilir. Bir programın yazılımlarında kötü amaçlı kodların bulunup bulunmadığını tespit etmek, sıradan bir kullanıcı için neredeyse imkânsızdır.

Muhtelif programlara bağlı bir şekilde bilgi sistemlerine sızan ve kendini iyi bir şekilde gizleyebilen yazılımların sebep olabileceği yıkımlar karşısında son derece dikkatli olmak gerekmektedir. Bu kapsamda, alanında uzman kişiler tarafından, mevcut yazılımlar için rutin kontrollerin gerçekleştirilmesi ve güçlendirme çalışmalarının yapılması önem arz etmektedir.

2. Diğer Programlardan Bağımsız Siber Saldırı Yazılımları

a. Bakteri (Bacterium)

Bakteriler, bağımsız olarak çoğalabilen ve sızmayı hedeflediği sistemde farklı versiyonlarını oluşturabilen kötü amaçlı yazılımlardır. Sürekli artarak oluşan her yeni versiyon, disk üzerinde daha fazla yer kaplayarak çalışma işleyişini zayıflatmaktadır.

---

[57] Çölgeçen, s. 40.
[58] Çifci, s. 172.
[59] Salih Bıçakcı, "NATO'nun Gelişen Tehdit Algısı: 21. Yüzyılda Siber Güvenlik", **Uluslararası İlişkiler**, Cilt:10, Sayı:40, 2014, s. 109.

Sistem kaynaklarının bu şekilde kullanılması, işletim sistemini olumsuz etkilemekte ve nihayetinde tüm alan dolduğunda sistem kullanılamaz hale gelmektedir.[60]

b. Solucan (Worm)

Solucan, bir sistemde bağımsız olarak varlığını sürdürebilen ve kendini kopyalayarak farklı sistemlere de yayılabilen bir siber saldırı yazılımıdır. İçinde bulunduğu sisteme bağlanan depolama ve ağ aygıtlarına hızlı bir şekilde kopyalanabilmektedir.[61]

Solucanların en önemli özelliği oluşturulmaları haricinde hiçbir insan etkileşimine ihtiyaç duymamasıdır.[62] Sistemde kendiliğinden bir tünel oluşturarak, sistemin uzaktan kontrol edilmesi yolunu açmaktadır. Bu durum ağların çökmesi, bağlantıların kopması, sistemin yavaşlaması ve kilitlenmesi sonuçlarını doğurabilmektedir.[63]

1988 yılında ilk bilgisayar solucanı karşımıza çıkmıştır. ABD'de bilgisayar sistemlerinin ilk örneklerinden olan 6000 bilgisayar terminalinde bazı sorunlar ortaya çıkmıştır. Kullanıcılar bilgisayar terminallerini kullanamamış ve sistemler de iş yapamaz hale gelmiştir. Olayın nereden kaynaklandığı araştırıldığında, Robert Morris isimli bir kişinin oluşturup internete bıraktığı solucan programı tespit edilmiştir.[64] İfadesinde kendini kanıtlamak ve eğlenmek istediğini söyleyen bu kişinin eylemi sonucunda, sistem kontrolden çıkmış, internet ağı çökmüş ve 98 milyon dolarlık bir zarar meydana gelmiştir.[65] Ayrıca, gerçekleştiğinde uluslararası çapta büyük etkileri olan Conficker, Slammer gibi solucanların kullanıldığı önemli örnekler de bulunmaktadır.[66]

---

[60] Keleştemur, ss. 94-95.
[61] Keleştemur, s. 94.
[62] Emir, s. 25.
[63] Tokdaş, s. 35.
[64] Aşır Sertçelik, "Siber Olaylar Ekseninde Siber Güvenliği Anlamak", **Medeniyet Araştırmaları Dergisi**, Cilt:2, Sayı:3, 2015, s. 31.
[65] Mustafa Güneş ve Ahmet Alabacak, "Bilgisayar Virüsleri", **D.E.Ü. İ.İ.B.F. Dergisi**, Cilt:11, Sayı:2, 1996, s. 239.
[66] Çifci, s. 169.

B. Başlıca Siber Saldırı Yöntemleri

1. Hizmet Engelleme (Denial of Service - DoS/DDoS)

En yıkıcı siber saldırılardan biri olan hizmet engelleme, internet üzerinden verilen bir hizmete bağlı sistem ya da ağın kullanılamaz hale getirilmesidir. Bu saldırı sunucu, aygıt, hizmet, ağ, uygulama ve uygulama içindeki özel işlemleri engellemek suretiyle gerçekleştirilmektedir. Başlangıçta, hizmet sağlayan sunucu sisteme gerçekte var olmayan talepler göndererek sistemin işlem alanını doldurur. Aşırı veri ve bilgi istemlerine cevap veremeyen sistem kilitlenir ya da çöker.[67] Hizmet engelleme saldırılarının birden fazla kaynak üzerinden tek bir hedefe yöneltilmesi halinde Dağıtılmış Hizmet Engelleme (Distributed Denial of Service – DDoS) saldırısından söz edilmektedir. Bu tür saldırılarda yüzlerce hatta binlerce makineden tek bir sistemi tamamen çökertmek amaçlanmaktadır.[68]

Hizmet engelleme saldırıları genellikle hükümet, ticaret, bankacılık ve medya kuruluşlarının web sunucularına yönelik bir şekilde gerçekleştirilmektedir. Bu çerçevede saldırının ortadan kaldırılıp sunucuların tekrar normal seyrine döndürülmesi sürecinde birçok mali kayıp yaşanmaktadır.[69] Kritik siber altyapıların ve kontrol sistemlerinin zarar görmemesi adına gerekli özverinin gösterilmesi, kalıcı hasarların önüne geçmek için önem arz etmektedir.

2. Zombi/Köle Bilgisayar (Botnet)

Zombi/köle bilgisayar, sahibinin haberi olmaksızın saldırganlar tarafından kullanılabilen ve siber saldırı yazılımlarının içine sızmış olduğu sistemdir. Birbirine bağlı bulunan zombi bilgisayar ağları, genellikle kötü amaçlı yazılımların yayılmasını sağlamak ve siber suç eylemlerini gerçekleştirmek için kullanılır. Siber saldırı

---

[67] Can Bolat, **Siber Saldırılara Karşı Meşru Müdafaa Hakkının Uluslararası Hukuk Açısından İncelenmesi**, (Yayınlanmamış Yüksek Lisans Tezi), İstanbul Üniversitesi Sosyal Bilimler Enstitüsü, İstanbul, 2020, s. 29.

[68] Keleştemur, ss. 98-99.

[69] James Graham, Richard Howard ve Ryan Olson (Ed.), **Cyber Security Essentials**, CRC Press, 2011, s. 159 ve Abdulkadir Bilen, **Akıllı Yöntemler ile Siber Saldırı Tespit Sistemi Geliştirilmesi**, (Yayınlanmamış Yüksek Lisans Tezi), Fırat Üniversitesi Fen Bilimleri Enstitüsü, Elazığ, 2021, s. 11.

gerçekleştirmek amacıyla ele geçirilen zombi bilgisayar grubu, *'botmaster'* adı verilen bir yönetici tarafından komuta edilir. Botmaster, söz konusu bilgisayarları altyapısının yettiği alan boyunca komutlar ve saldırı emri verildiğinde saldırmaya hazır bekleyen bir ordu haline getirir.[70]

Günümüzde en tehlikeli siber saldırı yöntemlerinden biri olarak kabul edilen zombi bilgisayar; açık etki bırakan, zekice kurgulandığı takdirde geniş ve planlı bilgisayar gruplarıyla harekete geçilebilen bir kullanım alanına sahiptir. Kişisel bilgisayarlarda gerekli güvenlik önlemi alınmadığı takdirde, kullanıcılardan habersiz birçok siber suçun kolayca işlenebileceği ve mağduriyetlere sebep olabileceği unutulmamalıdır.

3. Yetki Artırımı (Privilege Escalation)

Yetki artırımı, siber saldırıların yolunu açan önemli adımlardan biridir. Saldırganlar, hedef sistemdeki yönetici ya da geliştiricilerin erişimini elde etmek yahut bu kişilerin sistemdeki ayrıcalıklarını kullanabilmek amacıyla güvenlik açıklarından faydalanmaktadır. Nihayetinde saldırgan, yetkilendirme kodlarını ele geçirerek istediği zaman sisteme sızabileceği bir konuma gelir. Böylece sistemdeki uygulamalara zarar verebilir, mevcut kodları değiştirebilir, sistemin gerçek kullanıcılarının erişimini engelleyebilir ve daha ötesinde yöneticinin şifrelerine ulaşarak sistemi tamamen bozabilir.[71]

4. Sosyal Mühendislik (Social Engineering)

Sosyal mühendislik, güvenlik sistemlerindeki en zayıf bileşen olarak bireylerin görülmesi üzerine kullanılan bir siber saldırı yöntemidir. Bireyler bu süreçte sosyal mühendis tarafından etkileme, aldatma, zorlama, dürüstlüğü ya da bağlılığı azaltma faaliyetlerine maruz kalarak; erişim sağladığı sistemle ilgili veri ve bilgileri aktarmaktadır. Böylece sosyal mühendis, sistem güvenliğini insan faktörü aracılığıyla

[70] Tokdaş, s. 38.
[71] Bolat, s. 30.

aşarak hedefine erişim sağlamakta ve dolaylı olarak itibar zedelenmesine sebep olmaktadır.[72]

Sosyal mühendisin asıl amacı, sisteme erişim sağladıktan sonra bilgisayar korsanlarının verileri silme, bozma, çıkarma ve sistemi kullanılamaz hale getirme çalışmalarına izin vermektir.[73] Fiziki güvenlik açıkları ve psikolojik zayıflıklardan yararlanmayı iyi bilen sosyal mühendisler, son derece tehlikelidir. Ancak vurgulamak gerekir ki, sosyal mühendislik çalışmaları tek başına bir anlam ifade etmez, siber uzaydaki diğer araç ve yöntemlerle desteklenmesi gerekir.

5. Gelişmiş Sürekli Tehditler (Advanced Persistent Threats)

Son birkaç yıldır adından söz ettiren gelişmiş sürekli tehditler, tamamen hedefe odaklı, iyi organize edilmiş, uzun bir sürece yayılan ve arkasında büyük destekler barındıran bir saldırı yapılanmasıdır. Hedef alınan sistemi başarılı bir şekilde ele geçirmeden durmayan bu saldırının esas amacı, tam erişime sahip olarak veri elde etmektir. Gizli, odaklı, çok yönlü ve uyarlanabilir bu saldırılar sürekli dönüşüm içindedir.[74]

Gelişmiş sürekli tehditler, diğer siber saldırılardan farklı olarak önceden belirlenmiş ve üzerinde araştırma yapılmış bir hedefe yönelik, sisteme giriş yaptıktan sonra öğrenme, yayılma ve gizli bilgileri elde etme amacı taşıyan, herhangi bir program ya da ağ bağlantısı gerektirmeyen ve kendi kendini gizleyip uzun süre saldırıyı devam ettirebilen bir oluşumdur.[75] Keşif, hazırlık, hedef saptama, erişim elde edip sürekli hale getirme, veri toplama ve sızdırma aşamalarıyla geniş ölçekli bir proje niteliğinde olan bu tehdide karşı olabildiğince yoğun önlemler alınmalıdır.

Devletlerin ulusal sınırlar içerisinde siber güvenliği sağlama ihtiyacı uluslararası ilişkilerde de benzer şekilde kendini göstermiş, bu alanın tanımlanması ve sınırların çizilmesi önemli hale gelmiştir. Bu kapsamda söz konusu siber saldırı

---

[72] Hasan Bağcı, "Sosyal Mühendislik ve Denetim", **Denetişim**, Sayı:1, 2009, s. 43.

[73] Tim Thornburgh, "Social Engineering: The "Dark Art"", **1st Annual Conference on Information Security Curriculum Development**, 2004, s. 134.

[74] Murat Akın ve Şeref Sağıroğlu, "Gelişmiş Sürekli Tehditler", **Türkiye Bilişim Vakfı Bilgisayar Bilimleri ve Mühendisliği Dergisi**, Cilt:10, Sayı:1, 2017, ss. 1-2.

[75] Eric D. Knapp ve Joel Thomas Langill, **Industrial Network Security**, Second Edition, Elsevier Inc., Waltham, 2015, ss. 47-48.

yazılım ve yöntemlerine karşı iç ve dış aktörler iyi tanınmalı, güvenlik önlemleri artırılmalı ve mevcut düzenlemeler somut etkilerle desteklenmelidir.

IV. SİBER AKTÖRLER

Siber aktör, siber uzayda var olan ve faaliyete geçip siber uzayda değişiklik yaratabilme yetisine sahip olan kişi, kurum ve devletlerin bütününe verilebilecek isimdir. Devletler bu hususta en büyük paydada söz sahibi olan ve siber faaliyet sürecini yönlendiren aktör konumundayken, devlet dışı aktörlerin önemi de yadsınamayacak kadar büyüktür. Devletler ve devlet dışı aktörler arasındaki sınırlar siber uzayda belirsiz hale gelebilmektedir. Devletler, uluslararası kurumlar ve devlet dışı aktörler, iyi ve kötü birçok amaçla siber uzayda varlıklarını göstermektedir.

Siber uzayda uluslararası sorumluluk ve isnadiyet, siber eylemi gerçekleştiren kişinin ve konumunun tespiti sürecinde önemlidir. Siber uzayda gerçekleştirilen eylemler, coğrafi sınırlamalara tabi olmadan devletler arasında sorumluluğa ilişkin sorunlara yol açabilmektedir. Bu sebeple siber faaliyetlere ilişkin bağlantı noktaları, devletlerin dikkat etmesi gereken konulardan biridir.

Toplumu oluşturan bireyler, ağ altyapısı ve internet aracılığıyla devletlerin sınırını aşan etkileşimlerde bulunabilmekte ve sosyalleşebilmektedir.[76] Bu sebeple, siber uzayda politika geliştirme ve mevcut siyasi oluşuma entegre etme yolunda, bireylerin etkinlikleri de göz önüne alınmalıdır. Nitekim bireylerin siber faaliyetlere yönelik tutum ve davranışları, herhangi bir devlet içinde dahi ciddi karışıklıklara yol açabilmektedir.

Devlet, devlet dışı aktör ve birey sınıflandırmasını büyük ölçüde değiştiren siber uzayda; net bir sınıflandırma yapmak zordur.[77] Esasen siber uzayda sınırları belirlemek, siber uzayın mahiyeti ve şahsına münhasır doğası sebebiyle her somut olayda farklılık göstermektedir. Ancak yine de devletler ve devlet dışı aktörler temelinde bir ayrımla bu hususu incelemek daha kolay olacaktır.

---

[76] Sevda Korhan, "Siber Uzayda Aktör - Güç İlişkisi", **Cyberpolitik Journal**, Cilt:2, Sayı:4, 2018, s. 79 (Aktör - Güç İlişkisi).

[77] Vahit Güntay, "Siber Güvenliğin Uluslararası Politikada Etki Aracına Dönüşmesi ve Uluslararası Aktörler", **Güvenlik Stratejileri Dergisi**, Y. 14, Sayı:27, 2018, s. 95.

A. Devletler

Devletlerin temel aktör olarak karşımıza çıktığı uluslararası arena; egemenlik ve dış politika etkenleriyle yakından ilişkilidir. Resmi faaliyetler aracılığıyla kendini gösteren ve varlığını sürdüren devletler için siber uzay, egemenlik düşüncesini ve ulusal sınırları farklı bir açıdan ele almaya zorlayan, yeni bir oluşumdur. Klasik bakış açısının değişmesindeki temel husus ise, siber uzayın kendine has özellikleriyle devletlere de zarar verebilecek niteliğe sahip olmasıdır.[78]

Küreselleşmeyle birlikte insan hakları, çevre, ekonomi, küresel ısınma gibi alanlardaki ulusal sınırları aşan belli başlı sorunların çözümünde uluslararası işbirliği önem kazanmıştır. Teknoloji ve iletişimdeki yenilikçi gelişmelerle gündemdeki yerini koruyan siber uzaydaki sorunların da bu kapsamda değerlendirilmesi gerekmektedir. Geleneksel silahlı saldırıların aksine siber uzayda gerçekleşen saldırılar, kural ve engel tanıma konusunda daha esnektir. Nitekim devletlerin ulusal ağ altyapılarını korumak ve güçlendirmek amacıyla gerçekleştirdiği eylemlerin çoğu; özel sektör, hizmet sağlayıcıları, uzmanlar, sanayileşmiş ülke grupları ve işbirliği sağlanan hükümetler arasında karşılıklı adımlarla hayata geçmektedir.[79] Bu noktada devletler ve diğer siber aktörler arasındaki ince çizginin belirsizleştiği ve ülkesel sınırların önemsiz hale geldiği rahatlıkla söylenebilir.

Uluslararası işbirliğinin yanında devletler, güvenlik amaçlı bir yaklaşımla siber uzayda devamlılığını sağlama çabasındadır. İnternet altyapısına ve siber uzaya olan bağımlılıkla orantılı olarak; devletlerin bu ortamdaki faaliyetlerden etkilendiği ve politikalarını söz konusu etkenlere uygun şekillendirdiği görülmektedir.[80] Birçok devlet tarafından *'beşinci muharebe alanı'* olarak görülmeye başlanan siber uzaydaki rekabetin sonucunda; siber ordulara, savunma ve istihbarat sistemlerine önemli ölçüde yatırım yapılmaktadır.[81] Mücadelede etkin rol oynayacak bu emir-komuta zinciri siber savaşı takip etme ve harp teknikleri geliştirme hususlarında görevlendirilmektedir.[82]

---

[78] Güntay, s. 96.
[79] Sai Felicia Krishna-Hensel, "Preface", **Power and Security in the Information Age: Investigating the Role of the State in Cyberspace**, (Ed. Myriam Dunn Cavelty, Victor Mauer ve Sai Felicia Krishna-Hensel), Ashgate Publishing, 2007, s. xi.
[80] Güntay, s. 97.
[81] Korhan, Aktör - Güç İlişkisi, s. 80.
[82] Güntay, s. 100.

Siber ordu, savunma ve istihbarat yapılanmaları, bizzat devlet tarafından oluşturulan ve resmi olarak kullanılan birimler olabileceği gibi; devlet tarafından desteklenen ancak resmi niteliğe sahip olmayan gönüllü birimlerden de oluşabilmektedir.[83] Siber uzaydan gelebilecek tehdit ve saldırılara karşı koruma sağlayacak ve gerektiğinde karşılık verebilecek yetenekteki bilgi güvenliği uzmanlarının çalıştığı bu yapılanmalar, devletin her kurumunu koruyan görünmez bir el gibidir.

B. Uluslararası Kurumlar ve Devlet Dışı Aktörler

Uluslararası hukuk ve politikada devletlerden sonra gelen devlet dışı yapılanmalar, genellikle uluslararası kurumlar olarak karşımıza çıkmakta ve uluslararası kuralların oluşturulmasında rol oynamaktadır. Ancak siber uzayda devlet dışı aktör kavramı, daha geniş bir topluluğu tanımlamak üzere kullanılmaktadır. Siber uzayda bireysel amaç ve dokunuşlarla değişiklik yapabilen her kişi ve kurum, devlet dışı aktörlerin bir parçasıdır. Nitekim devlet dışı aktörler siber uzaya ilişkin düzenlemelerin ortaya çıkarılmasında arka planda olsa da siber saldırılar söz konusu olduğunda roller değişmektedir.

Siber uzaydaki aktörlerin kendilerine özgü amaçlarla eyleme geçebildiği noktada, her birinin bağımsız bir şekilde dikkate alınması gerektiği aşikârdır. Nitekim tüm siber aktörler, siber uzaydaki sanal ortamı etkileyebilecek niteliğe sahiptir. Bu sebeple, söz konusu aktörlerin ulusal ve uluslararası güvenliği de göz önüne alarak açıklanması oldukça önemlidir. Böylece siber uzayda tehlike yaratabilecek kişiler gözden kaçırılmayacaktır.

Siber uzaydaki devlet dışı aktörlerin hangi etken, hedef ve yöntem üzerinde faaliyetlerde bulunduğuna ilişkin *Johan Sigholm*'ün sınıflandırması oldukça yeterli ve bilgilendiricidir. Söz konusu içerik ile devlet dışı aktörlerin özellikleri itibariyle hangi şekilde harekete geçebileceğine ilişkin bir şematik düzen oluşturulmuştur. İlgili sınıflandırma şu şekildedir:

[83] Güntay, s. 100.

Tablo 1: Devlet Dışı Siber Aktörler

Aktör	Etken	Hedef	Yöntem
Sıradan vatandaşlar	Yok (veya zayıf)	Herhangi bir şey	Dolaylı yöntemler
İnternetle ilgili yeterince bilgisi olmayan, tehlikeli kişiler (script kiddies)	Merak, heyecan, ego	Bireyler, şirketler, hükümetler	Daha öncesinde yazılmış komut dosyaları ve araçlar
Bilgisayar eylemcileri (hacktivists)	Siyasi veya sosyal değişim	Karar verme mercileri veya masum kurbanlar	Ağ protestoları, sayfa tahrifleri veya DDoS saldırıları
Siyah şapkalı bilgisayar korsanları (black-hat hackers)	Ego, kişisel düşmanlık, ekonomik kazanç	Herhangi bir şey	Kötü amaçlı yazılımlar, virüsler, güvenlik açığı istismarları
Beyaz şapkalı bilgisayar korsanları (white-hat hackers)	İdealizm, yaratıcılık, kanuna saygı	Herhangi bir şey	Sızma (penetrasyon) testi, yama
Gri şapkalı bilgisayar korsanları (grey-hat hackers)	Belirsiz	Herhangi bir şey	Değişken
Vatansever bilgisayar korsanları (patriot hackers)	Vatanseverlik	Kendi ulus devletinin düşmanları	DDoS saldırıları veya tahrifler
Siber üyeler	Finansal kazanç, intikam, şikayet	İşveren	Sosyal mühendislik, arka kapılar, manipülasyon
Siber teröristler	Siyasi veya sosyal değişim	Masum kurbanlar	Bilgisayar tabanlı şiddet veya yıkım
Kötü amaçlı yazılım yazarları	Ekonomik kazanç, ego, kişisel düşmanlık	Herhangi bir şey	Güvenlik açığı istismarları
Siber dolandırıcılar	Finansal kazanç	Bireyler, küçük şirketler	Sosyal mühendislik
Organize siber suçlular	Finansal kazanç	Bireyler, şirketler	Dolandırıcılık için kullanılan kötü amaçlı yazılımlar, kimlik hırsızlığı, şantaj için DDoS saldırıları
Şirketler	Finansal kazanç	Bilgi ve iletişim teknolojisi tabanlı sistemler ve altyapılar (özel veya genel)	Saldırı veya etki operasyonları için çeşitli teknikler
Siber casusluk ajanları	Finansal ve siyasi kazanç	Bireyler, şirketler, hükümetler	Bilgi elde etmek için çeşitli teknikler
Siber savaşçılar/milisler	Vatanseverlik, profesyonel gelişim	Kendi ulus devletinin düşmanları	Grup yetenekleri

Kaynak: Johan Sigholm, "Non-State Actors in Cyberspace Operations", **Journal of Military Studies**, Cilt:4, Sayı:1, 2016, s. 11.

Görüldüğü üzere, devletlerle herhangi bir bağı ya da devlet desteği bulunmayan her aktör, devlet dışı siber aktörler kategorisine girmektedir. Söz konusu aktörler

olumlu sonuçlar ortaya çıkarabileceği gibi, olumsuz sonuçlara da sebep olmaktadır. Çalışmamız kapsamında devletle ilgili sorunlara ve uluslararası uyuşmazlıklara sebep olabilecek aktörleri daha yakından inceleyeceğiz. Her devlette farklı tanımları ve yasal çerçeveleri olan bu aktörler hakkında, genel kabule göre açıklamalarımızı aktaracağız.

1. Bilgisayar Eylemcileri (Hacktivists)

Bilgisayar eylemciliği, siber uzay kaynaklarının yasal yahut yasa dışı yollarla genel bir protesto aracı olarak kullanılması, daha önceden ifade edilmiş bir ideolojinin herkese aktarılması ya da politik gündemin teşvik edilmesi için harekete geçmektir. Dolaylı olarak gizli, siyasi, askeri ya da ticari amaçlar güden bilgisayar eylemcileri; internet sitelerini tahrif etmek, internet kaynaklarını yönlendirmek, hizmet reddi saldırıları düzenlemek, bilgi hırsızlığı yapmak, internet sitesi parodileri kullanmak ve sanal siteler açmak suretiyle yıkıcı faaliyetlerde bulunur.[84]

Bilgisayar eylemcilerinin temel amacı, siyasi, sosyal veya dini fikirleri etkileyip değişmesini sağlamaktır. Günümüzde ifade özgürlüğü, medeni haklar, dini haklar ve sair konularda halkı protestoya davet eden her eylemin bir noktada bilgisayar eylemcilerine bağlandığını söylemek gerekir.[85] Bilgisayar eylemcileri, sivil itaatsizliği benimseyenlerin ve sorgulayıcıların siber uzaydaki yansımasıdır.

2. Bilgisayar Korsanları (Hackers)

Bilgisayar korsanı, teknik bir problem olarak gördüğü herhangi bir hususu çözüme kavuşturmak için bilgisayar ve ağ iletişimindeki yeteneklerini kullanan kişidir. Genellikle suç oluşturan eylemlerde yeteneklerini kullanan bilgisayar korsanları, sistemlere yahut ağlara yönelik yetkisiz erişim elde etme amacındadır.[86] Yetenek, bilgi birikimi ve niyetlerine göre şapka rengiyle sınıflandırılan bilgisayar korsanları; siyah, beyaz ve gri şapkalı olmak üzere alt kategorilere ayrılmaktadır.

---

[84] Sigholm, s. 14.
[85] Jason Andress ve Steve Winterfeld, **Cyber Warfare: Techniques, Tactics and Tools for Security Practitioners**, Second Edition, Elsevier Inc., 2014, s. 211.
[86] Bolat, ss. 18-19.

Siyah şapkalı bilgisayar korsanları, bilgisayar sistem ve ağlarını kendi amaç ve çıkarları çerçevesinde kullanan kişilerdir. Güvenlik açıklarını bulup istismar eden bilgisayar korsanları, maddi ya da manevi olarak tatmin olacağı eylemlere girişmektedir. Söz konusu korsanlar, kanunlar, bozulan sistemler ve kurbanlar bakımından doğacak sonuçlara saygı duymadan hareket etmekte ve bu kapsamda bilgisayar korsanlarının arasındaki en kötü niyetli aktör olarak görülmektedir.[87]

Beyaz şapkalı bilgisayar korsanları, etiğe önem veren ve yüksek ahlaki değerlere sahip olan; siyah şapkalı bilgisayar korsanlarını engellemek amaçlı hareket eden kişilerdir. Bu kişiler, sistemdeki güvenlik açıklarını kaldırarak olası sorunların önüne geçmek amaçlı çalışmaktadır. Mevcut sistemi sızma (penetrasyon) testine tabi tutarak güçlendirmek, sistemin güvenliğini sağlamak ve kullanıcıları doğrulama yöntemlerini geliştirmek; beyaz şapkalı bilgisayar korsanlarının görevidir. Nihayetinde bir sorun tespit edilirse, sistem sahibi yahut yönetici uyarılarak sisteme yama yapılması gündeme gelebilmektedir.[88]

Gri şapkalı bilgisayar korsanları, siyah şapkalı korsanlardaki kötü niyet olmaksızın hareket eden, çoğu zaman beyaz şapkalı korsan standartlarına uyan ve esasen mevcut sistemi korumak amaçlı çalışan kişilerdir. Ancak bu kişiler amaç ve çıkarlarına aykırı bir sorun tespit ettiğinde, bunu bertaraf etmek adına çalışabilmekte ve kanuni sınırları aşabilmektedir.[89]

Şapkalı korsanlardan farklı olarak, vatansever bilgisayar korsanları olarak adlandırılan bir alt kategori de mevcuttur. Vatansever bilgisayar korsanları, kendi ulus devletine dış dünyadaki bir çatışma ya da savaşta yardım etme amacı güden bağımsız kişilerdir.[90] Bu kişiler, diğer bilgisayar korsanlarıyla aynı amaçlarda hareket etmekte ancak daha milliyetçi davranışlar sergilemektedir. Ayrıca, bilgisayar eylemcilerinden daha keskin ve yönlendirilmiş bir yapıda olduklarını da belirtmek gerekir.[91] Bilgisayar korsanları, iyi ve kötü birçok amaçla siber uzayda faaliyet gösterebilmekte, bu sebeple somut olayda rollerinin tespit edilmesi ve kendilerine karşı önlem alınması önem arz etmektedir.

[87] Andress ve Winterfeld, s. 210 ve Sigholm, s. 15.
[88] Sigholm, s. 16.
[89] Sigholm, s. 16.
[90] Sigholm, s. 16.
[91] Andress ve Winterfeld, s. 211.

3. Siber Teröristler

Siber teröristler, hakkında birçok tartışma söz konusu olan, oldukça karmaşık ve kışkırtıcı bir siber aktör grubudur. Bu kişiler, siyasi hedefler ya da ideolojiler doğrultusunda bir devleti etkilemek amacıyla hareket etmektedir. Siber teröristler, halk içinde korku, panik ve kafa karışıklığı yaratan eylemleri siber uzayda bilgisayar ve ağ teknolojilerinin kullanılmasıyla gerçekleştirmektedir.[92]

Siber terörizm, anonimlik, büyük zarar potansiyeli, psikolojik etki ve medyanın ilgisini çekme hususlarıyla birlikte değerlendirildiğinde; modern teröristler için cazip bir seçenektir.[93] Siber terörizm eylemlerinin ölçeği ve yoğunluğu göz önüne alındığında, bilgisayar eylemcileri ve korsanlardan daha büyük bir yıkım yaratabileceği ortadadır. Geleneksel terör kavramlarında da olduğu gibi; herkes tarafından bilinen, aleni ve yaygın hedefler tercih edilerek devletin güç ve egemenliğinin tehdit edildiği görülmektedir. Bu sebeple başarılı olabilecek saldırılara karşı gerekli önlemler alınmalı ve siber terörizmin önüne geçilecek adımlar atılmalıdır.

4. Organize Siber Suçlular

Siber suçlular, suç işlerken bilgisayar ve ağ teknolojilerini araç ya da hedef olarak gören kişilerdir. Bu kişiler virüs yaymak, bilgi hırsızlığı yapmak ve sair kötü amaçlarla sistemlere saldırıp mağduriyet yaratmaktadır. Böylece, dolandırıcılık ve yasa dışı bahis gibi suçlara sıradan kişiler de alet olmaktadır. Organize bir şekilde grup olarak çalışan siber suç şebekeleri; suçu asıl olarak yönlendiren bir liderden, siber suçları planlayanlardan, emir-komuta zinciriyle roller üstlenen ve etkili iletişim halinde olan kişilerden oluşmaktadır.[94] Siber suçun boyutuna ve etki alanına göre devletler ve uluslararası ilişkiler bu suçlardan etkilenebilmektedir. Bu kapsamda Türkiye'nin de taraf olduğu *"Avrupa Konseyi Sanal Ortamda İşlenen Suçlar Sözleşmesi"*[95] ile siber suçlarla mücadelede uluslararası işbirliği sağlanmaktadır.

---

[92] Andress ve Winterfeld, s. 212.
[93] Gabriel Weimann, "Cyberterrorism: How Real is the Threat?" **United States Institute of Peace**, Special Report 119, 2004, s. 1.
[94] Bolat, ss. 19-20.
[95] Avrupa Konseyi Sanal Ortamda İşlenen Suçlar Sözleşmesi, RG 09.08.2014, Sayı:29083.

5. Şirketler

Siber uzayda faaliyet gösteren şirketler, kanuni düzenlemelere uyan ve siber ekonomik gücü elinde bulunduran yönlendiriciler konumundadır. Bu şirketler, genellikle bir devletin talebi üzerine, hükümet sözleşmesiyle yahut korumasıyla özerk bir şekilde eylemlerini sürdürmektedir. Devlete bağlı istihbarat teşkilatları, paravan olarak kurumsal şirketleri de kullanabilmektedir.[96]

Daha büyük çaplı ve piyasaya hâkim şirketler, teknik endüstride iyi organize olmuş ve eğitimli çalışanlarla hizmet vermektedir. Bununla birlikte siber uzayda söz sahibi olacak teknoloji, donanım ve küresel iletişim altyapısına ilişkin güç ve kaynakları elinde bulundurmaktadır.[97] Bu tür büyük şirketlerin uluslararası ilişkilerdeki stratejik önemi yadsınamayacak kadar büyüktür.

6. Siber Casusluk Ajanları

Casusluk, temel olarak, bilgi sahibinin izni olmadan gizli ya da hassas verilerin elde edilmesidir. Bir devletin askeri güçleri, istihbarat birimleri, şirketler, suç örgütleri yahut herhangi bir kişi casusluk faaliyeti yürütebilir. Devletlerin özel ve gizli bilgileri edinme amaçlı gerçekleştirdiği eylemler, casuslukla yakından ilişkilidir. Siber casuslukta ise ajanlar, siber uzayın kaynaklarını kullanarak veri ve bilgi toplamaktadır. Toplanan sonuçlar analiz ve rapor edilerek görevlendirme yapan kişi yahut kuruma teslim edilmektedir. Bu durumdan her iki tarafın da ekonomik ve siyasi çıkarı bulunmaktadır.[98]

Siber casuslar, esasen bilgisayar korsanlarının bir türevidir.[99] Sistem savunmalarını aşarak bilgisayar yapılanmalarını yetkisiz bir şekilde araştırmaktadır. Bu çerçevedeki izinsiz sistem girişleri, birçok devletin iç hukukunda suç teşkil etmektedir. Ancak bazı görüşlere göre günümüz şartlarında siber casusluk, ekonomik rekabetin vazgeçilmez bir parçası haline gelmiştir. Ayrıca, potansiyel düşmanların

[96] Sigholm, s. 21.
[97] Andress ve Winterfeld, s. 211.
[98] Sigholm, ss. 21-22.
[99] Güntay, s. 106.

siber faaliyetleri ve yeteneklerinin gizlice izlenmesi, ulusal savunma için de gerekli görülmektedir.[100]

7. Siber Savaşçılar/Milisler

Siber savaşçılar/milisler, kişisel amaçlar dışında, daha büyük bir amaca hizmet etmek için bir araya gelmiş ve siber saldırı yetenekleri olan gönüllü gruplardır. Ortak bir iletişim ağıyla, gerçek kimliklerini gizleyerek hareket eden kişiler, herhangi bir kurum ve kuruluşa bağlı olmadan, maddi bir kazanç elde etmeden çalışmaktadır. Geçici ya da kalıcı bir grup olabilen bu savaşçılar, esnek bir örgütlenmedir. Herhangi bir sözleşmesel yükümlülükleri bulunmaz. Nihayetinde siber savaşçılar, tüm bu özelliklerle diğer organize gruplardan ayrılmaktadır.[101]

Siber savaşçılar, bilgisayar sistemlerini korumak ya da onlara saldırmak için harekete geçebilmektedir. Siber uzay kaynaklarını kullanarak savaşan bu kişiler, tespit hususunda da kendilerini ve izlerini saklamakta ustadır. Bu sebeple sistemlerin korunmasına özen gösterilmelidir.

Uluslararası sahada herhangi bir alanda faaliyet gösteren aktörler ve bu aktörlerin ilişki biçiminin tanımlanması her zaman önem arz etmektedir. Siber uzayın yönetimi, düzenlenmesi ve seyrinde kritik rol oynayan devletlerle birlikte, bağımsız olarak güçlerini kullanan devlet dışı aktörler de bulunmaktadır. Siber uzayda farklı amaçlar edinmiş birçok aktörün varlığı, siber eylemlerin anonim yapısı ve kimliğin basit bir şekilde gizlenebilmesi durumlarıyla bir arada düşünüldüğünde; sorumluluk konusunda da karmaşık sonuçlar ortaya çıkabilmektedir.

Birçok farklı tanım ve açıklamadan da anlaşıldığı üzere siber uzay, siber alandaki en temel kavramdır. Tanımlar arasında benzerlik olsa da henüz bir uzlaşı sağlanmamıştır. Bilginin çeşitli cihazlar aracılığıyla kontrol edilebildiği bu düzlemde, hukuka aykırı eylemleri uygulamaya dökmek daha kolaydır. Bununla beraber siber

[100] Clay Wilson, "Cyber Crime", **Cyberpower and National Security**, (Ed. Franklin D. Kramer, Stuart H. Starr ve Larry Wentz), National Defense University Press, Washington, 2009, s. 423.
[101] Rain Ottis, "Proactive Defense Tactics Against On-Line Cyber Militia", **Proceedings of the 9th European Conference on Information Warfare and Security (ECIW 2010)**, 2010, s. 234.

uzay daha az maliyetli, ani, anonim ve sınır aşan saldırıların ortaya çıkabileceği bir alan olarak; ulusal ve uluslararası güven ilişkilerini sarsabilecek bir yapıya sahiptir.[102]

Bilgi ve iletişim teknolojilerinin güvenli kullanımı, dünya genelinde temel bir ihtiyaç haline gelmiştir. İnternetin önemi, her yaştan insanın ulaşabileceği bir konuma ulaşmasıyla artmış; siber saldırıların anlam kazanmasındaki süreç, hız kazanmıştır. Siber uzayın temeli olan internetin devletlerin egemenlik sınırlarını aşan, kullanımının engellenmesi[103] ihtimali bulunsa da fiziksel olarak sınırlanması mümkün olmayan bir altyapıya sahip olması; uluslararası ilişkilerin bir parçası haline gelmesine sebep olmuştur. İnternet üzerinden yapılabilecek neredeyse her şeyin kilometrelerce ötede sonuçlar doğurması ihtimali, emniyet ve güvenlik endişelerini had safhaya çıkarmaktadır.[104] Bu çerçevede siber uzay, bilgisayarlardan ve dijital bilgilerden daha fazlası olarak görülmekte; siber saldırılara yönelik etkin ve güçlü savunma sistemlerinin inşa edilmesi için, ulusal ve uluslararası çalışmalara hız kazandırılmıştır.

[102] Sevda Korhan, **Siber Uzayda Uluslararası İlişkilerin Değişen Parametreleri**, (Yayınlanmamış Yüksek Lisans Tezi), Selçuk Üniversitesi Sosyal Bilimler Enstitüsü, Konya, 2018, ss. 6-7 (Parametreler).

[103] Dünyada internetin filtrelenmesi, içeriklere erişim engeli getirilmesi konusunda çeşitli uygulamalar bulunmaktadır. Çin, İran, Birleşik Arap Emirlikleri, Kuzey Kore gibi ülkelerde internet kullanımında devlet tarafından yoğun denetim ve kısıtlama mekanizmaları işletilmekte, altyapıya müdahale edilerek internet kullanımı engellenmekte yahut belirli sınırlar dahilinde internet kullanımına izin verilmektedir. İnternet kullanımının engellenmesi hakkında daha ayrıntılı açıklama için bkz. Doğan Kılınç, "Türk Hukukunda ve Mukayeseli Hukukta İnternet Sitelerine Erişimin Engellenmesi ve İfade Hürriyeti", **Gazi Üniversitesi Hukuk Fakültesi Dergisi**, Cilt:14, Sayı:2, 2010, ss. 408-433.

[104] Mehmet Nesip Öğün ve Adem Kaya, "Siber Güvenliğin Milli Güvenlik Açısından Önemi ve Alınabilecek Tedbirler", **Güvenlik Stratejileri Dergisi**, Y. 9, Sayı:18, 2013, ss. 147-148.

İKİNCİ BÖLÜM
ULUSLARARASI HUKUKUN İLGİLİ TEMEL KURALLARI VE SİBER SALDIRILAR

I. DEVLETLERİN EGEMENLİĞİ

A. Egemenliğin Mahiyeti

Uluslararası hukuk, devletlerin varlığını devam ettirmesi üzerine kurulmuş bir düzeni ifade etmektedir. Devletler ise, varoluşunun temeli olan hak ve yükümlülüklerle birlikte egemenlik kavramı üzerine inşa edilmiştir.[105] Egemenlik, ülke ve millet unsurlarıyla birlikte, bir devletin olmazsa olmaz unsurlarından biri olarak kabul edilmektedir.

Egemenliğin tanım ve anlamına ilişkin birçok tartışma söz konusudur. Bağımsızlık, otorite gibi kavramlarla iç içe olan egemenliğin aynı zamanda soyut ve çok yönlü bir kavram olması, bu tartışmaların odak noktasını oluşturmaktadır. Hakkında birçok tartışma olsa da egemenlik, özü itibariyle uluslararası hukukun vazgeçilmez bir parçası ve önemli bir politika aracıdır.

Egemenliğin anlam ve değerini kavramak için, egemenlik kavramının tarihsel gelişim sürecini dikkate almak gerekmektedir. Nitekim egemenlik, bu süreçteki hadiselerle ortaya çıkan siyasi bir kavramdır. İlk Çağ'da, devletin gücüyle rekabet edebilecek farklı bir oluşum bulunmadığı için, egemenlik ve devlet birbirini tamamlayan ifadeler olarak karşımıza çıkmaktadır. Orta Çağ'ın sonlarına doğru, devletlerin varlığını tehdit eden dini ve feodal güçlerle mücadele başlamış, egemenlik kavramına ilişkin tartışmalar da baş göstermiştir.[106]

Jean Bodin, egemenliği sistematik ve ayrıntılı bir şekilde açıklamış ilk düşünürdür.[107] Ünlü Fransız hukukçusu, *'Devletin Altı Kitabı'* adlı eserinde, egemenliği Latincede *'en yüksek, en üst'* anlamına gelen *'superanus'* kelimesinden

---

[105] Malcolm N. Shaw, **International Law**, 8. Baskı, Cambridge University Press, United Kingdom, 2017, s. 361.

[106] M. Aydoğan Özman, "Devletlerin Egemenliği ve Milletlerarası Teşekküller", **Ankara Üniversitesi Hukuk Fakültesi Dergisi**, Cilt:21, Sayı:1, 1964, s. 56.

[107] H. Emrah Beriş, "Egemenlik Kavramının Tarihsel Gelişimi ve Geleceği Üzerine Bir Değerlendirme", **Ankara Üniversitesi SBF Dergisi**, Cilt:63, Sayı:1, 2008, s. 57.

türetmiş ve *'souveraineté'* olarak adlandırmıştır. Bodin'in egemenlik tanımı, bir devletin mutlak ve daimi gücünü ifade etmek için kullanılmıştır. Buna göre egemenlik mutlaktır; güç, işlev yahut süreyle sınırlı değildir. Egemenliğe getirilecek herhangi bir sınırlama, egemenliğin doğasına aykırıdır. Egemenliği elinde bulunduran otoritenin üzerinde Tanrı haricinde bir güç yoktur.[108]

Thomas Hobbes, egemenlik kavramının gelişmesinde rol oynayan kişilerden bir diğeridir. İngiliz düşünür, *'Leviathan'* adlı eserinde egemenlikle ilgili görüşlerini açıklamıştır. Egemenliği devletle özdeşleştiren Hobbes, egemenin mutlak, üstün, sürekli, bölünmez bir niteliğe sahip olduğunu ve kurallar koyup bu kurallarla bağlı olmadığını ifade etmiştir. Hobbes, uyrukların menfaatleri sonucu ortaya çıkan egemenliğe yönelik herhangi bir sınırlama ve müdahalenin söz konusu olamayacağını da ayrıca vurgulamıştır.[109]

Jean-Jacques Rousseau, egemenliği demokratik bir bakış açısıyla ele alan, halkın karar alma ve yöneticisini seçme mekanizmalarını devletin temeli olarak gören bir düşünürdür. Cenevreli düşünür, *'Toplum Sözleşmesi'* adlı eserinde halk ve egemenliğe ilişkin görüşlerini ayrıntılı bir şekilde açıklamıştır. Rousseau'ya göre, devletin varlığı egemenlikle donatılmış olmasına bağlıdır. Devletin var olması için halkın özgür bir şekilde seçtiği mutlak ve egemen bir gücün olması gerekir. Genel irade olarak adlandırılan bu çoğunluğun sağlanması ise egemenliğin kayıtsız, şartsız halkta olması anlamına gelmektedir. Bu bakımdan egemenlik devredilemez, temsil edilemez, mutlaktır ve yanılmaz.[110]

Tüm görüşlerin ortak paydası olarak egemenliğin tezahürüne ilişkin nitelikler, şu başlıklar altında özetlenebilmektedir:[111]

- Egemen, bulunduğu toplum içerisinde mutlak güce sahip olmalıdır.
- Egemen, mutlak bağımsızlık ile hareket edebilmelidir.
- Egemen, hukuken tam yetki ve güce haiz bir uluslararası hukuk kişisi olmalıdır.

---

[108] Jean Bodin, **On Sovereignty: Four chapters from The Six Books of the Commonwealth**, (Ed. ve Çev. Julian H. Franklin), Cambridge University Press, United Kingdom, 1992, ss. 1-4.

[109] Thomas Hobbes, **Leviathan**, (Çev. Semih Lim), 6. Baskı, Yapı Kredi Yayınları, İstanbul, 2007, ss. 131-138.

[110] Jean-Jacques Rousseau, **Toplum Sözleşmesi**, (Çev. Vedat Günyol), 9. Basım, Türkiye İş Bankası Kültür Yayınları, İstanbul, 2012, ss. 23-31.

[111] Timothy Endicott, "The Logic of Freedom and Power", **The Philosophy of International Law**, (Ed. Samantha Besson ve John Tasioulas), Oxford University Press, Oxford, 2010, s. 245.

Düşünürler arasındaki tartışmalarla birlikte, uluslararası hukuk bağlamında değer kazanan egemenlik kavramına ilişkin ilk adımlar ise, 1648 yılında gerçekleşen *'Westphalia Barışı'* sonucunda ortaya çıkmıştır.[112] Orta Avrupa'da Katolikler ve Protestanlar arasında din temelli bir mücadele olarak başlayıp uzun süre devam eden Otuz Yıl Savaşları'nın ardından büyük bir yıkım meydana gelmiştir. Nihayetinde, 1648 yılında imzalanan Osnabrück ve Münster Andlaşmaları ile barış sağlanmış, modern devletin temeli atılmış ve devletlerin egemen eşitliğine dayanan yeni bir uluslararası düzen kurulmuştur. 1789 yılında gerçekleşen Fransız Devrimi, 1900'lü yıllarda gerçekleşen I. ve II. Dünya Savaşları'ndan sonra da egemenliğe ilişkin birçok gelişme kaydedilmiştir. Uluslararası işbirlikleri ve küreselleşme hususlarıyla birlikte egemenliğin önemi artmaya devam etmektedir.[113]

B. Devletlerin Egemen Eşitliği İlkesi

Modern uluslararası hukukun doğumunun ardından muhtelif devletlerin uluslararası toplumu etkileyecek birbirinden farklı istekleri, egemenliğe ilişkin anlayışlarda farklılaşmaya yol açmıştır. Her devlet ülkesi üzerinde egemenliğe sahiptir ve ülkesel egemenliğin ihlali uluslararası hukuka aykırıdır. Uluslararası hukuktaki egemenlik anlayışında, devletlerin iç işlerinde otoriter, dış işlerinde egemenlik ve bağımsızlık hususlarında diğer devletlerle eşit olduğu kabul edilmektedir. İç egemenlik ve dış egemenlik olarak adlandırılan bu ayrımla birlikte, bir devletin başka bir devletin iradesine müdahalede bulunması, yetkisel talepler yahut otoriter baskılarla bir devletin işleyişinin kontrol edilmesi engellenmektedir.[114]

Devletlerin egemen eşitliği söylemi, Westphalia döneminde ortaya atılmış, uluslararası hukukta zamanla kabul görerek temel ilkelerden biri haline gelmiştir. 18. yüzyılın sonunda İsviçreli felsefeci Emmerich de Vattel tarafından; büyük/küçük, güçlü/güçsüz ayrımı gözetilmeksizin tüm devletlerin uluslararası haklar nezdinde eşit

[112] Beriş, s. 58.
[113] Sur, ss. 5-7.
[114] Özman, s. 59, Beriş, s. 64 ve Abdullah Ahmet Buyuran, **Devlet Başarısızlığı, Egemen Eşitlik ve Uluslararası Hukukta Müdahale**, (Yayınlanmamış Doktora Tezi), Millî Savunma Üniversitesi Atatürk Stratejik Araştırmalar ve Lisansüstü Eğitim Enstitüsü, İstanbul, 2023, s. 56.

olduğu ifade edilmiştir. Nihayetinde eşit bir egemenlik anlayışı, uluslararası sistemde birlikte var olabilmeyi mümkün kılmıştır.[115]

Özellikle 1815 senesindeki Viyana Kongresinden itibaren, devletlerin egemen eşitliği prensibi hakkında birçok kodifikasyon çalışması yapılmış, çeşitli düzenlemeler ile uluslararası barış ortamının sağlanması hedeflenmiştir. Başlarda ekonomisi ve siyasi ağırlığı küçük devletlerin kendi kaderini tayin etmesi dahi mümkün değilken, zamanla bağımsızlıklarını ilan edebilen devletler ortaya çıkmıştır. Pratikteki sorunlar, tarihsel süreçte yaşananlardan ders alınarak aşılmıştır. Bu kapsamda 1899 ve 1907 yılları arasındaki Lahey Konferansları bir dönüm noktası olarak tarih sahnesinde yerini almıştır.[116]

18 Mayıs 1899'da gerçekleştirilen Lahey Konferansında, 26 devlet bir araya gelerek büyüklüğü, gücü ve delege sayısı ne olursa olsun tüm devletlerin tek oya hakkına sahip olacağı kabul edilmiş, gündemdeki konular hakkında eşitlik prensibi gözetilerek kararların verilmesi sağlanmıştır. İlk konferanstaki olumlu ortam üzerine, Güney Amerika devletleri dahil olmak üzere 46 devlete davet gönderilerek 1907 yılında ikinci bir Lahey Konferansı düzenlenmiştir. Her devletin eşit oy hakkına sahip olduğu yeniden belirtilerek önemli tüm kararların oybirliği esasıyla alınması kabul edilmiştir. Ancak bu durum hâlihazırdaki dünya düzeni ile uyum sağlamamış, bazı uygulamalar fiiliyata geçememiştir. Uluslararası Sürekli Adalet Divanına (Permanent Court of International Justice – USAD/PCIJ) ilişkin proje bakımından, devletlerin mahkemede yargıç bulundurma ve görev süreleri gibi hususlarda fikir birliğine varamaması sebebiyle süreç ertelenmiştir.[117]

Egemenliğe ilişkin birçok tartışma, I. Dünya Savaşı'yla birlikte gündemdeki önemini artırarak korumuştur. Nihayetinde devletlerin kendini eşit bir şekilde temsil edebileceği bir platform kurulması ihtiyacı kuvvetle kendini hissettirmiş ve Milletler Cemiyeti kurulmuştur. Milletler Cemiyeti Misakında açık olarak egemen eşitlik ilkesi düzenlenmemiş, ancak Milletler Cemiyeti döneminde, daha öncesinde kurulması planlanan USAD kurularak, mahkeme kararları içerisinde egemenliğin, temel bir

[115] Buyuran, s. 58.
[116] Buyuran, ss. 65-68.
[117] R. P. Anand, "Sovereign Equality of States in International Law", **International Studies**, Cilt:8, Sayı:3, 1966, ss. 221-223.

uluslararası hukuk ilkesi olduğu vurgulanmıştır.[118] Bu kapsamda Bozkurt-Lotus[119] ve Wimbledon[120] gibi kararların önemi büyüktür.

27 Ağustos 1928 tarihinde on beş devletin katılımıyla imzalanıp 25 Temmuz 1929 tarihinde yürürlüğe giren Briand-Kellog Paktı[121] ile devletlerin egemen eşitliği ilkesi kaleme alınarak, tekrar bir dünya savaşı yaşanmaması adına savaş yasaklanmış ancak nihai bir yaptırım öngörülmemiştir. Söz konusu Pakt ile sorunlara çözüm bulunabileceği düşünülse de herhangi bir yaptırımın olmaması, bu ihtimali çürütmüştür.[122]

Milletler Cemiyetinin kurulma amacı, uluslararası ilişkilerde etkili olan alanları tüm devletlerin lehine olacak şekilde esas noktalarıyla düzenlemek ve uluslararası barışın kalıcılığını sağlamaktır. Bu sebeple temel ilkelere dayanarak ilerlenmesi, dönemin şartları göz önüne alındığında makul görünse de yeterli olmamış, 18 Nisan 1946 tarihli son oturumuyla Milletler Cemiyeti dağılmıştır. II. Dünya Savaşı'nın ardından Birleşmiş Milletler (BM) kurularak uluslararası hukuku daha ayrıntılı bir biçimde ele alan düzenlemeler yapılmış ve Uluslararası Adalet Divanının

[118] USAD'ın tüm kararlarına ulaşmak için bkz. United Nations, **Summaries of Judgments, Advisory Opinions and Orders of the Permanent Court of International Justice**, 2012, (USAD Kararları), https://legal.un.org/PCIJsummaries/documents/english/PCIJ_FinalText.pdf (03.12.2023).

[119] 2 Ağustos 1926 tarihinde, Mersin'e doğru hareket eden kömür yüklü Bozkurt isimli Türk vapuru ile Lotus isimli Fransız ticaret gemisinin Midilli Adası açıklarında çarpışmaları ve 8 Türk gemicinin kurtarılamaması sonucunda İstanbul'da Bozkurt Kaptanı Hasan Efendi Lotus Nöbetçi Kaptanı Süvari Jan Demons yargılanmıştır. Fransa tarafından tepkiyle karşılanan bu karar sonucunda uyuşmazlık USAD'a taşınmıştır. Egemenlikle ilgili dünya ve Türkiye tarihi açısından önem arz eden bu uyuşmazlıkta, Mahmut Esad Bozkurt'un ses getiren savunmasının katkılarıyla, egemenliğin devletler için son derece önemli bir ilke olduğu vurgulanmış, yargı yetkisinin egemenliğin bir tezahürü olduğu ve devletlerin inisiyatifine bırakıldığı açıklanmıştır. Söz konusu karar hakkında ayrıntılı bilgi için bkz. USAD Kararları, ss. 96-109 ve Durmuş Tezcan, "Bozkurt-Lotus Davasının Uluslararası Hukuktaki Önemi ve Yeri, **Çağdaş Türkiye Tarihi Araştırmaları Dergisi**, Cilt:2, Sayı:4, 1994, ss. 267-274.

[120] 21 Mart 1921 yılında Birleşik Krallık'a ait silah yüklü Wimbledon buharlı gemisinin Kiel Kanalı üzerinden Polonya'ya geçmek istemesi, ancak Almanya'nın tarafsızlık ilkesini öne sürerek buna izin vermemesinin diğer devletler tarafından tepkiyle karşılanmıştır. Almanya'nın Versailles Andlaşması m. 380 hükmüne aykırı davrandığı düşünülmüş ve uyuşmazlık USAD'a taşınmıştır. USAD tarafından söz konusu uyuşmazlık hakkında, uluslararası ilişkilerde andlaşmalar akdetme yetkisinin egemenliğin bir göstergesi olduğu belirtilerek egemenlik ilkesi vurgulanmış, Almanya'nın imzacı olduğu andlaşmaya uymamasının hukuka aykırı olduğu ifade edilmiştir. Söz konusu karar hakkında ayrıntılı bilgi için bkz. USAD Kararları, ss. 13-17.

[121] League of Nations, **General Treaty for Renunciation of War as an Instrument of National Policy**, 1929, https://treaties.un.org/doc/Publication/UNTS/LON/Volume%2094/v94.pdf (12.10.2023).

[122] Aslan Gündüz, **Milletlerarası Hukuk**, (Ed. Reşat Volkan Günel), 11. Baskı, Savaş Yayınevi, Ankara, 2021, ss. 91-92 ve Levent Ersin Orallı, "Uluslararası Hukukta Ve BM Sisteminde Askeri Müdahale Olgusu", **Tesam Akademi Dergisi**, Cilt:1, Sayı:1, 2014, s. 109.

(International Court of Justice - UAD/ICJ) kurulması suretiyle mahkeme kararları ile söz konusu düzenlemeler desteklenmiştir.[123]

Birleşmiş Milletler Andlaşması[124] m. 2/1 ile devletlerin egemen eşitliği tanınmış, iç işlere karışmama ilkesi ve müdahale yasağı kavramlarının temeli somutlaşmıştır. Bu hususta BM Andlaşması'nın ilgili hükmü *"Teşkilât bütün Üyelerinin egemen eşitliği prensipi üzerine kurulmuştur."* cümlesiyle kaleme alınmıştır.

BM Genel Kurulu tarafından kabul edilen 24.10.1970 tarih ve 2625(XXV) sayılı *"Devletlerarasında İşbirliği ve Dostça İlişkiler Bildirisi"*nde[125], devletlerin egemen eşitliği ilkesi ayrıntılı bir şekilde ifade edilmiştir:[126]

> *Tüm devletler egemen eşitlikten yararlanır. Eşit haklara ve görevlere sahiptir ve ekonomik, sosyal, siyasi ya da diğer niteliksel farklılıklarına bakılmaksızın uluslararası toplumun eşit üyeleridir.*
> *Egemen eşitlik, özellikle aşağıdaki unsurları içerir:*
> *(a) Devletler hukuken eşittir;*
> *(b) Her devlet, tam egemenliğin doğasında bulunan haklardan yararlanır;*
> *(c) Her devlet, diğer devletlerin kişiliğine saygı göstermekle yükümlüdür;*
> *(d) Devletin toprak bütünlüğü ve siyasi bağımsızlığı dokunulmazdır;*
> *(e) Her devletin kendi siyasi, sosyal, ekonomik ve kültürel sistemlerini özgürce seçme ve geliştirme hakkı vardır;*
> *(f) Her devlet, uluslararası yükümlülüklerine tam olarak ve iyi niyetle uymak ve diğer devletlerle barış içinde yaşamakla yükümlüdür.*

Egemenlik bahsindeki en temel kararlardan biri olan Korfu Boğazı Kararı'nda[127], devletlerin egemenliğinin önemi *"Bağımsız devletler arasında ülkesel*

---

[123] Murat Can Arasan, **Uluslararası Hukukta Devletlerin Egemen Eşitliği İlkesi**, (Yayınlanmamış Yüksek Lisans Tezi), Ankara Üniversitesi Sosyal Bilimler Enstitüsü, Ankara, 2017, ss. 37-44.

[124] Birleşmiş Milletler Andlaşması, RG 24.08.1945, Sayı:6092, sonraki değişiklikleri içeren güncel metinler için bkz. Gündüz ss. 95-109 ve United Nations, **United Nations Charter**, https://www.un.org/en/about-us/un-charter/full-text (03.12.2023).

[125] United Nations General Assembly, **Declaration on Principles of International Law concerning Friendly Relations and Cooperation among States in accordance with the Charter of the United Nations**, 2625(XXV), 1970, https://digitallibrary.un.org/record/202170/files/A_RES_2625%28XXV%29-EN.pdf (31.12.2021).

[126] **United Nations General Assembly**, Declaration on Principles of International Law concerning Friendly Relations and Cooperation among States in accordance with the Charter of the United Nations, s. 124.

[127] 1946 yılında, İngiliz kraliyet donanmasına ait savaş gemileri Korfu Boğazı'ndan geçerken bir dizi olay yaşanmış, İngiltere ve Arnavutluk arasında uyuşmazlık meydana gelmiştir. İlk olarak, İngiliz savaş gemilerinin boğazdan geçişi sırasında Arnavutluk tarafından gemilere ateş açılmıştır. Bir sonraki geçişte gemiler mayına çarpmış ve can kaybı meydana gelmiştir. Nihayetinde İngiltere, Arnavutluk karasularında mayın temizleme faaliyetine girişmiştir. Kriz çözülemeyecek boyuta ulaşınca durum Uluslararası Adalet Divanı'na taşınmıştır. Uluslararası Adalet Divanı, **Korfu Boğazı Davası**, 1949, (Korfu Boğazı Kararı). İngilizce karar metnine ulaşmak için bkz. https://www.icj-cij.org/public/files/case-related/1/001-19490409-JUD-01-00-EN.pdf (05.01.2022).

egemenliğe saygı, uluslararası ilişkilerin esas temelidir." cümlesiyle vurgulanmıştır:[128]

Devletler arasında fiili bir eşitlik olması, farklı gelişim ve değişimlerin gerçekleşmesi sebebiyle, mevcut dünya düzeninde mümkün değildir. Devletlerin egemen eşitliği ilkesi, hukuki eşitliği sağlamak yönünde işlev görmektedir. Böylece fiiliyattaki gücüne bakılmaksızın her devlet, uluslararası hukukta söz sahibi olabilmekte; hak ve sorumlulukları doğabilmektedir.[129] Tüm bu sebeplerle egemenlik ve egemenlikten doğan yetkilerin korunması, uluslararası hukuk için büyük önem arz etmektedir.

C. Siber Uzayda Egemenlik

Siber uzay, uluslararası hukukta belirli kurallarla düzenlenmiş mekânlardan (kara, hava, deniz ve uzay) farklı olarak; egemenlik kapsamında farklı etkileri olan, tartışmalı ve güncelliğini koruyan bir alandır. Siber saldırı ve savunma hususlarındaki sürekli değişim, devletlerin kurallar üzerinde uzlaşmasını zorlaştırmakta; teknolojik gelişmelerin hızı, kodifikasyon sürecini geciktirmektedir.[130] Bu sebeple, siber uzayın egemenlik çatısı altında nasıl değerlendirileceği hususu, güncelliğini ve önemini korumaktadır.

Siber uzayın ülkesel sınırları aşan yapısı ve kendine has özellikleri, devletlerin egemen eşitliği ilkesiyle çatışabilmektedir. Devlet dışı siber aktörlerin internet altyapısı ve uygulamalarındaki baskın konumu, bu alanda devletlerin egemenliğini sarsabilecek nitelikleriyle uluslararası hukuk düzeninde belirsizliğe neden olmaktadır.[131] BM Genel Kurulu nezdinde konuyla ilgili çalışmalar yürüten Uluslararası Uzmanlar Grubunun 2013 yılında hazırlamış ve 2015 yılında güncellemiş olduğu *"Uluslararası Güvenlik Bağlamında Bilgi ve Telekomünikasyon Alanındaki Gelişmelere İlişkin Rapor"* çerçevesindeki açıklamalara göre, siber uzayda temel

[128] Korfu Boğazı Kararı, s. 35.
[129] Sur, s. 126.
[130] Şinasi Özgür Mumcu, "Barış Zamanı Siber Operasyonların Egemenlik İlkesi Bakımından Hukuki Rejimi", **Bahçeşehir Üniversitesi Hukuk Fakültesi Dergisi**, Cilt:16, Sayı:201-202, 2021, ss. 996-997.
[131] Mumcu, s. 999.

uluslararası hukuk kurallarının uygulanacağı açıktır. Egemenlik ve egemenlikle ilişkili düzenlemelerin de vurgulandığı Raporda yer alan açıklamalar şu şekildedir:[132]

> *Uluslararası hukuk ve özellikle Birleşmiş Milletler Andlaşması, açık, güvenli, barışçıl, erişilebilir bir bilgi ve iletişim teknolojileri ortamının teşvik edilmesi, barış ve istikrarın korunması için geçerli ve esastır.*
> *Devlet egemenliği ve egemenlikten kaynaklanan uluslararası norm ve ilkeler, devletin Bilgi ve İletişim Teknolojileri ile ilgili faaliyetleri yürütmesi ve kendi topraklarındaki altyapı üzerindeki yargı yetkisi için geçerlidir.*
> *Devletler, bilgi ve iletişim teknolojilerinin kullanımında uluslararası hukukun diğer ilkelerinin yanı sıra, devlet egemenliği, egemen eşitlik, anlaşmazlıkların barışçıl yollarla çözülmesi ve diğer devletlerin iç işlerine müdahale etmeme gibi hususlara dikkat etmelidir. Uluslararası hukuk kapsamındaki mevcut yükümlülükler, bir devletin bilgi ve iletişim teknolojilerini kullanımında da geçerlidir. Devletler insan haklarına ve temel özgürlüklere saygı göstermek ve korumak için uluslararası hukuk kapsamındaki yükümlülüklerine uymalıdır.*

Bağlayıcılığı olmayan fakat devletlerarası bir uzlaşıyı ifade eden söz konusu Rapor'a göre, teknolojik gelişmelerin uluslararası hukuk düzenini tehdit etmesinin engellenmesi, yine uluslararası hukuk düzeniyle mümkün görülmüştür.

Tallinn Kılavuzu'nun 1 ila 5 Numaralı Kurallarında, egemenlik hususu daha ayrıntılı bir şekilde ele alınmaktadır. Kılavuzun amaçları doğrultusunda, siber uzayın katmanlarının egemenlik ilkesi kapsamında değerlendirildiği açıklanmaktadır. Buna göre, siber faaliyetler, devletlerin ülkesel sınırlarında, egemenliğe ilişkin yetkilerini kullanabileceği yerlerde, çeşitli nesneler aracılığıyla, farklı kişi ve kuruluşlar tarafından yürütülebilmektedir. Siber faaliyetlerin birden fazla sınırı geçerek, uluslararası sularda, uluslararası hava sahasında yahut uzayda gerçekleşmesi halinde dahi, bir ya da birden çok devletin yargı yetkisini kullanması mümkündür. Siber uzaya erişim sağlayan altyapının bir devletin kara, hava veya deniz ülkesinde bulunması, söz konusu devletin egemenliğinden feragat ettiği şeklinde yorumlanamaz. Bu çerçevede devletler, uluslararası hukuka uygun olarak siber altyapı ve internet üzerinde kısıtlama yapma hakkına da sahiptir.[133]

---

[132] United Nations General Assembly, **Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security**, A/68/98, 2013, s. 8, https://digitallibrary.un.org/record/753055/files/A_68_98-EN.pdf (31.12.2021) ve United Nations General Assembly, **Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security**, A/70/174, 2015, s. 12, https://digitallibrary.un.org/record/799853/files/A_70_174-EN.pdf (11.01.2022).

[133] Tallinn Kılavuzu, ss. 12-13 ve Harriet Moynihan, "The Application of International Law to State Cyberattacks: Sovereignty and Non-intervention", **Chatham House**, 2019, ss. 14-15.

Tallinn Kılavuzu'na göre devletler, kendisini bağlayan uluslararası hukuk kurallarına riayet etmek kaydıyla uluslararası ilişkilerinde siber faaliyetler yürütebilmektedir. BM Andlaşması m. 2/1'de de kabul edildiği üzere, devletler hukuken egemen ve eşittir. Bir devletin dış egemenliği bağlamında, diğer devletlerle eşit bir şekilde siber faaliyetler yürütmesi, uluslararası hukuka aykırılık oluşturmaz. Ancak bu hususta, diğer devletlerin egemenliğinin ihlali sonucunu doğuracak müdahale ve kuvvet kullanmaya ilişkin yasaklara özellikle dikkat edilmesi gerekmektedir. Bir devlet, başka bir devletin egemenliğini ihlal etmemeli, bu kapsamdaki siber faaliyetlerden sakınmalıdır.[134] Nihayetinde; bir devletin siber ortamdaki istihbarat amaçlı casusluk eylemlerinin, herhangi bir zarara mahal vermediği ve diğer devletlerin egemenliğini ihlal etmediği sürece, tek başına uluslararası toplumdaki huzur ve güvenliği tehdit etmeyeceği söylenebilecektir.

Temel olarak siber uzayda egemenlik, iç işlere karışma, müdahale ve kuvvet kullanmaya dair kuralların uygulanamayacağı boyutta bir siber eylem gerçekleştiğinde devreye giren bir çatı kavramdır. Bu çerçevede, devletlerin egemenliğini ihlal eden daha hafif nitelikteki siber eylemlerin de uluslararası hukukta haksız fiil olarak kabul edilmesi mümkündür.[135]

II. İÇ İŞLERE KARIŞMAMA İLKESİ VE MÜDAHALE YASAĞI

A. İç İşlere Karışmama İlkesi ve Müdahale Yasağının Mahiyeti

Uluslararası hukukta egemenlik hususunda yaşanan gelişmelerin paralelinde, devletlerin kendi kaderini tayin hakkı, iç işlere karışma ve müdahale yasağı gibi konularda da çeşitli gelişmeler yaşanmıştır. 1907 yılında gerçekleşen Lahey Konferansı'nda ve Briand-Kellog Paktında savaş ve karışma fiillerinin düşmanca olduğu vurgulanmış, ancak tam anlamıyla engelleyici bir düzenleme de yapılamamıştır. Esasen bu hususstaki efektif gelişmeler, BM'nin kuruluşu ile gerçekleşmiştir.[136]

---

[134] Tallinn Kılavuzu, ss. 16-17 ve Michael N. Schmitt ve Liis Vihul, "Respect for Sovereignty in Cyberspace", **Texas Law Review**, Cilt:95, Sayı:7, 2017, s. 1649.
[135] Mumcu, s. 1001.
[136] Buyuran, ss. 97-98.

Devletlerin egemen eşitliği ilkesinin uluslararası hukuktaki en somut yansıması, iç işlere karışmama ilkesidir. BM Andlaşması m. 2/7 uyarınca ve BM Örgütü nezdinde devletlerin iç işlerine karışmama ilkesi benimsenmiştir. Buna göre BM Örgütü, kural olarak bir devletin iç işlerine karışamaz ve üye devletlere de başka bir devletin iç işlerine ilişkin sorumluluk yüklenemez. İç işlere karışmama ilkesinin spesifik bir yönü ise müdahale yasağıdır. Nitekim devletlerin iç işlerine karışıldığında, ilgili devletin egemenliğinin ve egemenlikle ilişkili haklarının zarar görmesi de doğal bir sonuçtur. Bu hususta BM Andlaşması'nın ilgili hükmü şu şekilde kaleme alınmıştır:

> *İşbu Andlaşmanın hiçbir hükmü, ne özü itibariyle bir devletin millî yetkisi içinde bulunan işlere, Birleşmiş Milletlerin karışmasına cevaz verir, ve ne de Üyeleri, bu gibi işleri, işbu Andlaşma gereğince bir çözme tarzına bağlamaya icbar eder; bununla beraber, VII nci bölümde derpiş edilen zorlama tedbirlerinin uygulanmasına bu prensip hiçbir suretle halel getirmez.*

Devletlerarasında İşbirliği ve Dostça İlişkiler Bildirisi'nde, iç işlerine karışmama ilkesi ve müdahale yasağının örf ve âdet niteliği kabul edilmiş ve tüm devletler için bağlayıcı olduğu vurgulanmıştır. Ayrıca söz konusu ilke ve yasağın anlamı şu şekilde özetlenmiştir:[137]

> *Hiçbir devlet yahut devlet grubu, herhangi bir nedenle, doğrudan ya da dolaylı olarak, iç veya dış işlere müdahale etme hakkına sahip değildir. Bu sebeple, devletin kişiliğine veya siyasi, ekonomik ve kültürel unsurlarına yönelik silahlı ve diğer her türlü müdahale yahut tehdit teşebbüsü uluslararası hukuka aykırıdır.*

Devletlerin iç işleri olarak kabul edilen eylemlerin meydana gelebileceği alanlar, ulusal yetki alanı (mahfuz saha, domaine rêservê) olarak adlandırılmaktadır. Ulusal yetki alanı kara, hava ve deniz alanlarıyla birlikte devletlerin uluslararası hak ve yükümlülüklerinin kullanabileceği, sınırları olan bir üst kavramı ifade etmektedir. Ulusal yetki alanında meydana gelen eylemlere karşı, uluslararası toplumun bir müdahale hakkı ve görevi bulunmamaktadır.

İç işlere karışmama ilkesi ve müdahale yasağının pratikte karşımıza çıkan önemli örneklerinden biri, 1986 yılında Uluslararası Adalet Divanı tarafından verilen Nikaragua Kararı'dır.[138] Söz konusu kararda, iç işlere karışmama ilkesi ve müdahale

---

[137] **United Nations General Assembly**, Declaration on Principles of International Law concerning Friendly Relations and Cooperation among States in accordance with the Charter of the United Nations, s. 123.

[138] 1979 yılında Nikaragua'da yaşanan iç çatışmalar, sağ tabanlı Somoza diktatör rejiminin yıkılması ve yerine Sandinista devrimcilerinin yeni bir hükümet kurması gelişmelerini beraberinde getirmiştir.

yasağının örf ve âdet hukukunun bir parçası olduğu vurgulanmış, ilgili ilke ve yasağa ilişkin içerikle birlikte iki temel unsur belirtilmiştir. Bu çerçevede, bir devletin egemenliğinden kaynaklanan ve serbestçe karar alma özgürlüğünün olduğu meselelerde, bir başka devletin zorlayıcı yöntemler kullanması, ilgili ilke ve yasağı ihlal etmektedir. Devletlerin özgürce karar alabileceği meseleler ise, siyasi, ekonomik, sosyal, kültürel sistem seçimleri ve dış politikanın formüle edilmesi şeklinde ifade edilmiştir.[139] Devletler, kural olarak başka bir devletin ülkesinde herhangi bir eylemde bulunamaz. Ancak müdahale yasağı ve devletlerin iç işlerine karışmama ilkelerinin sınırı değişebilmekte, devletlerin rızası bu kapsamdaki eylemleri hukuka uygun hale getirebilmektedir. İnsan hakları, insani müdahale ve halkı koruma sorumluluğu gibi kavramlar çerçevesinde, nitelikleri gereği uluslararası alana geçtiği öne sürülen eylemlere ilişkin tartışmalar ise devam etmektedir.[140]

İç işlere karışmama ilkesi ve müdahale yasağı kavramlarına yer veren diğer önemli BM Genel Kurul Kararları, 21.12.1965 tarih ve 2131(XX) sayılı *"Devletlerin İç İşlerine Karışılmasının Reddi ve Bağımsızlıklarının ve Egemenliklerinin Korunması Kararı"*[141], 9.12.1981 tarih ve 36/103 sayılı *"Devletlerin İç İşlerine Müdahale ve Her Türlü Karışmanın Kabul Edilmezliği Bildirisi"*[142]dir. Ancak yine de iç işlere karışmama ilkesi ve müdahale yasağı hakkında, uluslararası hukuktaki gelişim ve değişimlere paralel olarak tartışmalar gündeme gelebilmektedir. Siber uzay da bu hususta önemli örneklerden biridir.

Yeni kurulan Sandinista Hükümeti, ülkeyi savaş sonrası felaketten kurtarmak ve sosyal adaleti sağlamak amacıyla çeşitli reformlar gerçekleştirmiştir. Bunun yanında dönemin sosyalist ülkeleri Sovyetler Birliği ve Küba ile yakın ilişki adımları atılmıştır. Sosyalist ülkelerle mücadele içinde olan ABD bu yakınlaşmayı çıkarlarına uygun görmemiştir. ABD, bazı ambargo ve askeri müdahale tehditleri sonrasında Sandinista Hükümetine muhalif gruplara askeri ve lojistik yardımda bulunmuş, taktik ve istihbarat eğitimi de vermiştir. Savaş sonrası yeni toparlanan Nikaragua, 'kontra' adı verdiği bu gruplara karşı başarılı olamamış; ABD'nin de fiillerini inkâr etmemesinin ardından olaylar Uluslararası Adalet Divanına taşınmıştır. Uluslararası Adalet Divanı, **Nikaragua'ya Karşı Askeri ve Bölgesel Faaliyetler Davası**, 1986, (Nikaragua Kararı). İngilizce karar metnine ulaşmak için bkz. https://www.icj-cij.org/public/files/case-related/70/070-19860627-JUD-01-00-EN.pdf (31.12.2021).

[139] Nikaragua Kararı, ss. 106-108, prg. 202-205.

[140] Ayrıntılı bilgi için bkz. Sur, ss. 127-135.

[141] United Nations General Assembly, **Declaration on the Inadmissibility of Intervention in the Domestic Affairs of States and the Protection of Their Independence and Sovereignty**, 2131(XX), 1965, https://digitallibrary.un.org/record/203886/files/A_RES_2131%28XX%29-EN.pdf (31.12.2021).

[142] United Nations General Assembly, **Declaration on the Inadmissibility of Intervention and Interference in the Internal Affairs of States**, 36/103, 1981, https://digitallibrary.un.org/record/27066/files/A_RES_36_103-EN.pdf (31.12.2021).

B. Siber Uzayda İç İşlere Karışmama İlkesi ve Müdahale Yasağı

Devletlerin egemenlik alanına uzaktan müdahale edilmesi olasılığını artıran siber eylemler, iç işlere karışmama ilkesini ihlal edebilecek şekillerde karşımıza çıkabilmektedir. Bu durum, hayatın olağan akışı çerçevesinde, devletlerin, bir başka devletin müdahalesine izin verebileceği meselelerden biri olarak görülmemektedir. Böylece, ulusal yetki alanı kavramını tartışmaya açık hale getiren siber uzayla birlikte, yeni bir bakış açısı geliştirilmesi zorunluluğu ortaya çıkmaktadır.

Tallinn Kılavuzu'nda, 66 ve 67 Numaralı Kurallar ile iç işlere karışmama ilkesi ve müdahale yasağına ilişkin ayrıntılı açıklamalar yapılmıştır. Siber uzay, küreselleşme ve bilgi teknolojisine ilişkin artan bağımlılık sebebiyle iç veya dış işlere müdahalenin kolaylaştığı bir alandır. Ancak uluslararası hukukta devletlerin egemen eşitliği ilkesine dayanan iç işlere karışma ve müdahale yasağı, siber uzayı da kapsayan geleneksel bir uluslararası normdur. Ayrıca, devletlerle birlikte BM, UAD ve birçok uluslararası kuruluş, söz konusu normun örf ve âdet statüsünü de tanımaktadır. Bu bağlamda devletler, siber yollar da dahil olmak üzere, iç veya dış işlere müdahale edemez.[143]

Tallinn Kılavuzu çerçevesinde bir devletin, başka bir devlete siber uzay bağlamında müdahale edebileceği olaylardan biri olarak; elektronik oy pusulalarının siber saldırılarla değiştirilmesi ve seçimin manipüle edilmesi örneği verilmiştir. Bunun yanında, devletlerin internetle ilgili iç mevzuatlarını değiştirmek, siber uzayda silahsızlanmaya yöneltmek ve uluslararası andlaşmalara taraf olmaya ilişkin kararlara karışmak gibi yöntemlere başvurmak da yasaklanmıştır.[144]

Kılavuz'da belirtilmiş olan yasaklar, yalnızca devletler arası ilişkilerde geçerlidir. Bir devlete yönelik düşmanca siber eylemlerde bulunan diğer siber aktörler için bu durum söz konusu değildir. Ancak, devlet dışı siber aktörlerin eylemleri herhangi bir devlete atfedilebilirse, müdahale yasağı ihlal edilmiş olur ve ilgili devletin uluslararası sorumluluğu doğar. Yine de siber uzay bakımından sürekli gelişen ve giderek iç içe geçen uluslararası ilişkilerde, iç işlere karışma ve müdahale yasağının nasıl uygulanacağına dair kesin sınırlar çizmek güçtür. Bu kapsamda, bir devletin

[143] Tallinn Kılavuzu, ss. 312-313.
[144] Tallinn Kılavuzu, s. 313.

özgürce karar verebileceği meseleler ve diğer devletin buna zorlayıcı yöntemlerle müdahale etmesi unsurları çerçevesinde bir değerlendirme yapılmalıdır.[145]

Tallinn Kılavuzu'na göre devletlerin iç işleri, esasen uluslararası hukuk tarafından düzenlenmeyen konulardan oluşan ulusal yetki alanı kavramı çerçevesinde türetilmiştir. Kısaca açıklamak gerekirse, uluslararası hukukun düzenlemediği konular, devletlerin ulusal yetki alanı kapsamında değerlendirilmekte ve diğer devletlerin müdahalesinden korunmaktadır. Bir devletin ulusal yetki alanına girebilecek hususlar ise zaman içinde değişebilmektedir. Hangi hususun ulusal yetki alanı kümesinde kabul edileceği devletlerin uygulamaları ve hukuki görüşleri ile şekillenmektedir. Nikaragua Kararı'nda da belirtildiği üzere, devletlerin egemenliğine dayanan meselelerdeki yetkileri sınırlamak yahut ortadan kaldırmak amacı güden zorlayıcı yöntemler müdahale yasağını ihlal etmektedir. Bu nitelikteki siber eylemler de aynı şekilde iç işlere karışmama ilkesi ve müdahale yasağını ihlal edecektir. Nitekim söz konusu ihlal, devletlerin tekeline ayrılmış olan diğer hususlarla büyük ölçüde aynı düzeydedir.[146]

Tallinn Kılavuzu, siber uzayda ulusal yetki alanı, iç işlere karışma, müdahale ve zorlayıcı yöntemler hakkındaki eşiğin daha iyi anlaşılması için çeşitli örneklerle konuyu detaylandırmıştır. Söz gelimi, A devletinde çoğunluk ve azınlık etnik gruplarının kullandığı iki resmi dilden, referandumla çoğunluğun kullandığı tek bir resmi dile geçiş yapılması planlanmıştır. Azınlık etnik grubuyla aynı kökene sahip B devleti, A devletini caydırmak için önemli hükümet web sitelerine hizmet engelleme saldırıları gerçekleştirip, web sitelerinin her iki dilde de sürdürülmesi için eyleme geçmiştir. Bu örnekte, A devletinin dil politikasına siber uzay aracılığıyla müdahale edilmesi, devletlerin özgürce karar verebileceği meseleler ve zorlayıcı yöntemler unsurlarını taşımakta ve müdahale yasağına aykırılık teşkil etmektedir.[147]

Farklı bir örnekte, X devletinin ticari bankalarına yönelik yıkıcı siber faaliyetler yürüten Y devleti ele alınmıştır. Y devleti, X devletinin üzerinde yaratacağı baskıyla, X devletinin altyapısına bağlı özel web sitelerindeki saldırgan olarak düşündüğü çevrimiçi içeriklerin kaldırılmasını talep etmiştir. Devletlerin çevrimiçi içeriklere ilişkin düzenlemeleri, uluslararası yükümlülüklerine aykırı olmadığı sürece,

[145] Tallinn Kılavuzu, s. 314 ve Jensen s. 775.
[146] Tallinn Kılavuzu, ss. 314-315 ve Moynihan ss. 26-35.
[147] Tallinn Kılavuzu, s. 315.

ulusal yetki alanı kapsamındadır ve bu tür siber faaliyetler de müdahale yasağına aykırı kabul edilmektedir.[148]

Devletler, uluslararası hukuk sisteminde, ikili yahut çok taraflı uluslararası andlaşmalar aracılığıyla bir meseleyi ulusal yetki alanı olarak görmekten vazgeçebilmektedir. Bu durum, siber faaliyetlerle ilgili herhangi bir uluslararası andlaşma için de geçerli olacaktır. Ancak söz konusu uluslararası andlaşmaya taraf olmayan devletler için bu uygulamanın geçerli olmayacağı ve diğer devletlere karşı ulusal yetki alanını korumaya devam edeceği unutulmamalıdır.[149] Nihayetinde, devletlerin özgürce karar vereceği meseleler ve zorlayıcı yöntemler görecelidir. Siber tehditlerin ulusal yetki alanı içerisinde etki göstermesi, devletlerin iç işleyişinde buna müdahalede bulunması için yeterlidir.[150] Bu hususlardaki her uyuşmazlığın somut olay ve şartlara göre değerlendirilmesi gerekmektedir.

Tallinn Kılavuzu'nun iç işlere karışmama ilkesi ve müdahale yasağına ilişkin düzenlemiş olduğu son husus BM Örgütünün siber faaliyetlerdeki konumudur. Buna göre, BM Örgütünün siber yollar da dahil olmak üzere devletlerin iç yetki alanlarına giren konulara müdahale etmemesi esas olarak kabul edilmiş; BM Andlaşması m. 2/7'de olduğu gibi, BM Andlaşması'nın VII. Bölümü çerçevesinde alınabilecek önlemler saklı tutulmuştur. Ancak, BM Andlaşması m. 1'de[151] belirtilen BM Örgütünün amaçları kapsamındaki ve özellikle uluslararası barış ve güvenliği ilgilendiren konular bu kuralın dışındadır.[152] Özetle, BM Örgütünün amaçları dahilinde, uluslararası barış ve güvenliği tehdit edebilecek nitelikteki siber eylemlere Örgüt tarafından müdahale edilmesi mümkündür.

---

[148] Tallinn Kılavuzu, ss. 315-316.
[149] Tallinn Kılavuzu, s. 316.
[150] Bolat, ss. 23-24.
[151] BM Andlaşması m. 1: *"Birleşmiş Milletlerin amaçları şunlardır: 1. Milletlerarası barış ve güvenliği muhafaza etmek, ve bu maksatla: Barışın uğrayacağı tehditleri önlemek ve uzaklaştırmak ve her türlü saldırma fiilini veya barışın başka suretle bozulması halini ortadan kaldırmak üzere, müessir müşterek tedbirleri almak; barışın bozulmasını intaç edebilecek milletlerarası mahiyette uyuşmazlıkların veya durumların düzeltilmesini veya çözülmesini, adalet ve devletlerarası hukuku prensiplerine uygun olarak barış yollariyle gerçekleştirmek; 2. Milletlerarasında, milletlerin hak eşitliği prensipine ve kendi mukadderatlarını kendilerinin tâyin hakkına saygı üzerine kurulmuş dostane münasebetler geliştirmek ve dünya barışının sağlamlaştırılması için elverişli her türlü diğer tedbirleri almak; 3. Ekonomik, sosyal, fikrî ve insani mahiyetteki milletlerarası dâvaları çözerek ve, ırk, cins, dil veya dm farkı gözetmeksizin herkesin insan haklarına ve ana hürriyetlerine karşı saygıyı geliştirerek ve teşvik ederek, milletlerarası işbirliğini gerçekleştirmek, 4. Milletlerin bu müşterek amaçlara doğru sarfettıkleri gayretlerin ahenkleştiği bir merkez olmak."*
[152] Tallinn Kılavuzu, s. 325 ve Jensen, s. 776.

Kılavuz'a göre, siber altyapı ve eylemlerin birbiriyle bağlantılı karakteri göz önüne alındığında, bir devlette yürütülen siber faaliyetlerin diğer devletleri etkileyeceği çok açıktır. Bu gerçek, uluslararası barış ve güvenlik boyutuyla düşünüldüğünde, bu tür faaliyetler BM Örgütünün gözetim ve denetimine duyarlı hale gelmektedir. Nitekim siber faaliyetler, uluslararası alandaki ekonomik, sosyal, kültürel ve insani konuları etkileyebilecek temel bir yapıya sahiptir. BM Örgütü nezdinde, yerel durumlara müdahale edilerek, daha büyük uyuşmazlıkların önüne geçilmesi mümkündür.[153]

BM Örgütü'nün, devletlerin egemen yetkilerinin bulunduğu meseleler hakkında, zorlayıcı yöntemler kullanılsın yahut kullanılmasın, herhangi bir şekilde karışma hakkı bulunmamaktadır. Örneğin; BM Örgütü'nün, devletlerin kendi topraklarında ve tamamen yerel amaçlarla gerçekleştirdiği siber faaliyetler hakkında belirli bir mevzuatın kabul edilmesine ilişkin talebi, iç işlere karışmama ilkesi ve müdahale yasağını ihlal etmektedir. Ancak uluslararası barış ve güvenliği korumak adına, BM Andlaşması'nın VII. Bölümü çerçevesinde, BM Güvenlik Konseyinin alacağı bir kararla devletlerin ulusal yetki alanına müdahale edilebileceği de unutulmamalıdır.[154]

Siber saldırıların doğası, geleneksel kurallar ile harmanlanmış yeni yorumların ortaya çıkmasına sebep olmaktadır. Nihayetinde, devletlerin bu alanda güttüğü politikalar ve izlediği yöntemlerin uluslararası hukuka uygun olma amacını taşıması gerektiği de rahatlıkla söylenebilecektir. Aksi halde siber uzayın karmaşık yapısı üzerinde bir uzlaşı sağlanması zor alacak ve farklı uygulamalar sorunlara yol açabilecektir.

III. KUVVET KULLANMA YASAĞI VE MEŞRU MÜDAFAA

A. Kuvvet Kullanma Yasağı ve Meşru Müdafaanın Mahiyeti

Uluslararası hukukta, kuvvet kullanma hakkı (jus ad bellum) ile kuvvete başvurulduğunda uyulması gereken çatışma kuralları (jus in bello) hakkındaki temel

[153] Tallinn Kılavuzu, s. 326 ve Jensen, s. 776.
[154] Tallinn Kılavuzu, ss. 326-327.

prensipler, farklı hukuki kuralların uygulama alanı bulduğu bir ayrıma sahiptir. Esasen, kuvvet kullanma hakkına sahip olunması, çatışma hukuku kurallarının uygulanmasına etki etmemekle birlikte, konumuz bağlamında bu ayrıma kısaca değinerek başlamak ve çalışmamızın içeriğinin jus ad bellum özelinde ilerleyeceğini belirtmek gerekecektir.

Jus ad bellum, devletlerin savaşa başlamak için meşru nedenlerinin olması gerektiğini belirtmektedir. Meşru nedenler genellikle savunma, ulusal güvenlik, uluslararası barışın korunması gibi etik, hukuki ve ispat edilebilir temellere dayanmaktadır. Eylemlerin makul ve hukuka uygun şekilde gerçekleştirildiğinin tespiti için somut olaylar özelinde değerlendirme yapılması gerekmektedir. Jus in bello, savaş başladıktan sonra uyulması gereken prensipleri ifade etmektedir. Temel olarak savaş sırasında meydana gelecek askeri eylemlerin orantılı, insancıl, sivilleri koruyacak mahiyette gerçekleştirilmesi beklenmektedir.[155]

İnsan varlığının bulunduğu her yerde, kuvvet kullanma devletler için bir sorun olmuştur. BM Örgütünün kurulması ve BM Andlaşması'nın uygulanmasına dek, kuvvet kullanma eylemi belirli şartlara bağlı kalınmak suretiyle devletlerin hakkı olarak görülmüştür. Kuvvet kullanma eyleminin meşru bir zeminde gerçekleşmesi adına, *'Haklı Savaş'* en önemli şartlardan biri olarak kabul edilmiştir.[156]

Haklı savaş, ilk olarak Hristiyanların savaşması ve insan öldürmesinin günah sayıldığı dönemlerde karşımıza çıkmaktadır. Dönemin ünlü düşünürlerinden Aurelius Augustinus, söz konusu kavramı sistematik bir şekilde ifade etmiş ve uygulanabilir hale getirmiştir. Hristiyanlığın Roma İmparatorluğu tarafından benimsenmesi ve imparatorluk dini olarak kabul edilmesinin ardından savaşın; haklı bir nedene dayanması, iyi niyetli olması ve meşru bir otorite tarafından ilan edilmesi kıstasları gözetilerek, yalnızca barışı tesis etmek amacıyla devletlerin kuvvet kullanabileceği bir düzen oluşturulmuştur.[157]

Doğal hukuk döneminden modern döneme geçişte dönüşerek etkinliğini sürdüren haklı savaş kavramı, 20. yüzyıla dek kullanılmış, kuvvet kullanımı ve meşru

---

[155] International Committee of the Red Cross, **International Humanitarian Law: Answers to your Questions**, ICRC Press, Switzerland, 2023, ss. 8-10.

[156] Cenap Çakmak, **Uluslararası Hukuk: Giriş, Teori ve Uygulama**, Ekin Yayınevi, Bursa, 2014, s. 177.

[157] Elif Uzun, "Haklı Savaş Düşüncesinin Batılı Kökleri: İlk Çağlardan Yirminci Yüzyıla Jus Ad Bellum Kavramı", **Uluslararası Hukuk ve Politika Dergisi**, Cilt:6, Sayı:21, 2010, ss. 21-22.

müdafaa egemenliğin verdiği doğal bir hak olarak görülmüş, bu sebeple devletler arasında her yüzyılda muhtelif savaşlar yaşanmıştır. Milletler Cemiyeti'nin savaşa dair yetkiyi sınırlayan yumuşak hükümlerinin yetersiz kalması sebebiyle I. Dünya Savaşı başlamış ve tüm devletler için yıkıcı sonuçlarla karşılaşılmıştır. Bunun üzerine devletlerin kuvvet kullanmaya başvurmasının bir hak olarak görülemeyeceği anlaşılmış ve uluslararası hukukta kuvvet kullanmanın yasaklanmasına ilişkin Briand-Kellog Paktı ile kodifikasyon çalışmaları başlamış, devletler savaşı kınamış ve uyuşmazlıkların barışçıl yollarla çözülmesi ve savaşa başvurmama yükümlülüğü kabul edilmiştir.[158] Paktın ilk iki maddesi şu şekilde kaleme alınmıştır:[159]

> *1- Yüksek Âkit Taraflar milletlerarası uyuşmazlıkların çözümü için savaşa başvurmayı red ve takbih ettiklerini ve birbirleriyle ilişkilerinde savaşı milli siyasetin bir aracı olarak görmekten vazgeçtiklerini milletleri adına resmi surette beyan ederler.*
> *2- Yüksek Âkit Taraflar, mahiyeti ve kaynağı ne olursa olsun, aralarında ortaya çıkabilecek bütün uyuşmazlıkların veya ayrılıkların hiçbir surette barışçı araçlar dışında çözümlenmeye veya giderilmeye çalışılmayacağı konusunda mutabıktırlar.*

Kuvvet kullanmaya dair kesin ve net düzenlemeler BM döneminin başlamasıyla gerçekleştirilebilmiştir. Devletlerin egemen eşitliği ilkesi temelinde, BM Andlaşması m. 2/4 hükmü uyarınca kuvvet kullanma yahut kuvvet kullanma tehdidinde bulunma yasaklanmış ve yasak, somut bir uluslararası hukuk kuralı olarak literatürdeki yerini almıştır. Söz konusu hüküm şu şekilde kaleme alınmıştır:

> *Teşkilâtın Üyeleri, milletlerarası münasebetlerinde gerek herhangi bir başka devletin toprak bütünlüğüne veya siyasî bağımsızlığına karşı, gerekse Birleşmiş Milletlerin amaçları ile telif edilemiyecek herhangi bir surette, tehdide veya kuvvet kullanılmasına başvurmaktan kaçınırlar.*

Kuvvet kullanma yasağı, günümüzde uluslararası örf ve âdet hukuku kurallarından evrilerek kabul edilen emredici bir düzenleme haline gelmiş ve bu kapsamda tüm devletler için bağlayıcı nitelik kazanmıştır.[160] BM Andlaşması, uluslararası hukukta kuvvet kullanmayı temel bir küresel norm olarak yasaklayan ilk andlaşma olarak tarih

---

[158] Fulya A. Ereker, "İlkçağlardan Günümüze Haklı Savaş Kavramı, **Uluslararası İlişkiler Dergisi**, Cilt:1, Sayı:3, 2004, ss. 29-30 ve Hüseyin Kocabay, **Uluslararası Hukukta Kuvvet Kullanımı**, (Yayınlanmamış Yüksek Lisans Tezi), Abant İzzet Baysal Üniversitesi Sosyal Bilimler Enstitüsü, Bolu, 2014, ss. 4-5.

[159] Gündüz, ss. 91-92.

[160] Shaw, s. 854 ve Fatma Taşdemir, "Uluslararası Anarşiye Giden Yol: Uluslararası Hukuk Açısından Önleyici Meşru Müdafaa Hakkı", **Uluslararası Hukuk ve Politika Dergisi**, Cilt:2, Sayı:5, 2006, s. 79.

sahnesinde yerini almıştır.[161] Görüldüğü üzere, söz konusu andlaşmanın BM Örgütü üyesi devletlere getirdiği en önemli yükümlülüklerden biri, uluslararası barış ve güvenliğin sağlanması için kuvvetten ve kuvveti tehdit olarak kullanmaktan kaçınmaktır.

Belirtmek gerekir ki; BM Andlaşması m. 2/4 hükmü, yalnızca devletler tarafından gerçekleştirilen ya da devletlere atfedilebilen kuvvet kullanma eylemlerine yönelik bir yasaktır. Nitekim bir devletin ülkesi içinde gerçekleşen ayaklanma, karışıklık, iç savaş durumlarında, farklı bir devletin davranışının etkili olduğu somut ve kuvvetli delillerle ispat edilemediği sürece kuvvet kullanma yasağı içinde değerlendirilmesi mümkün olmayacaktır.[162] Yasak kapsamına giren fiillerin tanımlanması ve bir devlete atfedilmesi; söz konusu saldırılara hukuki olarak cevap verilebilmesi açısından büyük bir öneme sahiptir.[163]

BM Andlaşması'nın yasaklamış olduğu kuvvet kullanma eylemlerinin yalnızca silahlı ve askeri kuvvet kullanımını kapsamadığı, ekonomik ve siyasi baskı yöntemlerinin de bu hüküm çerçevesinde değerlendirilmesi gerektiği yönünde muhtelif tartışmalar bulunmaktadır. *Pazarcı*'ya göre, hükmün silahlı kuvvet kullanımını yasakladığı aşikârdır.[164] Bu kapsamda, somut olayın incelenmesi ve mevcut eylemin kuvvet kullanma eşiğini hangi açıdan aştığına ilişkin değerlendirme yapılması önem arz etmektedir.

Kuvvet kullanma yasağına dair getirilen iki istisna bulunmaktadır. Bu istisnalar; BM Andlaşması'nda düzenlenmiş olan *'meşru müdafaa'* ve Andlaşma'nın VII. bölümü çerçevesinde uluslararası barışın tehdidi veya bozulması halinde BM Güvenlik Konseyi tarafından alınacak *'meşru müdahale'* tedbirleridir. Meşru müdafaaya ilişkin BM Andlaşması m. 51 hükmü şu şekildedir:

> *İşbu Andlaşmanın hiçbir hükmü, Birleşmiş Milletler Üyelerinden birinin silâhlı bir saldırmaya hedef olması halinde, Güvenlik Meclisi milletlerarası barış ve güvenliğin muhafazası için lüzumlu tedbirleri alıncaya kadar, tabii olan münferit veya müşterek meşru müdafaa hakkına halel getirmez. Bu meşru müdafaa hakkını kullanarak Üyelerin aldığı tedbirler derhal Güvenlik Meclisine bil dirilir ve Meclisin, işbu Andlaşmaya dayanarak milletlerarası barış ve güvenliğin*

[161] Hüseyin Pazarcı, **Uluslararası Hukuk**, 15. Baskı, Turhan Kitabevi, Ankara, 2016, s. 517.
[162] Pazarcı, ss. 517-518.
[163] Marco Roscini, "Cyber Operations as a Use of Force", **Research Handbook on International Law and Cyberspace**, (Ed. Nicholas Tsagourias and Russell Buchan), Edward Elgar Publishing, United Kingdom, 2015, s. 234.
[164] Pazarcı, s. 519.

muhafaza veya iadesi için lüzumlu göreceği şekilde her an hareket etmek yetki ve ödevine hiçbir veçhile tesir etmez.

Hüküm kapsamında meşru müdafaa, devletlerin doğal bir hakkı olarak görülürken, aynı zamanda bu hakkın kullanılmasına ilişkin uluslararası teamül hukukunda da kabul gören bazı kıstaslar bulunmaktadır. Söz konusu kıstaslar; silahlı saldırının var olması, aciliyet, gereklilik, oranlılık ve alınan önlemlerin BM Güvenlik Konseyi'ne bildirimi şeklinde ifade edilmektedir.[165] Güvenlik Konseyi'ne bildirim maddi bir şart niteliğinde değildir. BM Andlaşması m. 51'de bir prosedür olarak açıklanmakta ve usuli bir şart olarak kabul edilmektedir. Şartın yerine getirilmemesi meşru müdafaa hakkının varlığını ortadan kaldırmayacaktır. Nitekim meşru müdafaa hakkının özü aynı zamanda uluslararası teamül hukukuna, devletlerin egemenliğine dayanmaktadır. Bu nedenle BM Andlaşması'nın VII. Bölümünde karşımıza çıkan zorlayıcı askeri tedbirler istisnasından farklı olarak ilgili devlet, Güvenlik Konseyinin yetkilendirmesine tabi değildir. Ancak yine de devletlerin bu kapsamda aldıkları önlemlerin Konsey'e derhal bildirilmesi daha uygun olacaktır. Bildirim sonrasında Güvenlik Konseyinin olaya müdahil olarak kararlar alması halinde, meşru müdafaa hakkı sona erecektir.[166]

Oranlılık, gereklilik ve aciliyet koşullarına kısaca değinilecek olursa, meşru müdafaa tedbirlerini ortaya çıkaran durumun niteliğine göre bir değerlendirme yapmanın somut olay açısından önem arz ettiği söylenmelidir. Caroline Olayı ile devletler nezdinde kabul edilen bu koşullar için net bir tanım bulunmamaktadır. Dönemin Amerikan Dışişleri Bakanı Webster'ın görüşleri çerçevesinde yapılan açıklamalar şartları somut bir hale getirmek için yardımcı olmaktadır. Oranlılık şartında temel unsur mevcut saldırının giderilecek ölçüde bir müdahalede bulunulmasıdır. Gereklilik ve aciliyet şartlarında ise tehdit ani, karşı koyulamaz, başka suretle giderilemez bir boyut kazanmış, devletin kendini koruyabilmesi için son çare meşru müdafaa kalmıştır.[167]

Silahlı saldırının varlığı koşulunun gerçekleştiğine dair delilleri sunma külfeti, meşru müdafaa hakkını kullanmak isteyen devlete aittir. Nikaragua Kararı'nda da

---

[165] Gürcan Balık, "Anayasa'da "Milletlerarası Hukukun Meşru Saydığı Haller" Sorunu", **Uluslararası İlişkiler Dergisi**, Cilt:12, Sayı:47, 2015, s. 52.

[166] Sur, s. 295 ve Pazarcı, s. 523.

[167] Ömer Lütfi Kanburoğlu, "Önleyici Harekât Stratejileri ve ABD", 2012, http://www.kanburoglu.com/makale153.htm (05.01.2022).

ayrıca vurgulanan delilleri sunma külfetinin yerine getirilmemesi, gereklilik koşulunu da etkilemekte ve meşru müdafaa hakkının uluslararası hukuka uygun şekilde kullanılmasının zemini kaybolmaktadır.[168] Bir saldırının defedilmesi amacı taşıyan meşru müdafaa, bu amacı aşan bir eyleme dönüşmemeli yahut cezalandırma amacı gütmemelidir.

Meşru müdafaa hakkının en önemli koşulu olan silahlı saldırıya dair BM Andlaşması'nın içeriğinde kavramsal bir tanım bulunmamakla birlikte, birçok uluslararası çalışma yapılmış ve UAD kararlarıyla bir içtihat da geliştirilmiştir. Bu noktada 14.12.1974 tarih ve 3314(XXIX) sayılı *"Saldırının Tanımı Kararı"*[169] ve Karar'da saldırı olarak kabul edilebilecek eylemlerin m. 4 uyarınca örnekseyici olarak sayıldığı m. 3 hükmü karşımıza çıkmaktadır. Aynı zamanda BM Andlaşması m. 2/4'teki yasak kapsamında değerlendirilecek saldırı fiillerini açıklayan ilgili hüküm, şu şekilde kaleme alınmıştır:

> *Aşağıdaki fiillerden herhangi biri, bir savaş ilanına bakılmaksızın, 2. madde hükümlerine tabi ve bu hükümlere uygun olarak, bir saldırı fiili olarak nitelendirilecektir:*
> *(a) Bir devletin silahlı kuvvetleri tarafından, başka bir devlete istila yahut saldırıda bulunulması ve her ne kadar geçici olursa olsun bu tür bir istila ve saldırıdan ileri gelen herhangi bir askeri işgal ya da kuvvet kullanımı yoluyla devletin ülkesinin veya bir bölümünün ilhakı;*
> *(b) Bir devletin silahlı kuvvetlerinin, başka bir devletin ülkesini bombalaması veya diğer devletin ülkesine karşı herhangi bir silah kullanması;*
> *(c) Bir devletin limanlarının veya kıyılarının, başka bir devletin silahlı kuvvetleri tarafından ablukaya alınması;*
> *(d) Bir devletin silahlı kuvvetlerinin, başka bir devletin kara, deniz veya hava kuvvetlerine yahut deniz ya da hava filolarına saldırması;*
> *(e) Bir devletin silahlı kuvvetlerini andlaşmayla ülkesine kabul eden devlete karşı, silahlı kuvvetlerin andlaşmada belirtilen koşullara aykırı olarak kullanılması yahut andlaşma bittikten sonra da ülkede varlığını sürdürmesi;*
> *(f) Bir devletin ülkesini başka bir devletin tasarrufuna bırakması ve söz konusu diğer devletin üçüncü bir devlete karşı saldırgan eylemler gerçekleştirmek için ülkeyi kullanmasına izin verilmesi;*
> *(g) Bir devlet tarafından veya onun adına, başka bir devlete karşı yukarıda sayılan fiilleri gerçekleştiren silahlı çete, grup, düzensiz birlik veya paralı asker gönderilmesi yahut bu gibi fiillere esaslı katılım sağlanması.*

1986 tarihli Nikaragua Kararı, UAD'nin kuvvet kullanma, meşru müdafaa ve içeriğindeki kavramlar hakkında ayrıntılı açıklamalarını içeren ilk emsal karar

---

[168] Balık, s. 55.
[169] Gündüz, ss. 120-121 ve **United Nations General Assembly**, Definition of Aggression, 3314(XXIX), 1974, https://digitallibrary.un.org/record/190983/files/A_RES_3314%28XXIX%29-EN.pdf (05.01.2022).

niteliğindedir. Bir kuvvet kullanma eyleminin, silahlı saldırı olarak kabul edilebilmesi için çeşitli değerlendirmeler yapılan Nikaragua Kararı'ndaki tespitler şu şekildedir:[170]

- Silahlı saldırı BM Andlaşması m. 2/4'te düzenlenen kuvvet kullanma ve kuvvet kullanma tehdidinden daha dar bir anlam ifade etmektedir.
- Devletlerin kuvvet kullanması yahut kuvvet kullanma tehdidinde bulunması, BM Andlaşması m. 2/4'e aykırıdır ancak eylemin silahlı saldırı niteliğini taşıması için mutlaka 'büyük, yoğun ölçekli ve ciddi bir etkisinin olması' gerekir. Tek yahut kolektif bir saldırı mümkündür.
- Yoğunluğu ve etkileri bakımından önemsiz sayılabilecek, devletler tarafından gerçekleştirilmeyen sınır ötesi hareketler; silahlı saldırı yerine sadece 'sınır olayları' olarak değerlendirilebilir. Bu durumda devletler, meşru müdafaa hakkını kullanamasalar bile, kuvvet kullanımı içermeyen karşı tedbirlere başvurabilir.

Nikaragua Kararı'nda Saldırının Tanımı Kararına da atıf yapılmış, Saldırının Tanımı Kararındaki m. 3/g hükmü çerçevesinde örf ve âdet hukukunu yansıtan açıklamalar yapılmıştır. Bu çerçevede silahlı saldırının küçük çaplı sınır olaylarını aşarak devleti tehdit edecek düzenli güçlere dönüşmesi halinde meşru müdafaa hakkının doğabileceği ifade edilmiş; ayrıca doğrudan/dolaylı silahlı saldırı ayrımına dikkat çekilmiştir:[171]

- Bir eylemin doğrudan silahlı saldırı kapsamında sayılabilmesi için fail 'devlet' olmalıdır.
- Devletlerin doğrudan kendiyle bağlantısı olmayan düzensiz güçleri kullanarak dolaylı yoldan da silahlı saldırıda bulunması mümkündür. Eylemin dolaylı silahlı saldırı kapsamında olması için ise söz konusu devletin eylemlere esaslı katılımının olduğu belirlenmeli; somut olay değerlendirilerek eylem devlete isnat edilebilmelidir. İsnat edilebilirlik mümkün olmadığında, eylemin yoğunluğu hangi derecede olursa olsun, zarar gören devletin meşru müdafaa hakkını kullandığı iddiası tartışmalı hale gelebilecektir.

UAD, Nikaragua Kararı'na paralel bir şekilde, *"Kongo Demokratik Cumhuriyeti'ndeki Silahlı Faaliyetler"* hakkındaki kararında da meşru müdafaa

[170] Nikaragua Kararı, s. 103-104, prg. 195.
[171] Nikaragua Kararı, s. 103-104, prg. 195.

hakkının koşullarını açıklamıştır. Bununla birlikte, kuvvet kullanma yasağının BM Andlaşması'nın mihenk taşlarından biri olduğunu vurgulayarak meşru müdafaa hakkının BM Andlaşması m. 51 hükmüyle sınırlı kalmak üzere kullanılması halinde uluslararası hukukta geçerli kabul edilebileceğini ifade etmiştir.[172]

UAD'nin Nikaragua Kararı'ndaki tespitlerinin ardından, *James Green* tarafından oluşturulan, Divan'ın kabul ettiği müdahale, kuvvet kullanma ve silahlı saldırı eşiğini sınıflandıran tablo, çalışmamızın seyrinde önem arz etmektedir. Böylelikle, mevcut kuralların uygulamaya yansıması ve devletlerin hangi olayda ne şekilde tutum sergileyeceği somutlaşmış olacaktır. Nihayetinde, silahlı saldırı eşiğini geçemeyen eylemlerde, zorlayıcı ve zorlayıcı olmayan karşı önlemlere başvurulması hususuna da kısaca değinilecektir.

Tablo 2: Silahlı Saldırının Belirlenmesinde Genişletilmiş UAD Çerçevesi

Eylem	UAD Sınıflandırması	Hukuken Geçerli Yanıt	Kim Yanıt Verebilir?
Yeterli yoğunlukta düzenli kuvvetlerin gönderilmesi	Silahlı saldırı	Meşru müdafaa	Eyleme maruz kalan devlet veya o devletin talebi üzerine diğer devletler (bireysel ya da kolektif)
Yeterli yoğunlukta düzensiz kuvvetlerin gönderilmesi	Silahlı saldırı, kuvvet kullanımı, müdahale	Meşru müdafaa	Eyleme maruz kalan devlet veya o devletin talebi üzerine diğer devletler (bireysel ya da kolektif)
Sınır olayları/Yetersiz yoğunlukta düzenli veya düzensiz kuvvetlerin gönderilmesi	Kuvvet kullanımı, müdahale	Zorlayıcı karşı önlemler	Eyleme maruz kalan devlet (yalnızca bireysel olarak)
Silah/lojistik destek sağlanması	Kuvvet Kullanımı, müdahale	Zorlayıcı karşı önlemler	Eyleme maruz kalan devlet (yalnızca bireysel olarak)
İsyancılara finansman sağlanması	Müdahale	Zorlayıcı olmayan karşı önlemler	Eyleme maruz kalan devlet (yalnızca bireysel olarak)

Kaynak: James Green, **The International Court of Justice and Self-Defence in International Law**, Hart Publishing, Oregon, 2009, s. 61.

[172] Uluslararası Adalet Divanı, **Kongo Demokratik Cumhuriyeti'ndeki Silahlı Faaliyetler Davası**, 2005. İngilizce karar metnine ulaşmak için bkz. https://www.icj-cij.org/public/files/case-related/116/116-20051219-JUD-01-00-EN.pdf (03.12.2023).

Uluslararası hukukta, meşru müdafaa istisnasına varmayan ve devletlerin kullanımına açık iki tür karşı önlem bulunmaktadır. Bu önlemler, *'zararla karşılık ve misilleme'* olarak adlandırılmaktadır. Zararla karşılık; bir devletin başka bir devlete karşı, hukuk dışı yollar kullanarak düşmanca ve zarar veren eylemlerde bulunması ve bu duruma maruz kalan devletin hukuka aykırı eylemlerle karşılık vermesidir. Başlıca zararla karşılık örnekleri, ambargo, barış içinde abluka ve boykottur. Misilleme, zararla karşılıktan farklı olarak, hukuki ve meşru bir şekilde memnuniyetsizliğin ifade edilmesi yöntemidir. Diplomatik ilişkilerin kesilmesi, yabancıların sınır dışı edilmesi yahut haklarının sınırlanması, ekonomi ya da seyahat kısıtlamaları misillemeye verilebilecek örneklerdir.[173] Silahlı saldırı eşiğini geçmeyen, ancak devletlerin çıkarlarını zedeleyen eylemlere karşı misilleme yolu kullanılabilmektedir. Bunun yanında, devletlerin haklarını ihlal eden bir durum varsa hem zararla karşılık, hem de misilleme yolları gündeme gelebilmektedir. Böylece uluslararası barış ve güvenliğin korunması yönündeki adımlar kuvvetlenmekte, savaş gündeme gelmeden sorun ve uyuşmazlıkların çözülmesi sağlanmaktadır.

Savaş ve savaşa varmayan kuvvet kullanma eylemleri arasındaki sınırın belirlenmesi hakkında diğer önemli hükümler, 1949 Cenevre Sözleşmelerinin[174] ortak 2. ve 3. maddesidir. Uluslararası toplumun uyması gereken kuralları düzenleme çabasını yansıtan bu hükümler, insancıl muameleyi güvence altına almaktadır. Uluslararası insancıl hukukun temel prensipleri; ayrım gözetme, orantılılık, özen gösterme, askeri gereklilik ve gereksiz acıya sebep olmama şeklinde ifade edilmektedir.[175] Bununla birlikte, savaşan tarafların orantılılık ilkesi kapsamında belirli ölçütlere uygun davranması şart koşulmaktadır. Bu ölçütler; yeterli amaç,

---

[173] Ayrıntılı bilgi için bkz. M. Yusuf Eren, "Uluslararası Hukukta Savaşa Varmayan Kuvvet Kullanma Yolları", **İnönü Üniversitesi Hukuk Fakültesi Dergisi**, Cilt:3, Sayı:2, 2012, ss. 233-247.

[174] 1949 Cenevre Sözleşmelerinin ve bu Sözleşmelere Ek 1977 tarihli Protokollerin Türkçe metni için bkz. 12 Ağustos 1949 Tarihli Cenevre Sözleşmeleri ve Ek Protokolleri, (Yayına Hazırlayanlar: Melike Batur Yamaner, A. Emre Öktem, Bleda Kurtdarcan, Mehmet C. Uzun), Galatasaray Üniversitesi Yayınları, İstanbul, 2008. Sözleşmelerin İngilizce metni için bkz. International Committee of the Red Cross, **The Geneva Conventions of 12 August 1949**, https://www.icrc.org/en/doc/assets/files/publications/icrc-002-0173.pdf (03.02.2024). Sözleşmelere 196 devlet taraftır. Türkiye de Sözleşmeleri 21.01.1953 tarihli 6020 sayılı Kanun ile onaylamıştır. 10.02.1954 tarihinden itibaren de Sözleşmelere taraftır. Onaylama ve Sözleşme metinleri için bkz. RG 30.01.1953, Sayı: 8322.

[175] Ayrıntılı bilgi için bkz. İsmail Ataş, **Otonom Silah Sistemlerinin ve Siber Saldırıların Uluslararası İnsancıl Hukukun Temel Prensiplerine Uygunluğu**, Adalet Yayınevi, Ankara, 2023, ss. 59-74.

yoğunluk ve süre şeklinde ifade edilebilmektedir.[176] Böylece kuvvet kullanımının meşruluğu ve savaşın sürekliliği sınırlanmakta, savunma amaçlarına odaklanılmakta ve aşırı kuvvet kullanımının önüne geçilmektedir.

Bir silahlı saldırının hangi andan itibaren silahlı çatışma olarak görülebileceği ve çatışma hukuku kurallarının uygulanacağı, bahsi geçen ölçütlerin somut durumdaki yansımaları dikkate alınarak değerlendirilmelidir. Belirtmek gerekir ki; aşırı kuvvet kullanımı uluslararası insancıl hukuka aykırıdır ve savaş suçlarını gündeme getirebilmektedir.

B. Siber Uzayda Kuvvet Kullanma Yasağı ve Meşru Müdafaa

Uluslararası hukukta, siber uzay ve siber saldırılara dair herhangi bir özel düzenleme bulunmadığı için, mevcut kuralların ne şekilde uygulanacağı çeşitli tartışmalar yaratmaktadır. Bu sebeple, kuvvet kullanma yasağı ve meşru müdafaa hakkındaki temel ilke ve kuralların da ayrıca gözden geçirilmesi gerekmektedir. Tallinn Kılavuzu, bağlayıcı olmasa da bu konuyu ayrıntılı bir şekilde açıklayıp devletlere yol gösteren yegâne uluslararası çalışma olma özelliğini halen korumaktadır.

Kılavuz'un 68 ila 75 Numaralı Kurallarında siber saldırılar, kuvvet kullanma yasağı ve meşru müdafaa çerçevesinde ele alınmıştır. Buna göre, herhangi bir devletin toprak bütünlüğüne veya siyasi bağımsızlığına karşı tehdit oluşturan, kuvvet kullanımına varan yahut Birleşmiş Milletler'in amaçlarıyla bağdaşmayan siber saldırılar hukuka aykırı olarak kabul edilmiştir. Bununla birlikte, kuvvet kullanma yasağına aykırılık teşkil etmeyen faaliyetlerin, egemenlik, iç işlere karışma ve müdahaleye ilişkin temel düzenlemeleri ihlal edebileceği de ayrıca vurgulanmıştır.[177]

Tallinn Kılavuzu'nda, Nikaragua Kararı'ndaki tespitlere de atıf yapılan 69 Numaralı Kurala göre, siber saldırı; *'yoğunluk ölçeği ve etkileri açısından kuvvet kullanma olarak yorumlanabilecek, siber nitelikte olmayan bir başka saldırıyla karşılaştırılabilir seviyede'* ise kuvvet kullanımı anlamına gelmektedir. Bu hususta,

[176] Ayrıntılı bilgi için bkz. Didem Durmaz, "İnsancıl Hukukun Orantılılık İlkesi Çerçevesinde Tali Hasar Doktrinine Genel Bir Bakış", **Antalya Bilim Üniversitesi Hukuk Fakültesi Dergisi**, Cilt:10, Sayı:20, 2022, ss. 224-227.

[177] Tallinn Kılavuzu, ss. 329-330.

bir devletin vatandaşlarının hükümete duyduğu güveni sarsmak amacıyla gerçekleştirilen ve fiziksel herhangi bir tahribat yaratmayan psikolojik siber faaliyetlerin kuvvet kullanma yasağını ihlal etmeyeceği ifade edilmiştir. Diğer bir örnekte, bir isyanın parçası olarak siber faaliyetler yürüten bilgisayar eylemcilerine yalnızca finansal destek sağlayan devletin bu eyleminin kuvvet kullanma yasağına aykırılık teşkil etmediği belirtilmiştir.[178]

Kılavuza göre, kuvvet kullanmanın askeri yahut diğer silahlı kuvvetlerin istihdam edilerek gerçekleştirilmesi şart değildir. Bu sebeple organize bir silahlı gruba, siber faaliyetler yürütmesi için gerekli eğitimi veren ve kötü amaçlı yazılımlarla destek sağlayan devletler, kuvvet kullanmış ve yasağı ihlal etmiş olarak kabul edilmelidir. Ancak, bu hususun söz konusu devlete isnat edilmesinin ardından uluslararası sorumluluğun doğacağı da unutulmamalıdır.[179]

Tallinn Kılavuzu'nda siber saldırılara ilişkin, kuvvet kullanma yasağı çerçevesinde kullanılacak birtakım kriterler öngörülmüştür.[180] İlgili kriterler şu şekilde özetlenebilir:[181]

- Ciddiyet: Kapsam, süre, yoğunluk ve sonuçlarda büyük etki görülmesi.
- Aciliyet: Zararlı etkinin hissedilme ve azalma süresinin endişe verici boyutta olması.
- Doğrudanlık: Eyleme sebebiyet veren hususlar ve sonuç arasında dolaysız ve yakın bir ilişki bulunması.
- İstilacılık: Hedef ülke içinde bir siber ağa sızılması amacı güdülmesi.
- Ölçülebilirlik: Ölçü ve tanım yapılabilecek nitelikte somut olayların meydana gelmesi.
- Askeri Karakter: Eylemin askeri yahut silahlı organize kuvvetler aracılığıyla gerçekleştirilmesi.

---

[178] Tallinn Kılavuzu, s. 330.

[179] Tallinn Kılavuzu, s. 332.

[180] Tallinn Kılavuzu'nun hazırlanmasına öncülük eden Schmitt; siber saldırının bir silahlı kuvvet olarak görülmesinin önemini daha önceden fark ederek, meşru müdafaa hakkının kullanımında bazı genel geçer ölçütler belirlemeye çalışmıştır. Bu ölçütler; şiddet derecesi, zamansal yakınlık, doğrudanlık, yayılabilirlik, ölçülebilirlik ve muhtemel meşruiyettir. Bu ölçütler zaman içinde, teknolojinin ve siber uzayın gösterdiği gelişimle birlikte genişlemiştir. Ayrıntılı bilgi için bkz. Michael N. Schmitt, **Computer Network Attack and The Use of Force in International Law: Thoughts on A Normative Framework**, Research Publication 1 Information Series, Institute for Information Technology Applications, USAF Academy, Colorado, 1999, s.18-19.

[181] Tallinn Kılavuzu, ss. 334-336 ve Delerue, ss. 294-296.

- Devletin Katılımı: Devlet ve gerçekleşen siber eylem arasında yakın ve net bir ilişki bulunması.
- Muhtemel Meşruiyet: Gerçekleşen eylemin araç ve nitelikleri ile kuvvet kullanma kategorisine girmesi.

Bir siber saldırının kuvvet kullanma kapsamında değerlendirilmesinin ardından gelecek en önemli soru ve sorunlardan biri, siber saldırıların silahlı saldırı niteliği ve bununla paralel olarak meşru müdafaa hakkının doğmasıdır. Bu hususta somut olaydaki siber saldırı yahut saldırıların niteliğinin ve meşru müdafaa koşullarının tespiti önem arz etmektedir. Bu noktada, uluslararası barış ve güvenliğin korunması gerekliliği de dikkate alınarak, oldukça hassas bir teraziyle değerlendirme yapılması gerekmektedir.

Nikaragua Kararı'nda yoğunluk ölçeği ve etki kıstaslarıyla silahlı saldırı değerlendirmesi yapılmıştır. Tallinn Kılavuzu'nda, yine söz konusu karara atıf yapılarak siber saldırıların silahlı saldırı niteliği açıklanmıştır. Buna göre, siber saldırı düzeyine varan bir siber faaliyetin hedefi olan devlet, doğası gereği sahip olduğu meşru müdafaa hakkını kullanabilir. Siber faaliyetlerin silahlı saldırı boyutu ise, yoğunluk ölçeği ve etkilerinin ciddiyetine bağlıdır.[182]

Kılavuz'a göre, meşru müdafaa bağlamında kuvvet kullanma hakkı, dış dünyadaki kinetik saldırılarla birlikte siber uzaydaki araç ve yöntemlerle gerçekleştirilen saldırıları da kapsamaktadır. Nitekim bazı siber faaliyetler, silahlı saldırı olarak sınıflandırılabilecek boyutta ve ciddiyette olabilmektedir. UAD'nin 08.07.1996 tarihli *"Nükleer Silah Tehdidinin veya Kullanımının Yasallığı Hakkında Danışma Görüşü"*[183] uyarınca bir faaliyetin silahlı saldırı niteliği tespit edilirken, saldırı araçlarının seçimi önem arz etmemektedir. Bu durum devletlerin uygulamalarında da aynı şekilde karşımıza çıkmakta ve meşru müdafaa hakkının tetiklendiği evrensel olarak kabul edilmektedir. Zira kullanılan araç ve yöntem ne olursa olsun, ciddi ıstırap veya ölüm içeren sonuçlar ortaya çıkabilmektedir. Bu minvalde bir muhakemenin, siber faaliyetler için de geçerli olacağı rahatlıkla söylenmektedir.[184]

---

[182] Tallinn Kılavuzu, s. 339.

[183] Uluslararası Adalet Divanı, **Nükleer Silah Tehdidinin veya Kullanımının Yasallığı Hakkında Danışma Görüşü**, 1996. İngilizce metne ulaşmak için bkz. https://www.icj-cij.org/public/files/case-related/95/095-19960708-ADV-01-00-EN.pdf (10.01.2022).

[184] Tallinn Kılavuzu, s. 340.

Silahlı saldırıların temel unsurlarından bir diğeri, sınır ötesi yapıda olmasıdır. Siber saldırılarda sınır ötesi eylemler, bir devletin başka bir devlete karşı gerçekleştirdiği yahut devletlerin dış aktörleri kendi adına yönlendirdiği faaliyetler olarak kabul edilmektedir. Ancak devlet dışı aktörlerin tek başına sınır ötesi bir eyleme girişmesi ve bu sebeple doğacak meşru müdafaa hakkı konusunda tartışmalar bulunmaktadır. Kılavuz'u hazırlayan Uluslararası Uzmanlar grubunun çoğunluğu tarafından, *'11 Eylül Saldırıları'*[185] örnek verilerek, terörist yahut isyancı grupların ve nihayetinde devlet dışı aktörlerin gerçekleştirdiği siber saldırılara karşı da meşru müdafaa hakkının doğacağı kabul edilmektedir. Siber saldırılarda devlet dışı aktörlerin örgütlenme boyutu, coğrafi sınırlama ve bireysel eylemlere ilişkin belirsizlik ve tartışmalar ise halen devam etmektedir.[186]

Kılavuz'a göre, meşru müdafaa hakkının kullanılması, gereklilik, orantılılık, yakınlık ve aciliyet koşullarının varlığına bağlıdır. Şüphesiz, silahlı saldırının gerçekleşmiş yahut gerçekleşmek üzere olduğuna dair makul bir tespit, meşru müdafaanın asli temeli olarak karşımıza çıkmaktadır. Siber saldırılarda da geleneksel silahlı saldırılara paralel olarak, eylemin sebep olduğu hasarın boyutu, zarara uğrayan hedefin nitelik ve durumu, siyasi etkenlerin varlığı gibi kıstaslarla silahlı saldırının varlığı tespit edilmelidir. Devlete bağlı kurum, kuruluş, tesis, teçhizat ve personele yönelik saldırılar; diğer koşulları sağladığı sürece silahlı saldırı olarak nitelendirilmekte ve meşru müdafaa hakkı doğmaktadır. İlgili tüm hususların tespitinde somut olayın özellikleri önem arz etmektedir.[187]

Siber saldırılarda meşru müdafaanın gerekliliği, zorlayıcı yahut zorlayıcı olmayan karşı önlemlerin yetersiz olduğu durumlar için geçerlidir. Alternatif seçeneklerin işe yaramadığı durumların sonucunda, orantılı bir şekilde kuvvet kullanma yolu tercih edilebilecektir. Orantılılık koşulu, savunma tedbirlerinin ölçeği,

---

[185] 11 Eylül 2001 tarihinde, ABD'ye karşı gerçekleştirilen terör saldırılarında, Birleşik Havayolları ve Amerikan Havayolları'na ait 4 uçak, El-Kaide terör örgütüne mensup 19 kişi tarafından kaçırılmış; İkiz Kuleler ve çeşitli devlet binaları zarar görmüştür. Bununla birlikte söz konusu Saldırılar, binlerce insanın ölümüne sebep olmuştur. BM Güvenlik Konseyi tarafından, 'hain terör saldırıları' kınanmış, BM Andlaşması'nın VII. Bölümü içeriğine dahil olan 1368 ve 1373 numaralı kararların başlangıç kısmında ise uluslararası terör faaliyetlerinin uluslararası barış ve güvenliği tehdit eden boyutundan bahisle bireysel ve kolektif 'doğal meşru müdafaa hakkının' bulunduğuna atıf yapılmış ve uluslararası toplum nezdinde devlet dışı aktörlere karşı da meşru müdafaa hakkının doğacağı kabul edilmiştir. Yoram Dinstein, **War, Aggression and Self-Defence**, 4. Baskı, Cambridge University Press, United Kingdom, 2005, s. 285.

[186] Tallinn Kılavuzu, ss. 340-346 ve Delerue, ss. 330,465.

[187] Tallinn Kılavuzu, ss. 346-347.

kapsamı, süresi ve yoğunluğunu sınırlamaktadır. Savunma tedbirlerinin, saldırıyla aynı nitelikte olması gerekmemektedir. Bu nedenle, geleneksel silahlı saldırılara siber saldırıyla karşılık verilmesi yahut aksi şekilde tedbir alınması mümkündür. Mevcut saldırıyı defedecek düzeydeki başarılı bir savunma, orantılılık ilkesinin karşılığı olacaktır.[188]

Yakınlık ve aciliyet koşullarında ise, siber saldırının gerçekleştiği yahut gerçekleşmesinin kesin ve önlenemeyecek boyutta olduğu durumlar ifade edilmektedir. Siber saldırılara ilişkin hazırlık faaliyetleri yahut düşmanca tutumlar sergilenmesi, meşru müdafaayı gerektirmemektedir. Saldırı pek yakın ve geri dönülemez hale geldiğinde meşru müdafaaya başvurulmaktadır. Siber saldırının tespit edilemeden ilerlemesi ve belirlenememesi halinde ise harekete geçmeyi haklı kılacak bir hadisenin meydana gelmesi beklenmelidir.[189]

Siber saldırılarda, meşru müdafaa tedbirlerinin uygulanması ve savunmaya geçilmesi sürecinde egemenlik ilkesi dikkatle düşünülmelidir. Mağdur devletin talep etmesi ve rıza göstermesi halinde, talep kapsamıyla sınırlı olmak üzere, kolektif bir şekilde meşru müdafaa tedbirlerine başvurulabilmektedir. Nihayetinde, bireysel yahut kolektif meşru müdafaa tedbirlerinin BM Güvenlik Konseyi'ne bildirilmesi zorunludur. Bu zorunluluk asli bir koşul değildir, bildirimin yapılmaması meşru müdafaa hakkına halel getirmez. Ancak, BM tarafından uluslararası barış ve güvenliği korumak adına olaylara müdahil olunabileceği de unutulmamalıdır.[190] Nihayetinde siber saldırılar, silahlı saldırı eşiğini geçerek devletler arasında karşılıklı ve fiili bir anlaşmazlık halini alırsa, uluslararası insancıl hukuk ve silahlı çatışma hukuku kurallarının uygulanması tartışma konusu olabilecektir.

IV. DEVLETLERİN ULUSLARARASI SORUMLULUĞU VE İSNADİYET

A. Devletlerin Uluslararası Sorumluluğu ve İsnadiyetin Mahiyeti

Sorumluluk, bir hukuk düzeninin öznesi olan kişilerin sahip olduğu yükümlülükleri yerine getirmemesi sebebiyle ortaya çıkan zarar ve zararın tazminini

[188] Tallinn Kılavuzu, s. 349 ve Delerue ss. 480-481.
[189] Tallinn Kılavuzu, ss. 350-354 ve Delerue, ss. 468-476.
[190] Tallinn Kılavuzu, ss. 355-356.

ifade etmektedir. Hukukun olduğu her yerde hak, yükümlülük ve dolayısıyla sorumluluklardan bahsedilecektir. Devletlerin de hukuka aykırı eylemleri sebebiyle uluslararası sorumluluğu doğabilmektedir. Farklı bir açıdan, uluslararası hukukta mevcut olan hak ve yükümlülükleri ihlal eden eylemlerin yarattığı yeni hukuki ilişki, uluslararası sorumluluk olarak adlandırılmaktadır.[191] Zararı meydana getiren ve mağdur olan taraflar arasındaki söz konusu hukuki ilişkide ise, yeniden denge sağlanması amaçlanmaktadır.

Uluslararası sorumluluğa ilişkin esaslar, uluslararası örf ve âdet kuralları olarak kabul edilmekte ve tüm devletleri bağlamaktadır. BM Örgütü'nün kurulmasından itibaren uluslararası sorumluluk konusunda bağlayıcı bir düzenleme yapılması istenmiş; nihayetinde 2001 yılında, BM bünyesinde uluslararası hukukun geliştirilmesi ve kodifikasyonu alanında çalışan Uluslararası Hukuk Komisyonu tarafından 59 maddelik *"Devletlerin Uluslararası Hukuka Aykırı Eylemlerinden Doğan Sorumluluğuna İlişkin Tasarı"*[192] hazırlanarak devletlerin uluslararası sorumluluğu için düzenlemeler kaleme alınmıştır. Söz konusu Tasarı, hem mevcut örf ve âdet kurallarına yer vermekte hem de birtakım yeni standartlar getirmektedir.[193]

Bir devletin uluslararası sorumluluğunun doğması için, uluslararası hukuka aykırı eylem, zarar, illiyet bağı ve isnadiyet koşullarının sağlanması gerekmektedir. Kural olarak uluslararası hukuka aykırı eylemler, uluslararası yükümlülüklerin bulunduğu alanlarda gerçekleşmekle birlikte, uluslararası andlaşmalarla özel sorumluluk halleri de öngörülebilmektedir. Nihayetinde, UAD Statüsü m. 38 uyarınca, uluslararası andlaşma, hukukun genel ilkeleri, örf ve âdetin ihlali halinde, devletler için uluslararası sorumluluğun doğacağı rahatlıkla söylenebilmektedir. Nitekim Korfu Boğazı ve Nikaragua Kararları'nda çok yönlü niteliğe sahip ihlallerin olduğu da görülmektedir.[194] Bu çerçevede Tasarının ilk maddesi *"Bir devletin uluslararası hukuka aykırı her eylemi, uluslararası sorumluluğuna yol açar."* cümlesiyle kaleme alınmıştır.

---

[191] Ali Bal, **Devletin Uluslararası Sorumluluğunun Doğması**, (Yayınlanmamış Yüksek Lisans Tezi), Dokuz Eylül Üniversitesi Sosyal Bilimler Enstitüsü, 2006, ss. 6-8.

[192] International Law Commision, **Responsibility of States for Internationally Wrongful Acts**, A/56/49, 2001, https://legal.un.org/ilc/texts/instruments/english/draft_articles/9_6_2001.pdf (11.01.2022).

[193] Sur, s. 276.

[194] Sur, s. 277.

Zarar ve illiyet bağı koşullarında ise, m. 31 karşımıza çıkmaktadır. Buna göre, haksız bir eylemin sonucu olan, maddi ve manevi bütün zararlar uluslararası hukuk kapsamındadır. Bu zarara sebep olan devlet, zararı tazmin etmekle yükümlüdür. Nitekim maddi zararlardan farklı olarak, manevi zararların da devletin itibarını etkileyeceği; bu çerçevede egemenliğin ihlali sonucunun doğabileceği göz önünde bulundurulmalıdır.[195] Söz konusu hüküm, şu şekilde kaleme alınmıştır:

> *Uluslararası hukuka aykırı eylemden sorumlu olan devlet, sebep olduğu bütün zararı onarmak zorundadır.*
> *Zararın kapsamı, uluslararası hukuka aykırı eylemin sonucu olan maddi ve manevi zararın tamamıdır.*

Uluslararası yükümlülüklerin ihlali, yapılması gereken bir şeyin yapılmaması ya da yapılmaması gereken bir şeyin yapılması şeklinde meydana gelebilmektedir. Yine de söz konusu eylemin yahut eylemsizliğin devletlere isnat edilmesi halinde uluslararası sorumluluğun doğacağı aşikârdır. Bu durum Tasarının 2. maddesinde şu şekilde ifade edilmiştir:

> *Eylem ya da ihmal içeren bir davranış olduğunda, bir devletin uluslararası hukuka aykırı eyleminin mevcut olması için gerekli haller şunlardır:*
> *(a) Uluslararası hukuka göre devlete isnat edilebilmesi ve*
> *(b) Devletin uluslararası bir yükümlülüğünün ihlalini teşkil etmesi.*

Bu iki koşulun, somut olayda kümülatif bir şekilde bulunması gerekmektedir. Aksi takdirde devletlerin uluslararası sorumluluğu doğmayacaktır.

Devlet organlarının faaliyetlerinde devletin sorumluluğu şüphesiz ve net bir şekilde tespit edilebilirken, bir devletin talimatıyla hareket eden kişi ve kurumların tespiti için aynı şey mümkün değildir. Devletlerin sorumluluğuna ilişkin bir iddia elbette ciddidir ve böyle bir sorumluluğu öne süren tarafın 'açık, inandırıcı ve ikna edici delillerle' bunu ispatlaması yerleşik içtihatta kabul edilmektedir.[196] Çalışmamız kapsamında, bu ikili ayrım ve hukuka aykırı bir eylemin devlete isnat edilmesi büyük öneme sahiptir.

Tasarının 4 ila 11. maddeleri, devlet organlarının eylemleri ve devletin otoritesi altındaki kişi ve kurumların eylemlerinde devletin sorumluluğunu açıklayan hükümler içermektedir. İlgili hükümler özetlenecek olursa, kamu gücünün kullanıldığı bütün uluslararası hukuka aykırı eylemlerde devletlerin sorumluluğu doğmaktadır. Bununla

[195] Sur, s. 282.
[196] Shaw, ss. 590-591.

birlikte özel kişilerin faaliyetlerinde devletin emir, talimat ve telkini söz konusuysa, bu eylemlerden de ilgili devletler sorumlu tutulabilmektedir. Devletlerin bizatihi kendi davranışı olarak benimsediği ve kabul ettiği eylemler için de uluslararası sorumluluk işleyecek, zararın tazmin edilmesi gerekecektir. İsyan ve ayaklanma halindeki gruplarda ise, devletler özen yükümlülüğünü ihlal etmediği sürece, herhangi bir sorumluluk doğmayacaktır. Özen yükümlülüğünün ihlali, devletlerin kendi egemenlik alanının başka devletlere zarar verilmesini engelleyecek şekilde kullanılması ve denetlenmesine dayanmaktadır. Hukukun genel ilkeleri kapsamında karşımıza çıkan bu husus, Korfu Boğazı Kararı'nda da ayrıca vurgulanmıştır.[197]

Herhangi bir eylem sebebiyle doğrudan yahut dolaylı bir şekilde zarara uğrayan devlet tarafından, söz konusu eyleme ilişkin koşullar ispat edildiği takdirde eylemin sona ermesi ve tazminat süreci işlemeye başlayacaktır. Bu hususta mağdur devletin rızası, meşru müdafaa, hukuka uygun yahut zarar veren eylemle orantılı karşı önlemler, mücbir sebep ve zorunluluk hali uygulamaları saklıdır.[198]

B. Siber Uzayda Devletlerin Uluslararası Sorumluluğu ve İsnadiyet

Siber uzayda uluslararası sorumluluk ve isnadiyet, siber eylemi gerçekleştiren failin ve fiilin kimliğinin ve konumunun tespiti sürecinde önem arz etmektedir. Nitekim bu tespit, eyleme verilecek cevabın ve muhatabın belirlenmesinde rol oynamaktadır. Ancak siber uzayın anonim, katmanlı ve hızlı yapısı sebebiyle siber eylemlerin ardındaki üst aklın tespit edilmesi güçleşmektedir.[199]

Uluslararası Hukuk Komisyonu'nun hazırlamış olduğu Tasarı ve bu çerçevedeki örf ve âdet kuralları dikkate alındığında, siber uzay faaliyetlerinin uluslararası sorumluluğa yol açmasına ilişkin soru ve sorunlar gündeme gelmektedir. Tallinn Kılavuzu, söz konusu kurallarla birlikte ele alındığında, siber saldırıların uluslararası sorumluluk çerçevesinde değerlendirilmesi için üç halden biriyle

[197] Korfu Boğazı Kararı, s. 22.
[198] Sur, s. 281.
[199] David D. Clark ve Susan Landau, "Untangling Attribution", **Harvard National Security Journal**, Cilt:2, Sayı:2, 2011, s. 324.

gerçekleşmesi gerektiği sonucuna varılmaktadır. Söz konusu haller şu şekilde ifade edilmektedir:[200]

- Siber saldırının devletin organları tarafından gerçekleştirilmesi.
- Siber saldırının devletin ihmali yahut görmezden gelmesi ve özen yükümlülüğünün ihlali sonucu gerçekleşmesi.
- Siber saldırının devlet dışı aktörler tarafından devletin emri, yönlendirmesi yahut denetimi altında gerçekleştirilmesi.

Tallinn Kılavuzu'nun 14 ila 19 Numaralı Kurallarında, uluslararası sorumluluk bahsi ayrıntılı bir şekilde ele alınmaktadır. Buna göre bir devlet, uluslararası hukukta sahip olduğu bir yükümlülüğün ihlalini oluşturacak 'siber bağlantılı eylemler' için uluslararası sorumluluk taşıyacaktır. Siber bağlantılı eylemler terimi, devletlerin bizatihi gerçekleştirdiği yahut müdahil olduğu siber faaliyetlerle birlikte, siber altyapının başka bir devletin kötü amaçlı kullanımlarına tahsisi, siber altyapıya ilişkin ihmal yahut siber faaliyetler için yazılım ve donanım sağlanması hususlarını da kapsamaktadır.[201]

UAD, uluslararası sorumluluğun karakterini birçok kararında teyit ederek yükümlülük ihlali ve isnadiyetin uluslararası sorumluluğun asli unsurları olduğunu açıklamaktadır. Söz konusu yükümlülükler, uluslararası andlaşmalar, hukukun genel ilkeleri, örf ve âdet kurallarından doğabilmektedir. Bu çerçevede devletler, birbirlerine karşı yükümlülüklerinin yanında, uluslararası toplum nezdinde de yükümlülüklere sahiptir. Fiziksel hasar veya zarar verme niyeti, uluslararası sorumluluğun belirlenmesi sürecinde asli unsurlar olmamakla birlikte, somut olayda önem arz edebilmektedir.[202]

Kılavuza göre, uluslararası hukuka aykırı bir eylemin gerçekleşmesi sonucu uluslararası sorumluluğun doğması, barış zamanını düzenleyen kuralların ihlaliyle birlikte silahlı çatışmalar için de geçerlidir. Her iki alt kategoriyi de ilgilendiren egemenlik, kuvvet kullanma yasağı, iç işlere karışmama ilkesi ve müdahale yasağı gibi temel kurallar, ihlali söz konusu olabilecek başlıca normlar olarak öne çıkmaktadır. Bu çerçevede devletlere pozitif eylem gerektiren yükümlülükler de yüklenmektedir. Örneğin, bilgisayar eylemcileri, terörist örgütlenmeler ve sair grupların siber uzayı

[200] Muhammed Fatih Kafadar, "Uluslararası Hukukta Devletlerin Sorumluluğu Bağlamında Siber Saldırıların Atfedilebilirliği Meselesi", **Galatasaray Üniversitesi Hukuk Fakültesi Dergisi**, Sayı:2, 2020, s. 1042.
[201] Tallinn Kılavuzu, ss. 84-85.
[202] Tallinn Kılavuzu, ss. 84-86.

kullanması ve gerçekleştirilen siber faaliyetler için iç hukukta kontrol, denetim ve tedbir mekanizmalarının işletilmesi, devletlerin uluslararası hukuk nezdinde de görevi olarak görülmektedir.[203]

Siber uzayda gerçekleştirilen bir eylem, uluslararası hukukta uygulanması gereken kuralları ihlal niteliği taşımadığı sürece uluslararası hukuka tabi değildir. Devletlere açıkça izin verilen ya da uluslararası hukukta düzenlenmeyen hususlarda uluslararası sorumluluk doğmayacaktır.[204] Nitekim Bozkurt-Lotus Kararı'nda açıkça belirtildiği gibi, uluslararası hukukun düzenleme altına almadığı hususlarda, egemenlik ilkesi gereği devletin yetkisi esas olarak görülmektedir. Örneğin, bir devletin siber ortamdaki istihbarat amaçlı casusluk eylemleri, herhangi bir zarara mahal vermediği sürece, uluslararası toplumdaki huzur ve güvenliği tehdit etmemektedir. Devletlerin istihbarat, silahlı kuvvet, iç güvenlik ve sair hususlarda yetki alanını aşıp uluslararası hukuku ihlal niteliğindeki eylemlere girişmesi halinde ise uluslararası sorumluluğu doğacaktır. Söz konusu durum uluslararası örf ve âdet hukuk kurallarında, devletlerin kendi ülkelerindeki faaliyetleri ile bir başka devlete zarar vermesinin yasak olması ve bu kapsamda devletlerin gerekli özeni göstermesi (due diligence) şeklinde kabul edilmektedir.[205]

Siber uzayda uluslararası hukuka aykırı bir eylemin gerçekleştirilmesinde coğrafi sınırlama bulunmamaktadır. Devletler, söz konusu eyleme kendi topraklarında, zarar vereceği devletin topraklarında, üçüncü bir devletin topraklarında, açık denizlerde, uluslararası hava sahasında ya da uzayda girişebilmektedir.[206]

Son olarak, siber faaliyetlerin rıza, meşru müdafaa, karşı önlemler, gereklilik, mücbir sebep ya da zorunluluk hali çerçevesinde gerçekleşmesi durumunda hukuka aykırılık söz konusu olmamaktadır. Söz konusu haller uluslararası hukukta hukuka uygunluk sebebi olarak karşımıza çıkmaktadır.[207] Bu durumlarda, egemenlik ilkesinin bir yansıması olarak ilgili devlet kendi iç işleyişi hakkında karar vermekte, hukuka uygunluk sebepleri nezdinde çeşitli yöntemlere başvurabilmektedir.

[203] Tallinn Kılavuzu, s. 85.
[204] Tallinn Kılavuzu, s. 85.
[205] Bolat, s. 26.
[206] Tallinn Kılavuzu, s. 87 ve Jensen, s. 750.
[207] Tallinn Kılavuzu, s. 104.

1. Devlet Organları Tarafından veya Özen Yükümlülüğünün İhlali Sonucu Gerçekleştirilen Siber Saldırılar

Devletlerin Uluslararası Hukuka Aykırı Eylemlerinden Doğan Sorumluluğuna İlişkin Tasarı ve Tallinn Kılavuzu çerçevesinde, bir devletin organları ya da kamu gücünü kullanma yetkisine sahip kişi veya kuruluşlar tarafından gerçekleştirilen siber faaliyetler devletlere atfedilebilir. Söz konusu ifade oldukça geniştir; devletin nezaretinde, iç hukuk tarafından yetkilendirilmiş, işlevi yahut ülkedeki yeri ne olursa olsun devlet çatısı altındaki her kişi, kurum ya da kuruluş bu kapsamda görülmekte, yetki aşılarak gerçekleştirilse dahi girişilen her eylem, devlet için uluslararası sorumluluğa yol açabilmektedir.[208]

Devlet otoritesinin niteleyici unsurları, hükümetin temel işlevlerini ifade etmektedir. Farklı bir anlatımla, mevcut hükümetin yetkilerini kullandığı, dış işlerin yürütülmesi, vergi toplama, kolluk kuvvetlerini kullanma gibi eylemler devlet otoritesinin bir yansımasıdır. Ancak her eylemde devlet otoritesinin varlığı kesin değildir. Her bir somut olay bakımından devletin yetkilisi, amacı, geçmişten bu yana süregelen uygulamalar ve nihayetinde hesap verilebilirlik kıstaslarıyla değerlendirme yapılması gerekmektedir.

Devletler bizatihi devlet faaliyeti olarak yürütülmesi gereken meselelerde de gerekli teknik donanıma sahip olmaması ya da kendi kurumlarıyla faaliyet yürütmek istememesi hallerinde özel yahut gönüllü kuruluşlara başvurabilmektedir. Bu durumda uluslararası hukuka aykırı bir eylem meydana geldiğinde, söz konusu eylem devlete isnat edilebilir nitelikteyse devletin uluslararası sorumluluğu doğabilecektir. Siber eylem ve saldırılar için bu hususta, hükümet tarafından belirlenen askeri ağların siber savunmasını yürütmek için çalışan bir şirket tarafından gerçekleştirilen uluslararası hukuka aykırı eylemlerin devlete atfedilmesi örnek olarak verilebilmektedir. Bununla birlikte Tallinn Kılavuzu'na göre; şirket, yetkisini aşan bir şekilde, devletin ağlarına karşı gerçekleştirilen kötü amaçlı siber eylemleri bertaraf etmek için karşı siber saldırı yöntemlerine başvurursa, söz konusu eylemlerden devlete atfedilebilecek bir sorumluluk doğmaması mümkündür. Nitekim şirketin amacı ve verilen yetkiler doğrultusunda, yalnızca savunmayı sağlaması gerekli ve yeterlidir. Farklı bir örnekte

[208] Tallinn Kılavuzu, s. 87.

aynı şirketin, devlet içindeki özel kuruluşlar için bilgi güvenliği hizmeti yürütmesi halinde, söz konusu hizmette yetki aşımı sebebiyle karşılaşılan sorunlar, devletin sorumluluğunda olmayacaktır.[209] Yetkinin devlet tarafından, devlet kurumları için verilmiş olması ve söz konusu yetkinin sınırları aşılarak özel kişi ve kuruluşlar tarafından işlem yapılmaması, isnadiyet için asli koşullardır.

Uluslararası hukuka aykırı bir eylemde, devlet otoritesinin bulunduğuna ilişkin emareler, mağdur devlet tarafından ispat edilmelidir. Geleneksel olarak, tanklar ve savaş gemilerinin kullanımı yalnızca devlet eliyle gerçekleştirilebileceği için yeterli ve güçlü bir isnat göstergesidir. Siber uzaydaki eylem ve saldırılar için ise, benzer bir kolaylık bulunmamaktadır. Nitekim devlet dışı siber aktörlerin, hükümetin siber uzayda sahip olduğu ayrıcalık ve yetkileri ele geçirip siber altyapıyı kullanması yahut devletin siber altyapısına yönlendirmede bulunması mümkündür. Pratikte böyle bir durum devletler için sorun oluşturacak olsa da sorumluluğun doğması için yeterli görünmemektedir. Ancak devletlerin bu durumda başat rol oynadığına ilişkin güvenilir ve ispatı mümkün bir istihbarat, olayların seyrini değiştirebilmektedir.[210]

Kılavuza göre, bir devletin kendi yetkisindeki bir organı başka bir devletin tasarrufuna sunması halinde, söz konusu organın ikinci devletin emri altında gerçekleştirdiği siber faaliyetler, ikinci devlete atfedilebilir ve uluslararası sorumluluk söz konusu olur. Bununla birlikte, ilk devletin geri çağırma ve faaliyetleri durdurma şeklindeki özen yükümlülüğünü yerine getirmesi gerekmektedir. Aksi takdirde meydana gelecek uluslararası aykırı eylemden ilk devlet de sorumlu tutulabilecektir. Ancak organ, ilk devletin talimatlarına uygun bir şekilde hareket etmeyip eylemlerine devam ederse bu kural uygulanmayacaktır.[211]

2. Devlet Dışı Aktörler Tarafından Gerçekleştirilen Siber Saldırılar

Kural olarak özel kişi, grup ve kuruluşların siber faaliyetleri, devletlerin uluslararası sorumluluğuna yol açmamaktadır. Ancak Uluslararası Hukuk Komisyonu tarafından hazırlanmış Tasarı ve Tallinn Kılavuzu'na göre, devlet dışı aktörler tarafından yürütülen siber faaliyetler, bir devletin emri, yönlendirmesi yahut denetimi

[209] Tallinn Kılavuzu, ss. 90-91.
[210] Tallinn Kılavuzu, ss. 91-92 ve Jensen s. 751.
[211] Tallinn Kılavuzu, s. 93 ve Jensen s. 751.

altında gerçekleştirildiğinde ya da devletin bizatihi kendisine ait olarak kabul edip benimsediği meselelerde devletlere atfedilebilmektedir. Bu kıstasların fiili ilişkideki yansımaları, somut olaya göre değişkenlik gösterebilmektedir. Nitekim uluslararası hukukta her olay, kendi olgularına bağlıdır.[212]

Bir devletin talimatlarına göre hareket etmek, ekseriyetle devlet yetkisi çerçevesinde çalışan özel kişi ve kuruluşların eylemleriyle eşdeğerdir. Bu hususta aradaki fark, yasal olarak yetkilendirme unsurundan kaynaklanmaktadır. Konuya ilişkin en tipik örneklerden biri, bir devletin altyapısına karşı gerçekleştirilen kötü amaçlı siber eylemlerde, devletin krize müdahale etme amacıyla devlet dışı aktörleri teşvik etmesi, söz konusu aktörlerin devlete yardımcı olmak amacıyla gönüllü bir şekilde hareket etmesidir. Benzer bir şekilde, devletin geleneksel askeri faaliyetlerini desteklemek için belirli şekillerde siber saldırılar gerçekleştirmesi istenen aktörlerin talep kapsamındaki eylemleri de devletlere atfedilebilmekte, bu çerçevede uluslararası sorumluluk gündeme gelebilmektedir.[213]

Devlet dışı aktörlerin emir, yönlendirme ve denetim kapsamındaki davranışları, Nikaragua Kararı'nda belirtildiği üzere, devletin ciddi katılımı ve etkin kontrolü kavramlarıyla bir arada değerlendirilmelidir. Belirli bir siber faaliyetin yürütülmesinde, devlet dışı aktörlerin eylemi, süreci ve sonucu belirleyecek nitelikte, faaliyetin vazgeçilmez bir parçasıysa ve bu eylem bizzat devlet tarafından destekleniyorsa, devlete atfedilmesi gerekmektedir. Etkin kontrole örnek olarak, bir devletin, diğer bir devletin bilgisayarlarında kullanılan yazılıma, devlet dışı aktörlerin yardımıyla güvenlik açıkları yerleştirmesi ve bu açıklardan siber eylemlerle yararlanılması emrini vermesinde, aktörlerin davranışını kontrol eden devlet sorumlu tutulacaktır.[214]

Devlet dışı aktörlerin yetkisini aşan yahut devlet tasarrufundan bağımsız eylemlerde bulunması, devletlere atfedilemez ve bu çerçevede uluslararası sorumluluk doğmaz. Ancak bütünsel bir yaklaşımla, devletin ulaşmak istediği amaç yolunda, söz konusu eylemin önemli bir nitelik taşıdığı tespit edilirse, yine devlete isnadiyet mümkün olabilecektir. Bu hususta bir devlet tarafından, başka bir devletin

[212] Tallinn Kılavuzu, s. 95.
[213] Tallinn Kılavuzu, ss. 95-96.
[214] Tallinn Kılavuzu, s. 96 ve Jensen s. 751.

topraklarındaki devlet dışı aktörlere kötü amaçlı yazılım desteği sağlanması ve karışıklığa yol açılması örnek olarak verilebilmektedir.[215]

Nihayetinde devletlerin, uluslararası hukuka aykırı eylemlerin bilincinde olarak, bu eylemleri gerçekleştiren devletlere ve devlet dışı aktörlere yardım etme, eylemlere etkin bir şekilde müdahil olma ya da bu tür eylemlere zorlama şeklindeki davranışlarının tamamından sorumlu tutulabileceği, ehemmiyetle göz önünde bulundurulmalıdır. Kuvvet kullanma eşiğini aşan ve en az silahlı saldırı kadar etkili bir siber saldırının, devlet destekli olarak gerçekleştiğinin açık ve kuvvetli kanıtlarla ispat edilmesi halinde, kuvvet kullanma yasağının ihlali hususu gündeme gelebilecektir.[216] Ancak siber saldırıların anonim olabilme niteliği sebebiyle, isnat sürecinde muhtelif sorunlar yaşanabilmektedir.[217]

Siber eylemlerin ekseriyeti, kuvvet kullanma yasağını ihlal edecek kadar büyük ve kapsamlı sorunlara yol açmasa dahi, kalıcı ve izinsiz sistem girişlerinden oluşmaktadır. Başka bir devletin iç işlerine karışma, müdahale ve egemenlik bağlamında düşünüldüğünde, uluslararası hukukun siber faaliyetler için de geçerli olacağı ve gerekli şartların varlığı halinde uluslararası sorumluluğun doğacağı mühim bir gerçek olarak gün yüzüne çıkmaktadır.[218]

[215] Tallinn Kılavuzu, ss. 98-100 ve Jensen s. 752.
[216] Tallinn Kılavuzu, s. 100.
[217] Korhan, **Parametreler**, s. 32.
[218] Moynihan, s. 2.

ÜÇÜNCÜ BÖLÜM
SİBER UZAYDA DEVLET UYGULAMALARINA DAİR BAŞLICA ÖRNEKLER

Siber saldırılar, yıldırma ve zorlama gücüyle, modern ve teknolojik saldırı taktikleri arasında önemli bir konumdadır. Özellikle teknolojiye yatırım yapan gelişmiş devletler, siber uzayda aktif olarak rol almakta ve uluslararası arenada siber saldırıların mahiyeti hakkındaki tartışmalara yön vermektedir. Siber saldırıların farklı nitelikleri göz önüne alındığında, devletlere karşı gerçekleştirilen siber saldırılardan dolayı uluslararası barışın bozulabileceği, ülke ekonomilerinde ve toplumsal yapılarda sorun meydana gelebileceği ve nihayetinde siber saldırıların her konuda tehdit oluşturabileceği açıktır.

Genel olarak ifade etmek gerekirse; elektrik, doğalgaz, su ve internet hatları gibi devletlerin mahiyeti gereği sürekliliğini sağlayan ve vatandaşlarına sunması gereken temel hizmetler, uluslararası hukuktaki egemenlik alanları kapsamında değerlendirilmekte ve bu alanlara bir başka devletin müdahalesi uygun görülmemektedir. Bununla birlikte sınırların ve egemenliğin korunması amacıyla kullanılan askeri hizmetlerin sekteye uğratılması, nükleer merkezlerin ortadan kaldırılması, savaş teçhizatlarının bozulması, hava ya da deniz trafiğinde sorunlar yaşanması amacıyla gerçekleştirilen kötü niyetli saldırılar, kuvvet kullanma yasağı kapsamında değerlendirilebilmektedir. Nihayetinde devletlerle birlikte çok sayıda insanın sabotaja maruz kalması ve büyük ağırlıkta zararların meydana gelmesi ile sonuçlanan siber saldırılar, uluslararası mahiyette tartışmalara sebep olmaktadır.[219]

Devletler tarafından diğer devletleri istikrarsızlaştırmak, koruma sistemlerini felce uğratmak ya da kamu hizmetlerini akamete uğratmak için kullanılan siber saldırıların, uluslararası hukuktaki temel ilkelere uygunluk bakımından değerlendirilmesi giderek daha önemli hale gelmektedir. Uluslararası hukukta geçerli olan ve önemini her daim koruyan kuvvet kullanma ve müdahale yasağı kavramlarının siber saldırılardaki mahiyetinin değerlendirilmesi için çeşitli örneklerle konuya açıklık getirilmesi gerekmektedir. Bu kapsamda, dünya genelinde devletler tarafından diğer

[219] Erdi Şafak, "Uluslararası Hukukta Değişen Güvenlik Algısı Ve Saldırı Suçu Bağlamında Siber Saldırılar", **Selçuk Üniversitesi Hukuk Fakültesi Dergisi,** Cilt:28, Sayı:1, 2020, ss. 134-135.

devletlere yönelik gerçekleştirildiği iddia edilen siber saldırıların örnekler kapsamında değerlendirilmesi yararlı olacaktır. Devletlerle ilişkilendirilen siber saldırılar, yoğunluk ve etkileri de göz önüne alınarak, tarihsel bir sıralama ile konumuz dahilinde incelenecektir. Somut olaylara ilişkin değerlendirmeler yapılırken, tez konumuz boyunca aktarılan temel bilgiler ışığında ilerlenecektir.

I. EGEMENLİK, İÇ İŞLERE KARIŞMAMA İLKESİ VE MÜDAHALE YASAĞINA İLİŞKİN ÖRNEKLER

A. İlk Siber Saldırı ve Uluslararası Hukuk Tartışmaları: Estonya (2007)

Estonya, tarihi boyunca Rusya ve Almanya tarafından çeşitli zamanlarda işgal ve eziyetlerle karşı karşıya kalmış bir ülkedir. İkinci Dünya Savaşı sırasında Estonya, ilk olarak Sovyetler Birliği tarafından işgal edilmiş ve savaş sürecindeki çeşitli olaylarla birlikte Almanya'nın kontrolüne geçmiştir. Savaşın sonunda Sovyetler Birliği'nin tekrar Estonya'yı işgal etmesiyle Estonya, Soğuk Savaşın sonuna kadar Sovyetler Birliği'nin bir parçası haline gelmiştir.[220]

Soğuk Savaşın sona ermesinin ardından, Sovyetler Birliği'nin dağılması ile birlikte birçok devlet bağımsızlıklarını ilan etmiştir. Estonya da bağımsızlığını ilan eden devletlerden biri olarak tarih sahnesinde yerini almıştır. Ancak Estonya, Sovyetler Birliği'nden ayrılan birçok devletin aksine, birlikte yaşadıkları Rus azınlığa vatandaşlık vermeyi reddetmiştir. Bu azınlık ülke içindeki nüfusun yaklaşık %40'ını oluşturmaktadır.[221] Estonya hükümeti, bu politikayı ülkenin milli kimliğini koruma amacı ve güvenlik endişeleri çerçevesinde sürdürmüş olsa da bu durum, Estonya ile Rusya arasındaki ilişkilerde sorunlara yol açmıştır. Rus azınlığın vatandaşlık alamaması veya azınlık haklarının yeterince korunmaması, diplomatik gerginlikler ve siyasi anlaşmazlıklarla karşı karşıya kalınması sonucunu doğurmuştur. Estonya ve Rusya arasındaki ilişkilerdeki gerilim, çeşitli dönemlerde farklı boyutlar kazanarak uluslararası ilişkilerde tartışmalar yaratmaya devam etmiştir.

[220] Ferit Güven, **Siber Saldırılar ve Türk Kamu Yönetiminin Çözümleri**, (Yayınlanmamış Doktora Tezi), Süleyman Demirel Üniversitesi Sosyal Bilimler Enstitüsü, Isparta, 2022, ss. 289-290.
[221] Güven, ss. 289-290.

Estonya, 2000'li yılların başından itibaren internet temelli altyapı yatırımlarına büyük önem vermiştir. Yüksek ölçüde eğitimli nüfusu ve teknolojik mirasıyla birleşen bu yatırımlar sayesinde Avrupa'nın en gelişmiş *'e-devlet'* olarak isimlendirilen iletişim, telekomünikasyon, yazılım ve ağ teknolojilerini kapsayan bir sistem kurmuştur. Bu sistem devletlerin gelişimine destek olacak birçok teknolojik yeniliğin önünü açmıştır. Estonya'nın teknolojik altyapısı ve internet kullanımı, bu gibi yenilikçi projelerin doğmasını ve gelişmesini teşvik etmiştir. Bu da Estonya'yı dijital bir lider ve teknoloji merkezi haline getirmiştir. Estonya'nın görece ileri düzeydeki e-devlet sistemi, diğer devletlere örnek teşkil etmiş ve dijital dönüşüm konusunda ilham vermiştir.[222]

Estonya'ya yönelik siber saldırıların tetikleyicisi, Estonya hükümetinin Sovyetler Birliği döneminde yapılmış olan ve *'Bronz Asker'* olarak bilinen heykelin kaldırılması kararıdır. Bronz Asker heykeli, uzun yıllar boyunca Tallinn şehir merkezinde bulunmuş ve Estonya'nın Nazi işgalinden kurtuluşunu simgelemiştir. Hükümet, söz konusu heykeli şehir merkezinden alarak daha az görünür bir yere taşımak istemiştir. Bu karar, Estonya'nın Rus azınlığı içinde bir kışkırtma olarak algılanarak protestolara neden olmuştur.

Kötü amaçlı siber korsanlar yahut siber savaşçılar, heykelin kaldırılması kararını bir fırsat olarak değerlendirmiş ve Estonya hükümetinin kritik altyapı tesislerine saldırılar düzenlemiştir. Bu saldırılar, devlet başkanlığı, parlamento, siyasi partiler, internet hizmet sağlayıcıları ve bankaların çevrimiçi hizmetlerinin engellenmesine yönelik DDoS saldırıları şeklinde gerçekleşmiş ve altyapı sistemlerini hedef alarak büyük zararlara yol açmıştır. 75 ayrı ülkeden yaklaşık bir milyon bilgisayarın ele geçirilmesi suretiyle Botnet adı verilen bir yapı ağı kurulmuş ve zombi bilgisayarlar aracılığıyla yoğun internet trafiği oluşturulmuştur. Hedef sistemlerin yoğunluğa dayanamayarak çökmesi sonucunda devletin teknolojik yapılanmasında sorunlar meydana gelmiştir. Söz konusu siber saldırılar Estonya'yı büyük ölçüde

[222] A. Burak Darıcılı, "Rusya Federasyonu Kaynaklı Olduğu İddia Edilen Siber Saldırıların Analizi", **U. Ü. Sosyal Bilimler Enstitüsü Dergisi,** Cilt:7, Sayı:2, 2014, s. 6 ve Rain Ottis, "Analysis of the 2007 Cyber Attacks Against Estonia from the Information Warfare Perspective", **Proceedings of the 7th European Conference on Information Warfare and Security**, Plymouth, Reading: Academic Publishing Limited, 2008, ss. 167-168.

etkilemiş ve ülkenin internet hizmetlerinde kesintilere neden olmuştur.[223] Siber saldırılar 26 Nisan - 19 Mayıs 2007 tarihleri arasında üç hafta boyunca devam etmiş ve Estonya'nın devlet hizmetlerinin büyük bir kısmı etkilenerek kullanılamaz hale gelmiştir. Saldırılar sırasında Estonya hükümeti, ülkenin ulusal internet ağına ülke dışından erişimi engelleme kararı almış olsa da saldırılar devam etmiş ancak makul ve katlanılabilir bir seviyeye düşürülmüştür.[224] Bu saldırılar sonucunda Estonya hükümeti büyük maddi zararlar yaşamış ve saldırının etkilerini gidermek için, bire beş yüz oranına denk gelecek büyüklükte, yüksek miktarda kaynak harcamak zorunda kalmıştır.[225]

Süreç içerisinde Estonya devlet kurumları, internet hizmet sağlayıcıları ve bankalar, saldırılara karşı önlemler alarak direnmiş olsalar da Estonya hükümetinin NATO üyesi devletlerden yardım talep ettiği görülmüştür. Saldırıların arka planında, Rusya ve NATO arasındaki yeni bir gerilim hattı olarak "siber alan" temelinde gelişmeler yaşanacağı gündeme gelmiş ve uluslararası hukuk bağlamında tartışmalar başlamıştır. Süreç içerisinde, NATO Genel Sekreter Yardımcısı Büyükelçi Sorin Ducaru, Estonya'nın NATO bünyesinde siber güvenlik politikalarının şekillendirilmesinde önemli bir rol oynadığını ifade etmiştir. Ayrıca, Rusya'nın daha sonrasında Gürcistan, Ukrayna ve Kırım'a yönelik olarak benzer saldırılar gerçekleştirmesi sebebiyle tehdidin büyüklüğünü vurgulamıştır. Bu sebeple NATO ülkeleri, Tallinn'e siber güvenlik uzmanları göndererek savunma sistemleri konusunda yardımcı olmuştur. NATO, Ağustos 2008'de Müşterek Siber Savunma Mükemmeliyet Merkezini Estonya'ya taşıyarak çalışmalarını bu alanda yoğunlaştırmıştır. Bu merkez üzerinden NATO siber savunma kavram ve temelleri oluşturulmuş, uluslararası düzeyde siber tatbikatlar gerçekleştirilmeye başlanmıştır.[226] Ancak, saldırganların anonim yapısından dolayı kimliklerinin tespit edilemediği belirtilmiştir. Bununla

[223] Yavuz Yener, "8. Yılında Estonya Saldırılarına Çok Boyutlu Bir Bakış", **SiberBülten,** 2014, https://siberbulten.com/siber-saldirilar-2/8-yilinda-estonya-saldirilarina-cok-boyutlu-bir-bakis (27.12.2022).
[224] Ottis, s. 52.
[225] Stephen Herzog, "Ten Years After the Estonian Cyberattacks: Defense and Adaptation in the Age of Digital Insecurity", **Georgetown Journal of International Affairs**, Cilt:18, Sayı:3, 2017, ss. 69-73 ve Sergei A. Medvedev, **Offense–Defense Theory Analysis of Russian Cyber Capability**, Calhoun: The Naval Postgraduate School (NPS) Institutional Archive, California, 2015, s. 19.
[226] Herzog, ss. 69-73.

birlikte, Rusya'nın Kremlin Sözcüsü Dimitri Peskov da söz konusu saldırıların Rusya ile herhangi bir ilişkisi olmadığını iddia etmiştir.[227]

Sonuç itibariyle, Rusya'nın saldırının kendisi tarafından yapılmış bir saldırı olduğu yönündeki iddiaları reddetme yolunu tercih ettiği ve kimin bu denli büyük bir saldırıyı gerçekleştirdiği konusunda kesin bir kanıt sunulamadığı bilinmektedir. Bu tür siber saldırıların tespit edilmesi ve saldırganların kimliklerinin belirlenmesi genellikle zorlu bir süreçtir. Saldırının gerçekleştiği ülke ile diğer ülkeler arasında iş birliği ve bilgi paylaşımı gerekmektedir. Ayrıca, güvenlik önlemlerini güçlendirmek ve siber saldırılara karşı korunmak için siber güvenlik farkındalığını artırmak da önemli hale gelmektedir.

Estonya devlet görevlileri yaşanan bu olayları, Rusya tarafından kendilerine yönelik olarak gerçekleştirilen bir siber saldırı olarak kaydetmiştir. Estonya istihbarat görevlilerine göre, Rusya bu tür saldırıları gerçekleştirebilmek için gerekli niteliği haiz araçlara ve kaynaklara sahip görülmektedir. Bununla birlikte Estonya devletinin iddiasına göre, geniş çaplı DDoS saldırıları sırasında Rusça konuşulan sosyal medya platformlarında ve web sitelerinde, vatansever Rusların bu siber saldırılara destek vermeleri gerektiği yönünde propaganda yapıldığı tespit edilmiştir. Diğer yandan, dönemin Rus hükümetinin bu saldırıları organize ettiğine veya en azından desteklediğine dair farklı işaretler bulunduğu ifade edilmiştir. Bu kapsamda, saldırıya katılan bilgisayarların çoğunluğunun IP adreslerinin Rusya kaynaklı olduğu, bu saldırılara katılan kişilerin önemli bir kısmının siber saldırılar konusunda deneyimlerinin bulunduğu ve Estonya'ya yönelik saldırıların Rusya tarafından planlı ve örgütlü bir şekilde gerçekleştirildiği iddialarını destekler nitelikte bulgular saptandığı belirtilmiştir.[228]

Estonya'ya yönelik siber saldırılar, uluslararası hukuk alanında çalışmalarını sürdüren bilim insanları tarafından detaylı bir şekilde ele alınmıştır. *Schmitt*'e göre, zikredilen saldırıların hükümet işlemleri ve kamu hizmetleri üzerinde önemli bir etkisi olmuştur. Ayrıca, hükümetin ekonomik faaliyetleri ve işlemleri anlık olarak etkilenmiş ve sonuç olarak vatandaşlar, hükümet fonlarına ve sağladığı diğer yararlara erişememiştir. Bu saldırılar, devlet üzerinde sadece ekonomik ve siyasi baskı kurmakla

[227] Merve Yazıcı, "İlk Modern Siber-Atak: Estonya, **TUİÇ Akademi,** 2015, https://www.tuicakademi.org/ilk-modern-siber-atak-estonya (27.12.2022).
[228] Darıcılı, s. 6.

kalmayıp, aynı zamanda idari ve ekonomik işleyişi kasıtlı olarak bozmak amacındadır. Tallinn Kılavuzu'nun ve Schmitt'in konuyu değerlendirdiği el kitaplarında ifade ettiği görüşlere göre, Estonya'ya yönelik saldırılar silahlı saldırı eşiğini geçmemektedir. Bu sebeple söz konusu olayları kuvvet kullanımı olarak tanımlamak, kuvvet kullanma yasağı bağlamında değerlendirmek mümkün değildir. Ancak Estonya'nın egemenlik alanına müdahale edildiği kuşkusuz bir gerçektir.[229]

Tsagourias da benzer şekilde, Estonya'ya karşı gerçekleşen saldırıların kuvvet kullanımı niteliği taşıyıp taşımadığı konusunda, saldırının şiddetinin sınırlı olduğu, zararlı etkisinin kontrol edilebilir seviyede olduğu ve saldırıların işgal niteliğinin geçici olduğu görüşündedir. Ekonomik ve finansal sonuçlarının yıkıcı olmaktan ziyade zamansal bir etkisinin olduğu kanısındadır. Tüm bunlara rağmen, Tsagourias, söz konusu saldırıların Estonya hükümetini kararından geri adım attırabilmek amacıyla yapılan uluslararası bir baskı niteliğinde olduğunu vurgulamış ve bu nedenle saldırıları müdahale yasağı ve devlet egemenliğinin ihlali olarak değerlendirmiştir.[230]

Bazı farklı yazarlar ise mevcut düzenlemelerin geniş yorumlanması gerektiği görüşündedir. Bu çerçeveden bakmak gerekirse, siber saldırıların kinetik etkilerini araştırmak yerine, bu saldırıların doğrudan devletin varlığına ve varlığını sürdürme hakkına yönelik bir saldırı olduğuna ve saldırının geniş sonuçları üzerinde durulması gerektiğine dikkat edilmelidir. Estonya örneğinde, somut hizmet ve süreç akışının engellenmesinden farklı olarak bilgi akışının engellendiği belirtilmekte ve günümüzde bilgi akışının bir toplumun fiziksel ve maddi refahı için hayati önem taşıdığı, geçmişe kıyasla daha önemli hale geldiği vurgulanmaktadır.[231]

Her halükarda, gerçekleşen bu olaylar, etkisi ve büyüklüğü sebebiyle egemenlik, iç işlere karışmama ilkesi ve müdahale yasağı bağlamında değerlendirilerek bu konudaki tartışmaları başlatan ilk siber saldırı olarak tarihte yerini almıştır.[232] Söz konusu siber saldırılar, Estonya'nın siber savunma yeteneklerini gözden geçirmesi ve uluslararası toplumun siber güvenlik konusundaki farkındalığının

---

[229] Michael N. Schmitt, "The Law of Cyber Warfare: Quo vadis?", **Stanford Law & Policy Review**, Sayı:25, 2014, s. 290.

[230] Nicolas Tsagourias, "The Tallinn Manual on the International Law Applicable to Cyber Warfare: A Commentary on Chapter II - The Use of Force", **Yearbook of International Humanitarian Law**, (Ed. Terry D Gill), Cilt:15, 2014, s. 25.

[231] Sheng Li, "When Does Internet Denial Trigger the Right of Armed Self-Defense?", **Yale Journal of International Law,** Sayı:38, 2013, ss. 191-201.

[232] Marc Goodman, **Future Crimes**, Penguin Random House, London, Great Britain, 2015, ss. 53-57.

artması için önemli bir dönüm noktası olmuştur. Estonya, yaşananların ardından uluslararası arenada siber güvenlik konusunda liderlik rolü üstlenmiştir. Uluslararası hukukta siber saldırılara karşı korunma ve siber savunma stratejileri konusunda çalışmalar yürütmek için işbirliği içinde adımlar atılmaya başlanmıştır. Zamanla tartışmaların ortak bir paydada birleşeceği ve uluslararası hukukta devletlerin egemenliği, kuvvet kullanma ve müdahale yasakları gibi temel kavramlar bağlamında siber saldırıların da devletlere zarar vermeyecek şekilde bertaraf edileceği düşünülmektedir.

B. Siber Saldırıların Hibrit Niteliği: Gürcistan-Rusya Sorunları (2008)

2008 yılında, Rusya ile Gürcistan arasında yaşanan Güney Osetya ve Abhazya krizinin sonucunda askeri çatışmalar ve siber saldırılar yaşanmıştır. Rusya Silahlı Kuvvetleri, Gürcistan'a karşı yürüttüğü askeri harekâtta geleneksel yöntemlerle ilerlerken, siber uzayda da yoğun saldırılar gerçekleştirmiştir. Bu sayede, düşmanının dikkatini iki farklı alana dağıtarak Gürcistan'a yönelik üstünlük elde etmeyi amaçlamıştır. Söz konusu olaylar, siber güvenlik ve uluslararası ilişkiler açısından önemli dönüm noktalarından biri olarak görülmektedir.[233]

Abhazya ve Güney Osetya, Sovyetler Birliği'nin yıkılmasından sonra özerk bölgeler olarak varlıklarını sürdürmüştür. Ancak 2008 yılı yaz aylarında, Gürcistan'da milli provokasyonlar gündeme gelmiş ve Gürcistan Askeri Kuvvetleri tarafından Güney Osetya'ya yönelik bir operasyon başlatılmıştır. Bu operasyonların amacı, ülkenin toprak bütünlüğünü korumak ve Gürcistan'ın egemenliğini bölgede sağlamak olarak düşünülmüştür. Ancak, ertesi günlerde Rusya Silahlı Kuvvetleri müdahalede bulunarak Gürcistan topraklarına girmiş, Gürcistan'a yönelik bir dizi işgal faaliyetine başlamış ve siber saldırılar da dahil olunca durum daha da karmaşık hale gelmiştir. Bu gerilimin temelinde, ideolojik ve jeopolitik faktörlerin etkili olduğu düşünülmektedir. Özellikle, Gürcistan'ın Batı Bloğu ülkeleri ve NATO ile siyasi ilişkilerini geliştirmeye yönelik adımlar atması ve Rusya'nın kendi yakın coğrafyasında NATO üyesi bir

[233] Emmanuel Karagiannis, "The 2008 Russian-Georgian War via the Lens of Offensive Realism", **European Security**, Cilt:22, 2013, s. 76.

ülkenin olmasını egemenliğine yönelik bir tehdit olarak algılaması, sorunun temel unsurlarından biri olarak öne çıkmaktadır.[234]

Rus siber korsanların gerçekleştirdiği siber saldırıları, uluslararası kamuoyu oluşturmak ve Gürcistan hükümetini zayıflatmak şeklinde iki ana saikte ayırarak incelemek, olayların seyrini gösterebilmek adına daha uygun olacaktır. İlk amaç, uluslararası arenada Rusya'nın Gürcistan hükümetinin azınlıklara karşı baskı politikası uyguladığı propagandasını yayması suretiyle Gürcistan'ın imajını zedelemek ve kendi rolünü bir kurtarıcı olarak sunmak şeklinde tezahür etmiştir. Bu çerçevede, Rusya'nın Gürcistan'da azınlıkların haklarının ihlal edildiği iddialarını vurgulayarak kendini olumlu bir şekilde konumlandırmaya çalıştığı görülmüştür. Rusya'nın amacı, kurtarıcı nitelikte ve insan haklarına saygılı bir aktör olarak uluslararası hukuk bağlamında kendini savunmaktır. Kamuoyu uhdesinde bu bilgilerin doğru olduğunu düşündürmek için büyük bir internet ve yanlış bilgi trafiği oluşturulmuştur.[235]

Örneğin, Gürcistan'ın eski liderlerinden Saakashvili'nin Nazi lideri Adolf Hitler ile karşılaştırılmasına yönelik propaganda faaliyetleri dikkat çekicidir. Ancak, söz konusu propaganda faaliyetlerinin geniş ölçüde ifade özgürlüğünün bir yansıması olarak değerlendirilmesi de mümkündür. Uluslararası alanda ifade özgürlüğü, çeşitli görüş ve düşüncelerin serbestçe ifade edilebilmesi için önemli bir unsurdur. Bu tür propaganda ve retoriklerin, uluslararası toplumda farklı tepkilere neden olsa da, ifade özgürlüğünün korunması adına dikkatli bir değerlendirme ile ele alınması gerekmektedir.[236] Siber uzayda gerçekleşen bu tür faaliyetlerin, dijital alandaki ifade özgürlüğünü kısıtlamaması ve demokratik değerlere zarar vermemesi önem arz etmektedir. Ancak unutmamak gerekir ki, bu durumların hukuki ve etik sınırlar içinde kalması, diğer ülkelerin iç işlerine müdahale edecek nitelikte olmaması da önemli bir husustur.

Diğer taraftan, Rus siber korsanların Gürcistan hükümetini zayıflatmak için giriştiği faaliyetler ise ikinci amaç olarak karşımıza çıkmaktadır. Söz konusu faaliyetler ile Gürcistan'daki siyasi ve sosyal yapı istikrarsızlaştırılmak istenmiştir.

---

[234] Karagiannis, s. 7.
[235] Miroslav Mares ve Veronika Netolicka, "Georgia 2008: Conflict Dynamics in the Cyber Domain, **Strategic Analysis,** Cilt:44, 2020, s. 232.
[236] Mares ve Netolicka, s. 233.

Rusya'nın Gürcistan'a yönelik siber saldırıları, Estonya örneğine benzer şekilde ülkenin önemli altyapılarına yönelik DDoS saldırıları ile hükümeti paralize etme ve işlemez hale getirme amacını taşımaktadır. Gürcistan'daki Çatışma Hakkında Uluslararası Soruşturma Komisyonu (Internetional Fact-Finding Commission on Conflict in Georgia*)* tarafından hazırlanan rapora göre, bu siber saldırılardan başlıca önem arz edenler aşağıdaki gibidir:[237]

- 20 Temmuz tarihinde, Devlet Başkanı Saakashvili'nin internet sitesi 24 saat boyunca erişilemez hale getirilmiştir.
- 7 Ağustos tarihinde, Gürcistan'ın birçok sunucusu ve internet trafiği ele geçirilerek dışsal bir kontrol altına alınmıştır.
- 8 Ağustos tarihinde, geniş çaplı bir siber saldırı başlamış ve saldırıların kaynağı belirlenememiştir. Bazı raporlara göre, bu operasyonlar 'Rus İş Ağı (Russian Business Network)' adı verilen bir örgüte atfedilmiştir. Bu süreçte, Gürcistan hükümeti web siteleri, ABD, Birleşik Krallık ve Avrupa üzerinden kullanılamaz hale gelmiştir. Ayrıca, Türk AS9121 TTNet Sunucusu COMSTAR aracılığıyla erişimin engellendiği düşünülmüştür.
- 9 Ağustos tarihinde, Gürcistan Dışişleri Bakanlığı web sitesi siber saldırganlar tarafından ele geçirilmiş ve kışkırtıcı içerikler yayınlanmıştır. Aynı zamanda, İçişleri Bakanlığı, Savunma Bakanlığı ve Gürcistan yanlısı Güney Osetya Geçici İdaresi'nin internet siteleri de diğer siber saldırılarla hedef alınmıştır. Bu dönemde, Gürcistan Ulusal Bankası ve basın/medya siteleri DDoS saldırılarına maruz kalmış ve işlemez hale gelmiştir.
- 12 Ağustos tarihinde, Başkan Saakashvili'nin internet sitesi ve popüler Gürcistan televizyonu Rustavi Tulip Sistemlerine transfer edilmiştir. Tulip Sistemleri de ayrıca saldırıya uğramıştır.
- 12-13 Ağustos tarihlerinde, Savunma Bakanlığı internet sitesi geniş çaplı bir siber saldırıya maruz kalarak iki kez erişilemez hale gelmiştir.

Bu siber saldırılar, Gürcistan hükümetinin, ülkenin altyapısının etkilenmesi yoluyla ciddi bir şekilde zayıflatılmaya çalışıldığını göstermektedir. Bu tür saldırılar, siber güvenlik konusunda uluslararası toplumun dikkatini çekmekte ve devletlerin

[237] **Independent International Fact-Finding Mission on the Conflict in Georgia,** Report, Volume II, 2009, ss. 217-218, https://www.mpil.de/files/pdf4/IIFFMCG_Volume_II1.pdf (03.09.2023).

siber alanda alacakları önlemleri arttırmaları gerektiğini vurgulamaktadır. Siber saldırılar uluslararası ilişkilerde önemli sonuçlar doğurabilecek bir silah haline gelmiştir ve bu tür faaliyetlere karşı etkin tedbirlerin alınması önemlidir.

Saldırıların incelenmesi ve gerekli tahkikatların yapılmasının ardından, saldırılarda kullanılan sitelerin ABD'den çalışan kredi kartları ile Rusya ve Türkiye üzerinden açıldığı ve gereksiz e-postaların sistemi felç etmek amacıyla gönderildiği tespit edilmiştir. Bu tespitler, saldırının karmaşık ve çok yönlü bir yapı içerisinde gerçekleştirildiğini açık bir şekilde göstermektedir.[238]

Gürcistan üzerinde gerçekleşen siber saldırılar ile Estonya'daki yaşanan olaylar arasındaki birtakım benzerlikler bulunmaktadır. Saldırıları organize edenler tarafından Rusça siteler *'StopGeorgia.ru'* ve *'Zakep.ru'* ortaya çıkarılmış, saldırı talimatları ve saldırı araçları bu platformlardan yönlendirilmiştir. DDoS saldırıları ile birlikte fidye yazılımları ve sosyal mühendislik gibi yöntemler de kullanılmıştır. Bu kapsamda saldırıların organize bir yapı tarafından gerçekleştirildiği ve dış müdahalenin olduğu anlaşılmakta ve Rusya istihbarat servislerinin de destek verdiği düşünülmektedir.[239]

Akademik literatürde ve uluslararası arenada siber saldırılar için *'savaşın sisi (fog of war)'* benzetmesi yapılmıştır. Bu kavrama göre, siber saldırılar diğer askeri operasyonları desteklemek ve dikkatleri dağıtmak amacıyla gerçekleştirilmekte; belirsizlik, kaos, düzensizlik, aldatma, yanıltma ve propaganda faktörlerini bir araya getirmektedir. Bu durum siber saldırıların karmaşıklığını ve mahiyeti gereği askeri birimlerin bir parçası olarak değerlendirilmesi gerektiğini ortaya koymaktadır.[240]

Rusya'nın Gürcistan'a yönelik gerçekleştirdiği iddia edilen siber saldırılar, dijital altyapıyı hedef almakla birlikte, aynı zamanda askeri operasyonları desteklemek ve düşmanın dikkatini dağıtmak amacıyla kullanılan karmaşık ve planlı eylemler olarak karşımıza çıkmıştır. Bu tür siber saldırıların, modern anlamda kuvvet kullanma seviyesinde etkiler taşıyabileceği, bu sebeple zamanla daha önemli bir rol oynayacağı

[238] Salih Bıçakçı, "Yeni Savaş ve Siber Güvenlik Arasında NATO'nun Yeniden Doğuşu", **Uluslararası İlişkiler**, Cilt:9, Sayı:34, 2012, s. 218.
[239] Jeffrey Carr, **Inside Cyber Warfare: Mapping the Cyber Underworld**, O'Reilly Media, 2012, s. 205.
[240] Brian L. Steed, **Piercing the Fog of War: Recognizing Change on the Battlefield: Lessons from Military History 216 BC through Today**, Zenith Press, Mineneapolis, 2009, s. 222.

ve uluslararası toplumda bu tür eylemler nezdinde gerekli tedbirlerin alınması gerektiği aşikârdır.

Gürcistan örneğinde yaşananları, ABD ve Birleşik Krallık'ın ortaklaşa yürüttüğü 2003 Irak Operasyonu kapsamında kullanılan taktikler ile karşılaştırmak, siber saldırıların hibrit saldırılar içindeki konumunu daha iyi değerlendirmek için aydınlatıcı olacaktır. Kısaca ifade etmek gerekirse; 2003 yılındaki Irak Operasyonunda, ABD Irak'ın askeri iletişim sistemlerine sızmış ve Pentagon tarafından hazırlanan bazı mesajlar, Irak subaylarına gönderilmiştir. Söz konusu mesajlarda, ABD'nin Irak'a karşı büyük bir kuvvetle saldırıya geçtiği ve amaçlarının Irak halkının Saddam Hüseyin ve iki oğlundan kurtulmasını sağlamak olduğu ifade edilmiştir.[241] Bu minvalde siber saldırılar, modern savaşın bir parçası olarak askeri iletişim sistemlerine doğrudan müdahale etme yeteneği sağlamakta ve düşmanın algısını etkileme gücü taşımaktadır. Siber saldılar geleneksel saldırıları yönlendirebileceği gibi, psikolojik etkilemelere de aracılık edebilecektir. Bu, savaşın sadece fiziksel alanında değil, aynı zamanda siber alanda da kazanılmaya çalışıldığını ve psikolojik olarak da üstünlük kurmanın önemli olduğunu göstermektedir. Günümüzde siber saldırılar ve siber güvenlik, devletlerin stratejilerinde önemli bir bileşen haline gelmektedir.

Son olarak, Rusya ve Gürcistan gerginliğinin Schmitt Analizi kapsamında uluslararası hukukta nasıl değerlendirildiğini incelemek konumuz açısından gerekli ve yararlı olacaktır. Schmitt Analiziyle ele alındığında, Gürcistan'a yönelik siber saldırılar önemli hukuki ve siyasi boyutları olan bir mesele olarak değerlendirilebilecektir. Saldırıların yoğunluğu ve etkileri göz önüne alındığında, devlet kurumlarının uzun süreli kapanmasına, özellikle medya ve bankacılık faaliyetlerinin uzun bir süre boyunca durmasına neden olmasının ciddi zararlara yol açtığını ortaya koymaktadır. Ayrıca uluslararası hukukun temel ilkelerinden biri olan egemenliğin de ihlal edildiği değerlendirilmektedir.

Egemenlik, bir devletin iç ve dış stratejilerini belirleme ve çeşitli etkenlere karşı müdahale etme yetkisini içerir. Siber saldırıların Gürcistan'a yönelik etkisi, devletin iç işlerine ve ekonomisine yönelik tehdit oluşturduğu için egemenlik ilkesini

[241] Richard A. Clarke ve Robert K. Kanke**, Siber Savaş (Cyber War)**, (Çev. Murat Erduran), İstanbul Kültür Üniversitesi Yayınları, 2011, s. 8.

ihlal etmiştir. Devletin en önemli görevlerinden biri, vatandaşlarının güvenliğini ve refahını sağlamak olduğundan, bu tür bir saldırı, devletin esas işlevlerini yerine getirmesini engelleyerek vatandaşlar nezdinde de huzursuzluğa sebep olmuştur. Bu sebeple egemenlik ilkesinin ihlal edildiği ve uluslararası sorumluluk hukuku kapsamında ayrıca değerlendirilmesi gerektiği aşikârdır.

Siber saldırılar anlık olarak ve hızlı bir şekilde gerçekleşmiş, Gürcistan'a doğrudan zarar vermiştir. Ayrıca, bu saldırıların Rusya-Gürcistan Savaşının patlak vermesi ile aynı döneme denk gelmiş olması, Rusya'nın bu saldırılardan kendisinin sorumlu olduğunu reddetse bile, Rusya Federasyonu veya bizzat yönlendirdiği gruplar tarafından gerçekleştirildiği iddiasını güçlendirmektedir. Ayrıca, Gürcistan'daki Çatışma Hakkında Uluslararası Soruşturma Komisyonu'nun tespitlerine göre, bu saldırılara Rus istihbarat servislerinin de dahil olduğu iddiaları unutulmamalıdır.[242]

Saldırının temel hedeflerinden biri, Gürcistan'ın medyasını ve bankalarını işlemez hale getirmek olsa dahi, dönemsel olarak ülke nüfusunun internet erişimine sınırlı bir şekilde sahip olması, Gürcistan'ın bu saldırılardan Estonya örneğine nazaran daha az etkilenmesine sebep olmuştur.[243] Bu sebeple saldırıların uluslararası hukuktaki yansımaları da büyük örnekler karşında daha hafif kalmış ve kuvvet kullanma eylemleri içinde geleneksel saldırıların hazırlık aşamalarından biri olarak görülmüştür. Söz konusu olayların kuvvet kullanma yoğunluk ve seviyesinde olmadığı düşünülse dahi, geleneksel yöntemlerle birlikte değerlendirildiğinde iç işlere karışmama ilkesi ve müdahale yasağını ihlal edecek nitelikte olduğunun altı çizilmelidir.[244]

Gürcistan'a yönelik icra edilen siber saldırıların en önemli özelliği, tarihteki sıcak bir çatışmayı destekleyici nitelikte rol üstlenen ilk siber uzay eylemi olmasıdır. Bu durum, siber saldırıların modern anlamda hibrit saldırıların parçası olarak kullanıldığının öncü bir örneği olarak kabul edilmekle birlikte, Gürcistan ve Rusya arasındaki gerginliğin, geleneksel savaş başlamadan önce siber saldırıların kullanıldığı ilk vaka olarak tarihe geçtiği de ifade edilmektedir.[245]

---

[242] Kara, s. 49.

[243] Eneken Tikk, Kadri Kaska ve Liis Vihul, **International Cyber Incidents: Legal Considerations**, Cooperative Cyber Defense Centre of Excellence, Tallinn, 2010, ss. 73-74.

[244] Mehmet Yayla, "Uluslararası Hukukta Siber Saldırılara Karşı Kuvvet Kullanma", **Türkiye Barolar Birliği Dergisi**, Sayı:107, 2013, s. 206.

[245] Günay Süleymanova Rafael, **A Comparative Analysis of Major Russian Cyber Attacks in the Post-Cold War Era**, (Yayınlanmamış Yüksek Lisans Tezi), Bahçeşehir Üniversitesi Lisansüstü Eğitim Enstitüsü, İstanbul, 2022, ss. 52-53 ve Güven, s. 299.

Nihayetinde siber saldırılar, münferit olduğu kadar geleneksel askeri operasyonların bir ön parçası olarak da giderek önemini artırmakta, uluslararası hukuk ve siber güvenlik konularında daha fazla tartışmayı gündeme getirmektedir. Önemle belirtmek gerekir ki; siber saldırıların sınırlarını belirlemek güçtür. Uluslararası toplumun modern savaşın yeni yönlerini temsil eden bu tür olaylara nasıl tepki vereceği ve siber saldırıların engellenmesi hususlarında düşünme ihtiyacı doğmaktadır.

C. Baskı Amaçlı Siber Saldırılar: Abd-Sony-Kuzey Kore Üçgeni (2014)

2014 yılında, ABD merkezli Sony Pictures Entertainment şirketine yönelik düzenlenen siber saldırılar, o dönemde dünyada yankı uyandırmış ve uluslararası kamuoyunun gündemine oturmuştur. Teknoloji devi Sony'nin söz konusu saldırılara karşı etkili önlemler alamaması sonucunda bilgisayar sistemleri ele geçirilerek şirkete ait gizli belgeler ve e-postalar sızdırılmıştır. Bu durum önemli bir siber güvenlik başarısızlığı olarak kayda geçmiştir.

Gerginlik ve sorunların başlangıcı, ilginç şekilde bir sinema filmi olarak karşımıza çıkmaktadır. ABD'nin yakın tarihli sinema kültürü, ABD'ye ve genel olarak ABD kültürüne uzak devletlere eleştirel bir bakış açısı sunmayı amaçlayan filmleri içermekte ve ekseriyetle devletlere yönelik bazı alaycı tavırları da sinema üzerinden izleyiciye yansıtmaktadır. Sony'e yönelik siber saldırılar, Kuzey Kore lideri Kim Jong-il'in ölümünün ardından iktidara gelen Kim Jong-un hakkında hazırlanan *'Röportaj (The Interview)'* isimli komedi filmi sebebiyle ortaya çıkmıştır.[246]

Film, 11 Haziran 2014 tarihinde YouTube ve benzeri sosyal medya platformlarında tanıtılmıştır. Filmin konusu ise, bir söyleşi programı sunucusunun CIA tarafından işe alınması, yeni Kuzey Kore lideri ile röportaj yapma bahanesiyle Kuzey Kore'ye gitmesi ve ona suikast düzenlemesidir. Bu film, Kim Jong-un'un politikacı ve devlet başkanı kimliğini hedef alması nedeniyle Kuzey Kore tarafından tepkiyle karşılanmış; Kuzey Kore hükümeti, bu filmin yapımının durdurulmasını talep etmiştir. Nitekim söz konusu film, Kuzey Kore tarafından *'devlet'* olarak kendilerine yapılmış

[246] Stephan Haggard ve Jon R. Lindsay, "North Korea and the Sony Hack: Exporting Instability Through Cyberspace", **Asia Pacific Issues**, Sayı:117, 2015, s. 2.

bir saldırı olarak addedilmiş ve uluslararası alanda derhal ve şiddetle kınanmıştır.[247] Bununla birlikte, filmin tanıtımından yaklaşık iki hafta sonra Kuzey Kore'nin BM temsilcisi Ja Song-nam tarafından BM Genel Sekreteri Ban Ki-moon'a bir mektup yazılmıştır. Mektupta yer alan ifadeler şu şekildedir:[248]

> *Egemen bir devletin, görevdeki devlet başkanı hakkında suikasti konu alan böyle bir filmin yapımına ve dağıtımına izin verilmesi, bir savaş eylemi olduğu kadar, terörizme de en açık şekilde sponsorluk olarak görülmektedir. ABD yetkilileri derhal uygun önlemleri almalıdır, aksi takdirde terörizmi teşvik etmek ve desteklemekten tamamen sorumlu olacaktır.*

ABD'nin Şükran Bayramı tatilinden hemen önceki haftada, Sony'nin yöneticileri, *'God'sApstls'* adını taşıyan bir grup tarafından gönderilen ve siyasi talepler içeren bir e-posta almıştır. Birkaç gün sonra ise Sony çalışanlarının bilgisayarlarının siber saldırıya uğradığı tespit edilmiştir. Söz konusu saldırı, Sony şirketinin siber güvenlik açıklarını gözler önüne sermiş ve aynı zamanda organize bir suç eylemi olarak kaydedilmiştir. Çalışanlar, bilgisayarlarında rahatsız edici görüntüler, tehdit içeren mesajlar ve bazı bağlantılar bulmuştur. Bağlantıların, Sony'nin şirket verileri içerisinden alındığı iddia edilen bazı dosyaların listeleri olduğu görülmüştür. Bu durum, saldırının siber uzayda zarar vermekle sınırlı kalmadığını, aynı zamanda şirket içi veri sızdırma faaliyeti olduğunu açıkça ortaya koymuştur. Kendilerine *'Barışın Koruyucuları (Guardians of Peace - GoP's)'* adını veren siyah şapkalı bilgisayar korsanları, Sony'nin gizli, hassas ve korunduğu iddia edilen içeriklerini ele geçirmiştir.[249]

Saldırı, Sony'nin siber güvenlik açıklarını da gün yüzüne çıkarmıştır. Şirket, iç güvenliği ile ilgili olarak bu olayı soruşturmak üzere deneyimli bir siber güvenlik uzmanı olan Kevin Mandia'yı görevlendirmiştir. Mandia tarafından saldırı, dikkat çekici bir şekilde planlanmış ve organize edilmiş bir suç olarak ifade edilmiştir. Sony ve benzeri şirketlerin bu kapsamdaki bir atağa hazırlıklı olmadığı öne sürülmüştür.[250]

---

[247] Clare Sullivan, "The 2014 Sony Hack and the Role of International Law", **Journal of National Security Law & Policy**, Sayı:8, 2016, ss. 437-438.

[248] United Nations General Assembly Security Council, **Letter dated 27 June 2014 from the Permanent Representative of the Democratic People's Republic of Korea to the United Nations addressed to the Secretary-General**, A/68/934–S/2014/451, 2014.

[249] Sullivan, s. 439.

[250] Antonio DeSimone ve Nicholas Horton, **Sony's Nightmare Before Christmas: The 2014 North Korean Cyber Attack on Sony and Lessons for US Government Actions in Cyberspace**, The Johns Hopkins University Applied Physics Laboratory LLC, Laurel, 2017, s. 5.

Federal Soruşturma Bürosu (Federal Bureau of Investigation - FBI) tarafından saldırı sonrasında yapılan açıklamalarda, cereyan eden olayların terör eylemi niteliğinde olmadığına dair ifadeler bulunmakla birlikte, film gösterimi sürecinin olumsuz anlamda etkilendiği ve sekteye uğradığı bilgisi yer almaktadır.[251] Buradan hareketle, büyük bir şirketin iş planlarını baskı ve korkutma yoluyla değiştiren bir siber saldırının ilk kez gerçekleştiği görülmektedir.

Kuzey Kore yetkililerinin olaylara ilişkin açıklamalarında, siber saldırı ile ilgili herhangi bir sorumluluk ve etkilerinin bulunmadığı belirtilmektedir. Ancak 19 Aralık 2014'te FBI tarafından yapılan bir basın açıklamasında, Kuzey Kore'nin Sony'ye yönelik saldırısının ABD'nin ulusal güvenliğine yönelik en derin siber tehditlerden biri olduğunun bir kez daha doğrulandığı vurgulanmaktadır. FBI tarafından yapılan açıklamanın önemli kesitleri şu şekildedir:[252]

> *Araştırmamızın bir sonucu olarak ve ABD hükümetinin diğer bölüm ve kurumlarıyla yakın işbirliği içinde, FBI artık bu eylemlerden Kuzey Kore hükümetinin sorumlu olduğu sonucuna varmak için yeterli bilgiye sahiptir. Hassas kaynakları ve yöntemleri koruma ihtiyacı, tüm bu bilgileri paylaşmamızı engellese de, vardığımız sonuç kısmen aşağıdakilere dayanmaktadır:*
> *Bu saldırıda kullanılan veri silme kötü amaçlı yazılımının teknik analizi, FBI'ın Kuzey Koreli aktörlerin daha önce geliştirdiğini bildiği diğer kötü amaçlı yazılımlarla bağlantıları ortaya çıkarmıştır. Örneğin belirli kod satırlarında, şifreleme algoritmalarında, veri silme yöntemlerinde ve ele geçirilen ağlarda benzerlikler vardır.*
> *FBI ayrıca bu saldırıda kullanılan altyapı ile ABD hükümetinin daha önce doğrudan Kuzey Kore ile ilişkilendirdiği diğer kötü amaçlı siber faaliyetler arasında önemli bir örtüşme olduğunu da gözlemlemiştir. Örneğin FBI, bilinen Kuzey Kore altyapısıyla ilişkili çeşitli İnternet Protokolü (IP) adreslerinin, bu saldırıda kullanılan veri silme kötü amaçlı yazılımına sabit kodlanmış IP adresleriyle iletişim kurduğunu keşfetmiştir.*
> *Ayrı olarak, Sony Pictures Entertainment saldırısında kullanılan araçlar, geçen yıl Mart ayında Kuzey Kore tarafından Güney Kore bankaları ve medya kuruluşlarına yönelik gerçekleştirildiği iddia edilen siber saldırıyla benzerlik taşımaktadır.*

ABD menşeli siber güvenlik şirketlerinin bağımsız olarak yürüttüğü araştırmalar da saldırının Kuzey Kore hükümeti tarafından gerçekleştirildiği sonucuna ulaşmıştır. Ancak bu sonuçların spesifik ve kesin delillere dayanmadığı, genel çıkarımlar üzerine inşa edildiği anlaşılmakta, bu sebeple Kuzey Kore'ye isnadiyeti

---

[251] Haggard ve Lindsay, s. 2.
[252] FBI National Press Office, **Update on Sony Investigation**, 2014, https://www.fbi.gov/news/press-releases/update-on-sony-investigation (08.09.2023).

mümkün görünmemektedir.[253] Yaşanan gelişmelere paralel olarak aynı gün içinde, Dönemin ABD Başkanı Barack Obama, saldırının Kuzey Kore tarafından gerçekleştirildiğini ve büyük zarara yol açtığını açıklamış ve *"Biz buna cevap vereceğiz. Biz buna misliyle cevap vereceğiz ve bunu kendi seçtiğimiz bir zamanda, kendi seçtiğimiz bir yerde ve kendi seçtiğimiz bir şekilde yapacağız."* şeklindeki açıklamalarıyla duruma noktayı koymuştur.[254] Siber saldırılarda ismi geçen GoP adlı grup ise bu süreçte derhal dağılmıştır.

İki devlet arasındaki gerginlikler ve siber saldırıların ardından, Sony ve Sony'de çalışan kilit isimler, tartışmalı filmle ilgili endişeler taşımaya başlamıştır. Özellikle, Sony Şirketi'nin baş idarecisi Kazuo Hirai, film gösterime girmeden önce Sony'nin üst düzey yöneticisine yönelik gönderdiği bir e-postada bu endişelerini dile getirmiştir. Hirai'nin ifadelerinde filmle ilgili duyulan rahatsızlık açıkça belli edilmiştir. Yaşanan yeni gelişmeler sonucunda, filmde önemli değişiklikler yapılmış ve Kim Jong-un'un ölüm sahnesi gibi kışkırtıcı sayılabilecek içerikler filmden çıkarılmıştır.[255] Nihayetinde filmin, 25 Aralık 2014 tarihinde gösterime girmesi kararı alınmıştır.

Şirket tarafından filmin gösterime girmesi kararı alınmış olmasına rağmen, siber saldırı ve tehditlerin devam etmemesi, dikkate değer bir husustur. Ancak bu durumun, saldırganların gerçekleştirdikleri eylemlerin arzu ettikleri sonuca ulaştığının bir göstergesi olarak yorumlanabilecektir. Söz konusu eylemler, uluslararası hukukta bir devlet tarafından siber saldırıların baskı unsuru olarak kullanıldığına ilişkin tarihteki nadir örneklerden biri olarak karşımıza çıkmaktadır. ABD hükümetinin kendi özel şirketlerinin çıkarlarını açıkça ve kamusal olarak savunma iradesini göstermesi ise bu olayın önemini net bir biçimde ortaya koymaktadır.[256]

Farklı bir açıdan, Kuzey Kore'nin sorumluluğunu ve yönlendirici rolünü somut olarak kanıtlayacak herhangi bir delil sunulamamış olması, olayın vahametini gözler önüne sermektedir. Nitekim North Korea Tech'te görev alan ve teknoloji üzerine çalışmalar yürüten Martyn Williams, FBI'ın açıklamalarında tutarsızlıklar bulunduğunu, Kuzey Kore tarafından kullanılan siber saldırı teknik ve yöntemlerinin

[253] DeSimone ve Horton, s. 9.
[254] Haggard ve Lindsay, ss. 2-3.
[255] Sullivan, s. 437.
[256] Haggard ve Lindsay, s. 3.

mantığı düşünüldüğünde, *'Kuzey Kore usullerinin asla bu yöntemleri içermediğini'* ifade etmiş ve saldırıların Kuzey Kore hükümetiyle bağlantılı olmasının gerçek olamayacak kadar iyi bir ihtimal olduğunu farklı argümanlarla destekleyerek değerlendirmiştir.[257]

Schmitt, Birleşmiş Milletler Antlaşması'nın m. 2 ve 51 hükümleri ve uluslararası teamül hukuku uyarınca, Sony'ye yönelik kötü niyetli siber faaliyetleri ayrıntılı bir şekilde değerlendirmiştir. Bu kapsamda Schmitt'in tespitleri şu şekilde özetlenebilecektir:[258]

- Sony'ye yönelik siber saldırıların içeriği, öncelikle çalışanların tehdit edilmesi, hassas bilgilerin ifşa edilmesi ve verilerin yok edilmesi şeklinde tezahür etmiş, bazı durumlarda veri kaybı, etkilenen bilgisayarların düzgün şekilde yeniden başlatılmasını dahi engellemiştir. Buna rağmen, Sony'ye karşı gerçekleştirilmiş olan siber saldırılar 'silahlı saldırı' düzeyine çıkan bir 'kuvvet kullanımı' niteliğinde değildir. Her ne kadar son derece yıkıcı ve maliyetli olsa da bu minvaldeki etkiler, uzmanların silahlı saldırı olarak değerlendireceği düzeyde görülmemiştir.
- Bazı görüşler, meşru müdafaa hakkının devlet dışı aktörlerin saldırılarını da kapsadığı görüşünü reddetmektedir. Her ne kadar Sony olaylarında Kuzey Kore'nin rolü sorgulansa da bu tartışmanın bir önemi bulunmamaktadır. Nitekim söz konusu saldırılar siyah şapkalı bilgisayar korsanları tarafından gerçekleştirilmekte ve ilk etapta silahlı saldırı olarak nitelendirilememektedir.
- Kuvvet kullanma eşiği belirsizliğini korusa bile uluslararası toplumun Sony'ye yönelik saldırılar hakkındaki görüşler çoğunlukla müdahale yasağı ve egemenlik ilkesinin ihlali üzerine yoğunlaşmıştır. Kısaca belirtmek gerekirse, Sony'ye yönelik operasyonun ABD'ye yönelik hukuka aykırı bir 'müdahale' teşkil etmediği düşünülmektedir. Özel bir şirketin faaliyetlerini aksatmak, başka bir devletin hâkimiyet alanına izinsiz girilmesi ve dolayısıyla müdahale yasağına aykırı davranılması sonucunu doğuran eylemlerden değildir.

[257] Martyn Williams, "Analysis: Why North Korea might not be to blame for the Sony Pictures hack", **The Guardian**, https://www.theguardian.com/world/2014/dec/02/-sp-north-korea-hack-sony (08.09.2023).

[258] Michael Schmitt, "International Law and Cyber Attacks: Sony v. North Korea", **Just Security**, 2014, https://www.justsecurity.org/18460/international-humanitarian-law-cyber-attacks-sony-v-north-korea/ (08.09.2023).

Sony'nin karşılaşmış olduğu durum ise müdahale yasağının çerçevesinden son derece uzaktır.

- Mevcut durumda, Sony olaylarının ABD'nin egemenliğinin ihlali olarak nitelendirilmesi çok daha savunulabilir bir argüman olarak karşımıza çıkmaktadır. Egemenliğin ihlalinin oluşabilmesi için, bir eylemin bir devlete atfedilebilir olması gerekir. Saldırıyı gerçekleştiren GoP grubunun Kuzey Kore etkisi ve yönlendirmesi altında hareket ettiği ispat edildiği yahut söz konusu devlet tarafından bizzat kabul edildiği takdirde, sorumluluk Kuzey Kore'ye atfedilebilecek ve Kuzey Kore'nin egemenlik ilkesini ihlali hususun tartışılabilecektir. Bu durumda Sony'nin özel bir şirket olmasının da hiçbir önemi bulunmamaktadır. Zira söz konusu siber altyapı ABD topraklarında yer alarak ABD egemenliği sınırları içerinde faaliyet göstermektedir.
- Konuyla ilgili henüz fikir birliğine varılamamasına rağmen, bir devletin başka bir devletin topraklarındaki siber altyapıyı manipüle etmesini veya orada bulunan sistemlere kötü amaçlı yazılım yerleştirmesini içeren bir siber operasyonu, bu devletin egemenliğinin ihlali olarak nitelendirmek makul görünmektedir. Hal böyleyken, Sony'ye yönelik siber saldırının Kuzey Kore'ye atfedilebilmesi mümkün olursa, Kuzey Kore ABD egemenliğini ihlal etmiş olacaktır. Ayrıca söz konusu durum, uluslararası sorumluluk hukuku kapsamında değerlendirilecek ve 'uluslararası hukuka aykırı eylem' kapsamında yaptırımların ve karşı önlemlerin gündeme gelmesine sebep olacaktır. Saldırıların hukuki açıdan Kuzey Kore'ye atfedilemez olması halinde, Kuzey Kore için kendi ulusal sınırları içerisindeki bir faaliyetin diğer devletlere zarar vermemesi hususunda özen yükümlülüğünün ihlali sebebiyle yaptırımlar ve karşı önlemler gündeme gelebilecektir.

Somut olay nazarında Kuzey Kore'nin sorumluluğunun kanıtlanamaması, uluslararası ilişkilerde bu tür saldırıların nasıl ele alınması gerektiğine ilişkin çeşitli perspektiflerden tartışmaların ortaya çıkmasına sebep olmuştur. Saldırı, Sony'nin iş planlarını değiştiren farklı bir örnek olarak kaydedilse de mağdur olan taraf bir devlet olmadığı için müdahale yasağına aykırılık teşkil etmemektedir. Ancak saldırının Kuzey Kore'ye isnadiyeti mümkün olursa, egemenlik ilkesinin ihlaline dair tartışmalar gündeme gelebilecektir.

Nihayetinde belirtmek gerekir ki; uluslararası hukuk, kötü niyetli siber operasyonlar karşısında geniş bir yelpazedeki olası yanıt seçeneklerini kabul etmektedir. Devletlerin bu olasılıkları göz önünde bulundurarak eylemlerine yön vermesi ve uluslararası toplum barışını bozacak davranışlardan kaçınması gerekmektedir. Nitekim devletlere atfedilebilen uluslararası hukuka aykırı tüm eylemlerin uluslararası hukukta sonuçları olacaktır. Ayrıca bahsi geçen eylemler bakımından, yargı yetkisinin devreye girmesiyle birlikte iç hukuk kapsamında yasal önlemlerin alınabileceği de unutulmamalıdır. Siber saldırılara karışanlar, bilgisayar korsanlığı, ekonomik casusluk ve diğer suçlarla suçlanarak mağdur devletin hukukuna göre kovuşturma riskiyle karşı karşıya kalacaktır.

II. KUVVET KULLANMA YASAĞI VE MEŞRU MÜDAFAAYA İLİŞKİN ÖRNEKLER

A. Siber Saldırıların Desteği: Suriye-İsrail Orchard Operasyonu (2007)

2007 yılında Suriye, Kuzey Kore ile gizli bir işbirliği içerisinde, İsrail devleti için endişe uyandıracak bir nükleer tesis inşaatı üzerinde çalışmaktadır. Bu tesis, Al-Kibar adıyla bilinmekte ve Suriye'nin Deyr El Zour bölgesinde konumlanmaktadır. Tesisin, nükleer silah üretme kapasitesine sahip olabileceği yönünde ciddi iddialar mevcuttur. İddiaların temel dayanağı, İsrail İstihbarat Servisi Mossad'ın elde ettiği gizli belgelerdir. Suriyeli bir devlet yetkilisinin dizüstü bilgisayarı üzerinden *'Truva Atı'* adı verilen gelişmiş bir siber casusluk yazılımı kullanılarak elde edilen bu belgeler, tesisin *'yüksek derecede hassas'* olarak sınıflandırıldığını göstermektedir. Bununla birlikte, elde edilen verilerin içerisindeki fotoğraflar ve inşaat planlarından da nükleer silah üretimine yönelik bulgular tespit edilmiştir.[259]

Eylül ayında, Al-Kibar isimli bu tesis, henüz inşaat aşamasındayken bir bombalama sonucu patlamış ve tamamen yok olmuştur. Bu patlamanın doğrudan İsrail Hava Kuvvetleri tarafından gerçekleştirilen bir saldırı olduğu yönünde kuvvetli emareler bulunmaktadır. Şüpheli nükleer tesise yönelik saldırıyı gerçekleştirmeden önce, İsrail'in Türkiye-Suriye sınırı yakınlarında bulunan Tel Abyad bölgesine

[259] Warren Bass, **A Surprise Out of Zion?**, RAND Corporation, Santa Monica, 2015, s. 47.

yaklaşarak bir elektronik saldırı gerçekleştirdiği iddia edilmektedir. Bu saldırının bir güdümlü füze aracılığıyla icra edildiği düşünülmektedir. Söz konusu saldırının Suriye radar sistemini geçici olarak devre dışı bıraktığı ve böylece İsrail Hava Kuvvetleri'ne ait uçakların Suriye hava sahasına girişini tespit etmesinin engellendiği belirtilmektedir.[260] Siber saldırılarda sıklıkla karşımıza çıkan bu teknikler, savunma sistemlerinin etkisiz hale getirilmesi amacıyla kullanılmakta ve süreç içinde etkin rol oynamaktadır.

Suriye saldırıyı inkâr etse de, saldırıdan sonra ortaya çıkan fotoğraflarla tesisin grafit soğutmalı bir reaktör, yani gizli bir nükleer yapı olduğu açığa çıkmıştır. Bu reaktörün Kuzey Kore'deki plütonyum üretiminde kullanılan Yongbyon reaktörüyle neredeyse aynı olduğu anlaşılmıştır.[261] İsrail başlangıçta saldırının kendisi tarafından gerçekleştirildiğini reddetmiş olsa da elde edilen bazı veriler, operasyonun güçlü bir sinyal karıştırma (jamming) teknolojisi kullanılarak icra edildiğini ortaya koymaktadır.[262]

Suriye kamuoyunda önemli bir etki ve infial yaratmasına rağmen, devletler tarafından konuyla ilgili detaylı bir açıklama yapılmamıştır. Bu olay, bölgedeki siyasi gerilimleri ve güvenlik endişelerini daha da artırmıştır. Suriye'nin nükleer programının şeffaflığına dair uluslararası tartışmalar ve spekülasyonlar yaşanmış, İsrail-Suriye ilişkileri gerginleşmiştir. Gizli bir tesisin tam olarak ne amaçla inşa edildiği ve ne kadar ilerlemiş olduğu konusunda resmi açıklamalar yapılmamış olması, tartışmaları da beraberinde getirmiştir.

Nihayetinde, saldırıdan yaklaşık 11 yıl sonra, 21 Mart 2018 tarihinde, İsrail Savunma Bakanı Avigdor Liberman resmi olarak bu operasyonun sorumluluğunu üstlenmiştir. Bakan Libarman'ın üzülerek ve utanç verici olduğunu belirterek yaptığı açıklamaların yanında, İsrail hükümetinin Suriye'deki nükleer reaktörü imha etme yönündeki cesur duruşu ve başarılı operasyonunun hafife alınmaması gerektiği, İsrail'in varlığını tehdit eden ülkelere asla nükleer silah izni vermeyeceği de ayrıca

[260] Christopher Whyte ve Brian Mazanec, **Understanding Cyber Warfare: Politics, Policy and Strategy**, Routledge, New York, 2018, s. 109.
[261] Lior Tabansky ve Isaac Ben Israel, **Cybersecurity in Israel**, Springer, Switzerland, 2015, s. 65.
[262] John Markoff, "A Silent Attack but Not a Subtle One", **The New York Times,** 2010, https://www.nytimes.com/2010/09/27/technology/27virus.html (28.12.2022).

vurgulanmıştır.[263] Ancak önemle belirtmek gerekir ki, bu durumu kuvvet kullanma ve meşru müdafaa kavramlarıyla birlikte değerlendirmek gerekecektir. Kanımızca, somut olay kuvvet kullanma yasağının ihlali konusunda açık bir örnek olup, üzerinden uzun bir süre geçtiği için, saldırı ile meşru müdafaa hakkının kullanılması arasındaki zamansal yakınlık kriteri sağlanamayacak ve mağdur devletin meşru müdafaa hakkı bulunmayacaktır. Yine de bu tarz durumların diplomatik ilişkileri zedeleyebileceği ve uluslararası toplumda sorunlara yol açabileceği göz ardı edilmemelidir.

Orchard ve benzeri siber saldırılar, uluslararası hukuktaki değerlendirmeler açısından son derece önemlidir. Bu operasyonda İsrail tarafından geleneksel ve siber saldırı teknikleri bir arada kullanılmıştır. Söz konusu operasyon, devletler tarafından gerçekleştirilen siber saldırıların fiziki olarak yıkıcı etkileri olabileceğini gözler önüne seren ilk örneklerden biridir. İsrail'in stratejik güvenlik anlayışı çerçevesinde, Suriye, İran gibi ülkelerin nükleer silah gücünü elde etmesini engellemek ve ulusal güvenliği korumak amacıyla siber saldırılardan yararlanılmıştır.

Orchard Operasyonu aynı zamanda siber saldırıların devletler için stratejik bir avantaj sağladığını ortaya koymuştur. Siber saldırılar, savunma mekanizmalarını zayıflatarak fiziksel saldırıların etkinliğini artırabilir ve hatta bazı durumlarda fiziksel saldırıları tamamen önleyebilir. Bu durum siber saldırıların, devletlerin stratejik hedeflerini gerçekleştirme ve ulusal güvenliklerini sağlama konularında önemli bir araç olduğunu göstermektedir. Dolayısıyla, gelecekte siber saldırı yetenekleri, devletlerin askeri stratejilerinde merkezi bir rol oynayabilecektir.

B. Siber Saldırılarda Fiziksel Zarar Tartışmaları: Stuxnet (2014)

İran, geçmişten günümüze nükleer çalışmalardaki girişimleri ile karşımıza çıkmıştır. 2010 yılında İran'ın Natanz şehrinde bulunan nükleer tesisleri, yoğun etkili bir şekilde geliştirilmiş Stuxnet virüsü yoluyla siber saldırıya maruz kalmış ve İran, başlangıçta saldırıya uğradığını reddetse de, ciddi büyüklükte fiziksel zararla karşı

[263] Anna Ahronheim, "Liberman: Squabbling over credit for strike on Syrian reactor an 'embarrassment'", **The Jerusalem Post,** https://www.jpost.com/Israel-News/Liberman-praises-Israels-strike-on-Syrian-reactor-Livni-recalls-events-546640 (02.07.2023).

karşıya kaldığını açıklamıştır.[264] Söz konusu virüs, uluslararası hukukun temel ilkeleri bağlamında, bilgisayar ağ saldırıları için bir dönüm noktası olarak kabul edilmiş ve halen önemini koruyan birçok tartışmayı beraberinde getirmiştir.

İlk aşamada Stuxnet, 2010 yılının Haziran ayında Belarus'un Minsk şehrinde bulunan *'VirusBlokAda'* adlı bir anti-virüs şirketinde analist olarak çalışan Sergey Ulasen tarafından keşfedilerek karşımıza çıkmaktadır.[265] Sonrasında Stuxnet'in Alman menşeili Siemens şirketi tarafından endüstriyel sistem kontrolü taramasında tespit edildiği, Merkezi Denetleme ve Veri Toplama Sistemi *(Supervisory Control and Data Acquisition - SCADA)* için bu virüse karşı savunmasız kalındığı ifade edilerek müşterilerin uyarıldığı görülmektedir. Hedef aldığı tüm sistemi kontrol etme gücüne sahip olan bu virüs, küçük hafızalı bir taşınabilir bellek aracılığıyla aktarımı sağlanarak Windows işletim sistemlerinin güvenlik açıklarından faydalanabilmekte; yerel alan ağlarının içinde yayılarak casusluk ve sabotaj amacıyla da kullanılabilmektedir.[266]

Somut olayda Stuxnet virüsü, hedef aldığı yazılım programı içinde, nükleer tesiste bulunan SCADA sistemi gibi, bir denetim ve veri sağlama aracı olarak hareket etmiş ve sisteme entegre olduğu anda uzaktaki bir sunucuyla iletişim kurarak uzaktan kontrol edilebilir hale gelmiştir. İlk aşamada kötü amaçlı herhangi bir faaliyet başlatmadan ve kendini gizleyerek hareket eden virüs, çalışma döngüsü içerisinde normal işlemleri gizlice kaydetmiş, sistemde ve yerel ağa bağlı bilgisayarlarda meşru görünerek yayılma politikası izlemiştir.[267] Hedef sisteme *'ortadaki adam'* olarak adlandırılan bir yazılım yüklenmesiyle makine ile kontrolör arasındaki iletişim kesilmiş, ana bilgisayar bu hatayı ve iletişim sorununu tespit edememiş; bu nedenle ilk aşamada hasar fark edilememiştir. Tahminlere göre, bu saldırı sonucunda otuz bin bilgisayar etkilenmiştir. Ayrıca, basınç ayarlarının değiştirilmesi suretiyle en az iki bin nükleer başlığın kullanılamaz hale geldiği bildirilmiştir.[268]

---

[264] Tolga Erdem, **21. Yüzyılda Uluslararası İlişkilerde Yeni Güç Rekabet Sahası: Siber Uzay**, (Yayınlanmamış Doktora Tezi), Trakya Üniversitesi Sosyal Bilimler Enstitüsü, Edirne, 2020, ss. 248-250.

[265] Paul J. Springer, **Encyclopedia of Cyber Warfare**, ABC-CLIO, California, 2017, s. 279.

[266] Russell Buchan, "Cyber Attacks: Unlawful Uses of Force or Prohibited Interventions?", **Journal of Conflict & Security Law**, Cilt:17, Sayı:2, 2012, s. 219.

[267] Arash Nourian ve Stuart Madnick, "A Systems Theoretic Approach to the Security Threats in Cyber Physical Systems Applied to Stuxnet", **IEEE Transactions on Dependable and Secure Computing**, Cilt:15, Sayı:1, 2018, ss. 5-9.

[268] Şafak, ss. 139-140 ve Ramazan Güreşci, "Siber Saldırıların Uluslararası Hukuktaki Güç Kullanımı Kapsamında Değerlendirmesi", **Savunma Bilimleri Dergisi**, Cilt:18, Sayı:1, 2019, s. 83.

Siber uzayda kullanılan diğer kötü amaçlı yazılım örneklerinden önemli bir şekilde farklılık gösteren ve teknik karmaşıklık ve entegrasyon açısından benzeri görülmemiş bir seviyede performans sergileyen Stuxnet'in, bazı önemli hususlarda öne çıktığı rahatlıkla söylenebilecektir. Niteliği itibariyle Stuxnet'i diğerlerinden ayıran özellikler şu şekildedir:[269]

- Hata Yokluğu: Stuxnet, saldırı amaçlı yazılımlarda tipik olarak bulunan hataların neredeyse hiç bulunmadığı bir yazılım olarak dikkat çekmiştir. Şaşırtıcı bir şekilde, diğer siber saldırı yazılımlarının aksine, Stuxnet'in kodlarında hata tespit edilmemiştir.
- Sıfır Gün (Zero-Day) Güvenlik Açığı: Stuxnet, sıfır gün güvenlik açıklarını kullanarak sisteme yayılması özelliğiyle farklılık göstermiştir. Stuxnet'i kullanan saldırgan yahut saldırganların, hedef sistemde daha önce bilinen güvenlik açıklarını kullanmaktan ziyade daha önce algılanmamış yeni bir güvenlik açığını kullandığı tespit edilmiştir. Sıfır gün yöntemini kullanan saldırılar, siber güvenlik uzmanları ve yazılım geliştiricileri tarafından bilinmeyen ve dolayısıyla koruma önlemlerine karşı savunmasız olan nadir saldırı türlerinden biridir.
- Anti-Virüs Kaçınma Teknikleri: Stuxnet'in bilgisayar koruma yazılımlarını ve güvenlik duvarlarını yanıltmak için tasarlanmış bir dizi anti-virüs kaçınma tekniğine sahip olduğu tespit edilmiştir. Böylece Stuxnet, sistemde yayılırken tespit edilememiş ve amaçlarına ulaşma yolunda saldırganlara süre kazandırmıştır.

Tüm bu sebeplerle, İran'a gerçekleştirilen saldırının da uzun süre tespit edilemediği ve gerekli tedbirlerin alınamadığı ifade edilmektedir. Nitekim Stuxnet'in gündemdeki etkisinin azalmasının ardından, saldırının 2009 yılında başladığı ve 2010 yılına kadar durumdan haberdar olunamadığı da açıklanmıştır.[270] Stuxnet'in bu özellikleri, siber güvenlik uzmanları için büyük bir zorluk teşkil etmiş, siber saldırıların giderek daha komplike ve büyük hedeflere odaklı hale geldiğini göstermiştir.

Kamuoyunda dolaşan çeşitli spekülasyonlar ve basın-yayın kuruluşları tarafından sunulan raporlara göre, Stuxnet saldırısının ABD ile İsrail istihbarat

[269] Erdem, s. 251.
[270] Erdem, s. 251.

servisleri arasında gerçekleştirilen, *'Olimpiyat Oyunları'* olarak adlandırılan ortak bir operasyonun bir parçası olarak geliştirildiği ve kullanıldığı iddia edilmektedir. Ancak saldırının sonuçları ve sorumluluğu, resmi olarak herhangi bir devlet tarafından üstlenilmediği için, İran'ın uluslararası arenada herhangi bir karşılık verme hakkı doğmamıştır. Siber saldırı yeteneklerinin gelişim kapasitesini ortaya koyan ve fiziksel hasara neden olarak uluslararası güvenliğin tehlikeye atıldığı nadir bir örnek olarak kabul edilen Stuxnet, bu yönüyle de bir dönüm noktası olarak görülmektedir.[271]

Stuxnet'in çeşitli varyasyonlarının keşfedilmesi, siber saldırıların etki ve sonuçlarının düşünülenden daha fazla olabileceği olasılığını da gündeme getirmiştir. Örneğin, 2011 yılında keşfedilen ve Stuxnet ile benzer bir kod grubuyla işlenen *'Duqu'* virüsünün, Stuxnet'i yazan ekip tarafından geliştirildiği veya Stuxnet üzerinden gerçekleştirilen yeni programlamaların başarılı bir versiyonu olduğu düşünülmektedir. Ancak Duqu'nun amacının endüstriyel kontrol sistemi üreticileri gibi çeşitli kuruluşlardan istihbarat verileri toplamak ve bu verileri kritik altyapılara yönelik olarak kullanmak şeklinde tezahür ettiği bilinmektedir. Aynı şekilde, 2012 yılında Stuxnet ve Duqu'nun başka bir versiyonu olan *'Flame'* virüsü de araştırmacılar tarafından keşfedilmiştir. Flame, tasarım olarak Stuxnet ve Duqu'ya benzer, ancak daha özelleşmiş hedefli saldırılarda kullanılan karmaşık bir virüs olarak tanımlanmıştır. Medya raporlarına göre, Stuxnet, Duqu ve Flame kötü amaçlı yazılımlarının NSA tarafından Olimpiyat Oyunları operasyonları için geliştirildiği öne sürülmektedir.[272]

Stuxnet siber saldırısı, doğrudan fiziksel zarara yol açabilme yeteneği ve siber uzaydan ziyade alenen gerçek dünyada yıkıcı etkileri olan bir zarar verme amacıyla diğer örneklerden net şekilde ayrılmaktadır. Bu virüs, özellikle İran'ın uranyum zenginleştirme faaliyetlerini engellemek amacıyla kullanılmış ve İran'ın nükleer altyapısının önemli bir kısmını, kendi sistem yeteneklerini aleyhe bir şekilde kontrol ederek, bozguna uğratmıştır. Saldırı sonrasında İran yetkilileri binlerce nükleer

[271] Kay Hearn, Patricia A. H. Williams ve Rachel J. Mahncke, "International Relations and Cyber Attacks: Official and Unofficial Discourse", **11th Australian Information Warfare and Security Conference**, Edith Cowan University, Perth Western Australia, 2010, s. 10.

[272] Lawrence J. Trautman ve Peter C. Ormerod, "Industrial Cyber Vulnerabilities: Lessons from Stuxnet and the Internet of Things", **University of Miami Law Review**, Cilt:72, Sayı:3, 2018, ss. 800-801.

santrifüjün zarar gördüğünü kabul etmiştir. Bununla birlikte kamuoyu nezdinde resmi açıklamadan daha fazla zararın meydana geldiği yönünde bir intiba oluşmuştur.[273]

Stuxnet'in temel olarak, İran'ın nükleer çalışmalarını birkaç yıl boyunca engelleme amacıyla gerçekleştirildiği düşünülmektedir. Bu saldırının bir sonucu olarak İran'ın Bushehr şehrindeki nükleer güç tesislerindeki çalışmaların da geciktiği görülmektedir. Ancak bu durum İran'ın nükleer kalkınmaya ilişkin planlarını değiştirmemiş, aksine bağlılığı güçlenmiştir. İran, zenginleştirilmiş uranyum üretimini durdurmamış, farklı bir devletle anlaşma ya da işbirliği yoluna gitmemiştir.[274]

Stuxnet'e ilişkin bir diğer sonuç, maliyet ve etki açısından daha az maliyetle arzu edilen neticeye kısa yoldan ulaşılabileceğini göstermesidir. Açıktır ki, geleneksel bir kuvvet kullanma eyleminin maliyeti, siber saldırılardan çok daha büyük olacaktır. Ayrıca askeri müdahalelerin mevcut sorunlardan çok daha büyük sıkıntılara yol açma potansiyelinin bulunduğu da göz ardı edilmemelidir.

Stratejik olarak bakıldığında Stuxnet, siber suçlar ile devlet eylemleri arasındaki sınırların belirsizleştiğini göstermektedir. Devletler, şahsi olarak gerçekleştirilen siber suçlardan ve siber uzaydaki teknoloji gelişiminden faydalanabilmektedir. Nitekim devletlerin siber saldırı teknolojilerini kullanma yeteneğinin zayıf olduğu durumlarda, devlet dışı aktörlerin sürece dahil edilmesi ve siber saldırı operasyonlarının yürütülebilmesi gibi yeni olasılıkların mümkün olduğu görülmektedir.[275]

Tarihsel açıdan Stuxnet, siber saldırı sonucunda fiziksel sonuç elde etmeyi başaran ilk saldırı olarak kabul edilmekte ve bu sebeple söz konusu olayda uluslararası hukukta kuvvet kullanma eşiğinin aşıldığı yönünde değerlendirmeler bulunmaktadır. Örneğin Reese Nguyen, bu saldırılarla İran'a verilen zararın, İsrail tarafından 1987-2007 yılları arasında düzenlenen hava saldırıları sonucunda Bağdat ve Suriye'deki kısmen inşa edilmiş reaktörlerin yok edilmesine benzer bir etkiye sahip olduğunu ifade etmektedir.[276]

---

[273] Duncan B. Hollis, "An e-SOS for Cyberspace", **Harvard International Law Journal**, Cilt:52, Sayı:2, 2011, s. 383.

[274] Erdem, s. 255.

[275] Sean Collins ve Stephen McCombie, "Stuxnet: The Emergence of A New Cyber Weapon and Its Implications", **Journal of Policing, Intelligence and Counter Terrorism**, Cilt:7, Sayı:1, 2012, s. 88.

[276] Reese Nguyen, "Navigating Jus Ad Bellum in the Age of Cyber Warfare", **California Law Review**, Cilt:101, Sayı:4, 2013, s. 1082-1083.

Stuxnet sonrasında yaşanan gelişmeleri, uluslararası hukuk bağlamında değerlendirerek konuyu nihayete erdirmek faydalı olacaktır. Siber saldırının bir kuvvet kullanımı olarak kabul edilmesi için, Estonya olaylarında tartışıldığı gibi, bu kuvvetin fiziksel mahiyette bir askeri güç kullanımına denk gelip gelmediğini değerlendirmek gerekecektir. Stuxnet saldırılarıyla, siber uzay dışında, fiziksel olarak hedef alınan şeyin bozguna uğratılması veya tamamen yok edilmesinin amaçlandığı görülmektedir. Bu bağlamda tartışılması gereken husus, BM Andlaşması m. 2/4 hükmünde düzenlenen kuvvet kullanma yasağına aykırı eylemin gerçekleşip gerçekleşmediğidir. Walter Gary Sharp'a göre, doğrudan İran'ın altyapısı hedef alınarak yıkıcı etkileri olan bir siber saldırı gerçekleşmiştir.[277]

Stuxnet'in, açıkça yıkıcı bir saldırı olduğu ve bu saldırının etkilerinin bir milis füzesi veya bomba ile benzer sonuçlara yol açtığı uluslararası hukuk literatüründe hâkim görüş olarak kabul edilmekte ve egemenlik, iç işlere karışmama ilkesi, müdahale ve kuvvet kullanma yasağı gibi tüm temel prensiplerin ihlal edildiği değerlendirilmektedir. Ancak mağdur devlet İran dahil, hiçbir devletin bu durumu egemenlik ihlali olarak görmediğinin de altı çizilmelidir. Hukuken İran'ın nükleer sistemlerinin hedef alınmasının önemi açık olmakla birlikte, sistemin tamamen etkilenmemiş olması, siyasi sebeplerle İran'ın mevcut gerilimi dizginlemek yahut başka yöntemlerle karşılık vermek istemesi, bu durumun sebepleri arasında gösterilmektedir. Yine de saldırının şiddeti ve etkileri göz önüne alındığında, Stuxnet'in büyük sonuçları olduğu, yürürlükteki uluslararası hukuk kurallarına göre değerlendirmeye ihtiyaç duyulduğu açıktır. Devletlerin siyasi ve stratejik adımları ile hukuki gerçeklerin birbirinden ayrı şekilde değerlendirilmesi daha doğru olacaktır.[278]

François Delerue, geleneksel saldırılar ve Stuxnet arasındaki ilişkiyi, bazı önemli noktaları vurgulayarak şu şekilde özetlemiştir:[279]

> *Siber operasyonlar, yıkım, zarar, yaralanma veya insan hayatının kaybına yol açan faaliyetler olarak değerlendirilebilmekte, ancak bu tür saldırıların silahlı saldırı olarak kabul edilmesi için belirli bir şiddet derecesini taşıması gerekmektedir. Muhtemel senaryolar, bir siber operasyonun fiziksel sonuçlarının etkilerini değerlendirmek için belirli bir şiddet eşiğini aşması gerektiği görüşünü desteklemektedir. Örneğin, Stuxnet olayı incelendiğinde, bu saldırının etkilerinin hem şiddet eşiğini aştığı hem de altında kaldığı iddia edilebilmektedir. Bu*

[277] Hollis s. 390 ve Walter Gary Sharp, "The Past, Present, and Future of Cybersecurity", Journal Of National Security Law & Policy, Cilt:4, Sayı:13, 2010, ss. 13-14.
[278] Delerue, s. 297.
[279] Delerue, s. 333.

bağlamda, Stuxnet'in sadece etkisini hesaba katarak bir güç kullanımı olarak kabul edilmesi, ancak bir silahlı saldırı olarak kabul edilmemesi mümkündür. Bununla birlikte, bu saldırının bir nükleer tesisi hedef aldığı gerçeği, onu daha derinlemesine bir inceleme ve sonuçları itibarıyla bir silahlı saldırı olarak değerlendirme olasılığını güçlendirmektedir.
Tallinn Kılavuzu, bu tür olayların silahlı saldırı olarak kabul edilip edilmemesi konusundaki tartışmaları sunmaktadır. Stuxnet, fiziksel zararlara yol açan birçok santrifüjü etkilemiştir. Uluslararası Uzmanlar Grubunun bazı üyeleri, bu saldırının silahlı saldırı eşiğine ulaştığı görüşünü paylaşmaktadır. Stuxnet'in bu tarihe kadar kamuya açık şekilde bilinen ve derin etkilere sahip olan tek siber operasyon olması nedeniyle, siber operasyonların çoğunluğunu silahlı saldırı olarak kabul etmek ise şu an için olanaksızdır. Ancak gelecekte derin etkilere yol açabilecek bir siber operasyonun silahlı saldırı olarak kabul edilme ihtimalini dışlamak da mümkün değildir.

Uluslararası hukukta, uzun bir süre boyunca siber saldırıların geleneksel yöntemleri destekleyici rolü tartışılmış ve kabul edilmiştir. Stuxnet ile bu tartışmalar büyüyüp farklı bir boyut kazanmıştır. Uluslararası toplumun barış ve güvenliğini sağlamak adına, siber saldırılar hakkında daha fazla işbirliği ve uzlaşı ihtiyacı olduğu anlaşılmıştır. Nitekim ciddi anlamda fiziksel tahribat yaratabilecek bir siber saldırıya karşı, ulusal ve uluslararası somut adımlar atılması gerektiği açıkça görülmüş ve Stuxnet, hukuk açısından önemli bir dönüm noktası haline gelmiştir.

C. Süregelen Siber Saldırılar: Ukrayna-Rusya Gerilimi (2014-Günümüz)

Ukrayna ve Rusya arasındaki sorunlar; tarihsel, siyasi ve coğrafi faktörlerin bir sonucu olarak uzun bir geçmişe dayanmaktadır. 1991'de Sovyetler Birliği'nin dağılmasının ardından Ukrayna, bağımsızlığını ilan etmiş ve bağımsız bir devlet olarak uluslararası toplum tarafından tanınmıştır. Ancak bu bağımsızlık süreci, Ukrayna'nın doğusu ve Kırım gibi bölgelerde Rus azınlığın bulunması, etnik benzerlik, ekonomik ve siyasi baskı ve sair sebeplerle sancılı hale gelmiştir. 2000'li yılların başlarından itibaren Ukrayna'nın Avrupa Birliği ve NATO ile ilişkilerini güçlendirmeye yönelik adımlar atması, Rusya ile arasındaki gerilimi artırmıştır. Bu gerilim, son yıllarda özellikle siber saldırılar gibi modern teknolojilerin kullanımıyla yeni boyutlar kazanmıştır.

Kasım 2013 tarihinde, Ukrayna'nın Rusya yanlısı lideri Viktor Yanukovich'in yönetim anlayışından, hükümet politikalarından ve ekonomik durumdan memnun olmayanlar sebebiyle Ukrayna'da sorunlar baş göstermiştir. Sorunlar büyüyerek krize

dönmüş ve bir grup insan tarafından başkent Kiev'deki Bağımsızlık Meydanı'nda (Maidan Nezalezhnosti) protesto başlamıştır.[280] Kendilerine *'Euromaidan'* ismini veren protestocular, sosyal medya üzerinden de etkin bir şekilde çalışarak dünya gündeminde yer edinmiş ve 300.000 civarında protestocuyu Maidan'a toplamayı başarmıştır.

Protestoların etkisiyle krizin yoğunluğu ve şiddeti artmış, 2014 yılında 25.000 kişinin eylem yaptığı sırada Rusya yanlısı olduğu bilinen Berkut isimli özel kuvvetler 100'den fazla kişinin ölümüne sebep olmuştur. Nihayetinde 22 Şubat 2014 tarihinde, Yanukovich ve hükümeti görevden ayrılmış, protestocular kamu binalarını ele geçirmiş, Yanukovich ülkeyi terk ederek Rusya'ya sığınmıştır. Geçici bir hükümet kurularak Olexander Turchynov başına getirilmiştir. Ancak Rusya, söz konusu geçici hükümeti tanımadığını bildirmiştir.[281]

Rusya, geçmişten günümüze, Sovyetler Birliği dağılsa dahi, bağımsızlığını ilan eden devletler üzerinde siyasi kontrolünü korumayı amaçlamıştır. Bu sebeple Euromaidan protestolarını lehine kullanarak krizi askeri ve stratejik bir fırsata çevirmiştir. Ukrayna'nın çeşitli bölgelerinde başlayan çatışmalar, ülkeyi iç savaşa sürüklemiştir. 27-28 Şubat 2014 tarihlerinde, Kırım sınırına yığılan Rus askerleri ve bölgeye gönderilen Spetsnaz ismindeki özel kuvvet taburu, Kırım'daki Rus yanlısı kesimle birlikte devlet kurumlarının kontrolünü ele geçirmek için askeri operasyonlar gerçekleştirmiş; Kırım'ın başkenti Simferepol'de hükümet binalarındaki Ukrayna Bayrağı indirilerek Rus Bayrağı göndere çekilmiştir. Sergey Aksyonov dönemin başbakanı olarak atanmıştır.[282]

16 Mart 2014 tarihinde, Ukrayna ve diğer batılı devletler nezdinde tanınmamış bir referandum yapılmış ve %97 olumlu oyla Kırım'ın bağımsızlığı ilan edilmiştir. Hemen ardından Rusya ve Kırım liderleri, Rusya'nın başkenti Moskova'da bir araya gelerek Kırım'ın Rusya'ya katılması yönünde bir uluslararası andlaşma akdetmiştir. Böylece, Kırım'ın ilhakı resmen gerçekleşmiş ve Kırım, fiilen Rusya hâkimiyetine

[280] Jan Stinissen, "A Legal Framework for Cyber Operations in Ukraine", **Cyber War in Perspective: Russian Aggression against Ukraine**, (Ed. Kenneth Geers), NATO CCDCOE Publications, Tallinn, 2015, s. 125.

[281] Michael Kofman, Katya Migacheva, Brian Nichiporuk, Andrew Radin, Olesya Tkacheva ve Jenny Oberholtzer, **Lessons from Russia's Operations in Crimea and Eastern Ukraine**, RAND Corporation, California, 2017, s. 1.

[282] Kofman ve diğerleri, ss. 7-11 ve Güven, s. 303.

geçmiştir. Bölgede yaşayan Ukraynalılar ve Kırım Tatarları göç etmek durumunda kalmıştır.[283] 27 Mart 2014'te BM Genel Kurulu, Kırım Referandumunun geçersiz olduğunu bildiren kararını kamuoyuna açıklamış[284]; ABD, İngiltere, Fransa, Almanya, İtalya, Polonya, Kanada, Japonya, Hollanda, Güney Kore, Gürcistan, Moldova, Türkiye, Avustralya ve Avrupa Birliği Rusya'yı, Ukrayna'nın egemenlik alanını ihlal ettiği ve Ukrayna'nın iç işlerine müdahale ettiği gerekçeleriyle kınamıştır.[285]

Kırım'ın ilhakı, Rusya ve Ukrayna arasındaki gerilimi daha da tırmandırarak yeni bir boyuta taşımıştır. Ukrayna'nın doğusundaki Donetsk ve Luhansk bölgelerinde Rus nüfusun yoğun olması sebebiyle ayrılıkçı hareketler güç kazanmış ve Nisan 2014'te gerçekleştirilen bağımsızlık referandumlarıyla Donetsk ve Luhansk Halk Cumhuriyetleri ilan edilmiştir. Daha sonrasında, Donbass bölgesi olarak adlandırılan söz konusu iki yapılanmayı birleştirmek amacıyla Konfederal Yeni Rusya (Novorossiya) devleti kurulmuştur. Rusya, açık bir şekilde Ukrayna'nın doğusundaki fiili hâkimiyetini artırmaya devam etmiştir. Bu girişim uluslararası toplumda büyük ölçüde tanınmamış ve Ukrayna'nın toprak bütünlüğüne yönelik bir tehdit olarak kabul edilmiştir.[286]

Temmuz 2014'te, Malezya MH17 Boeing 777 uçağı Donetsk ve Luhansk bölgeleri üzerinde seyir halindeyken, ayrılıkçı politika güden Doğu Ukraynalı askerler tarafından düşürülmüş ve uçaktaki 298 kişiden kurtulan olmamıştır. Rus yapımı silahlar kullanılarak gerçekleştirilen bu olay, uluslararası toplumda da büyük bir yankı uyandırmış ancak sorumlular tespit edilememiştir. Nihayetinde yerel sorunlarla başlayıp büyüyen bu kriz, uluslararası barışı ve güvenliği tehdit eder hale gelmiş ve sıcak çatışmalar başlamıştır.[287]

Donbass bölgesindeki gerilim ve askeri çatışmalar, Ukrayna'nın egemenliğini ciddi şekilde sarsmış, Donetsk ve Luhansk nezdinde özerk yönetimler kurulmasının

---

[283] Erdem, s. 275.

[284] United Nations General Assembly, **Territorial integrity of Ukraine**, 68/262, 2014, https://documents-dds-ny.un.org/doc/UNDOC/GEN/N13/455/17/PDF/N1345517.pdf?OpenElement (03.10.2023).

[285] Robert Mandel, **Optimizing Cyberdeterrence: A Comprehensive Strategy for Preventing Foreign Cyberattacks**, Georgetown University Press, Washington, 2017, ss. 117-118.

[286] Güven, s. 304 ve Margarita Levin Jaitner, "Russian Information Warfare: Lessons from Ukraine", **Cyber War in Perspective: Russian Aggression against Ukraine**, (Ed. Kenneth Geers), NATO CCDCOE Publications, Tallinn, 2015, s. 92.

[287] Delerue, s. 91, Güven s. 304 ve Jean-Loup Richet, **Cybersecurity Policies and Strategies for Cyberwarfare Prevention**, Information Science Reference, Pennsylvania, 2015, s. 321.

kabul edileceği ve ateşkesin sağlanacağı bir mutabakat yapılması gündeme gelmiştir. Bunun üzerine 5 Eylül 2014 ve 12 Şubat 2015 tarihlerinde, Ukrayna, Donetsk, Luhansk, Rusya, Fransa ve Almanya ile birlikte Avrupa Güvenlik ve İşbirliği Teşkilatı (Organization for Security and Cooperation in Europe – OSCE/AGİT) temsilcilerinin katılımıyla Minsk Protokolleri[288] imza altına alınmıştır. Minsk Protokolleri, Ukrayna'nın doğu bölgesinde istikrarı sağlamak adına iki devletin olumlu mahiyette attığı ilk adımdır. Buna rağmen silahlı çatışmalar bir süre kesilse de siyasi anlaşmazlıklar devam etmiştir.[289]

Ukrayna ve Rusya krizi, başlangıcından günümüze değin çeşitli askeri ve sıcak çatışmalarla birlikte, siber saldırılardan da destek alınarak yürütülen sistematik operasyonlarla devam etmiştir. Rusya, Ukrayna aleyhine propaganda yapma, bilgi çarpıtma, iletişim ağ ve sistemlerini bozma amaçlarıyla gerçekleştirdiği siber saldırıları, diğer stratejilerini destekleyecek şekilde konumlandırmıştır. Aynı zamanda askeri harekâtlarını siber saldırılar ile örtbas ederek çatışma yaşanan bölgeleri görünmez kılmıştır.

Rusya, Ukrayna'ya yönelik siber saldırılarla casusluk faaliyetleri gerçekleştirmiş, bunun dışında altyapı sistemlerine zarar veren çeşitli yazılımlar da kullanmıştır. İlk olarak 2010 yılında, *'Snake/Turla/Uroboros'* isimleri ile bilinen virüsü kullanarak Ukrayna'nın devlet sistemlerine sızmıştır. Virüs tarama ve güvenlik programlarını kolaylıkla atlatabilen Snake, bilgisayar üzerindeki her türlü veriyi okuyup analiz ederek dışarıya gönderebilen nitelikleri sebebiyle etkin rol oynamıştır. Böylelikle Rusya, Ukrayna'nın strateji ve planlarına ulaşım sağlamış ve her zaman bir adım önde olabilmiştir.[290]

Euromaidan protestoları ve Kırım'ın ilhakı sırasında MiniDuke, NetTraveler ve RedOctober gibi kötü amaçlı programlar da Ukrayna sistemlerini hasara uğratmıştır. Berkut özel kuvvetleri ve Berkut ile ilişkisi olduğu düşünülen yahut bağımsız hareket eden siber gruplar, Ukrayna'yı yıpratacak nitelikte birçok zarar

---

[288] Protokollerin aslına erişim sağlamak için bkz. **OSCE**, Протокол о результатах консультаций Трехсторонней контактной группы, Минск, 5 сентября 2014 г., Minsk, 2014, https://www.osce.org/ru/home/123258 (12.10.2023) ve **OSCE**, Комплекс мер по выполнению Минских соглашений, Minsk, 2015, https://www.osce.org/ru/cio/140221 (12.10.2023).

[289] Gökhan Cin ve Hasan Hüseyin Tekin, "Rusya'nın Hibrit Savaş Kapasitesinin Kırım ve Donbas Vakaları Üzerinden Analizi", **Güvenlik Stratejileri Dergisi**, Cilt:17, Sayı:37, 2021, ss. 225-226.

[290] Jaitner, s. 90 ve Stinissen, s. 126.

vermiştir.[291] Söz konusu gruplar, devletin internet sitelerini erişilemez hale getirmiş, Ukrayna devlet görevlilerinin telefonlarını bloke etmiş, medya sitelerini ve Ukrayna destekçisi internet sitelerini çökertmiş, internet yoluyla iletişimi kesmiş, özel nitelikli kişisel verileri ele geçirerek yayınlamış, bankalardan dijital transfer yoluyla büyük miktarda para çalmış ve nihayetinde askeri sistemlerin hedef algılarını bozmuştur.[292]

Ukrayna ve Rusya arasındaki olaylar bununla sınırlı kalmamış, 2015 ve 2016 yıllarında Ukrayna'da yaşayan halkın büyük çoğunluğunu etkileyen elektrik kesintileri yaşanmıştır. Özellikle Ukrayna'da yaşanan elektrik kesintisi öncesi dönemde, Ukrayna taraftarı eylemciler tarafından Kırım'a elektrik sağlayan trafo merkezlerine fiziksel saldırılar gerçekleştirilmiş ve bu durumun sonucunda yaklaşık iki milyon Kırım nüfusu geçici olarak elektriksiz kalmıştır. 23 Aralık 2015 tarihinde ise, 6 ay boyunca Ukrayna enerji şirketlerine yönelik gerçekleştirildiği anlaşılan örgütlü ve ihtiyatlı siber saldırılar sonuç vermiş, Ukrayna'nın batısındaki Ivano-Frankvisk bölgesinde yaklaşık 700.000'den fazla kişinin saatlerce elektriksiz kalmasına sebep olmuştur. Bu saldırılar, birçok trafoyu devre dışı bırakarak çağrı merkezlerini kilitlemiş ve bilgisayarların önemli dosyalarını silerek sistemi çalışmaz hale getirmiştir. Bu olaylar, siber silahların modern bir savaş aracı olarak kullanılma potansiyelini açıkça gözler önüne sermiş ve güçlü bir ikaz niteliği taşımıştır.[293]

Bir yıl sonra, 17 Aralık 2016'da, Ukrayna'nın elektrik şebekesi büyük bir siber saldırıya daha maruz kalmış ve yaklaşık 225.000 kullanıcının elektriği kesilmiştir. 2015 yılındaki saldırıya benzer şekilde gerçekleştirilen saldırı, işçilerin trafo merkezlerine giderek manuel yöntemlerle kesicileri kapatması suretiyle birkaç saat içinde etkilerini yitirmiştir. Söz konusu saldırıda kullanılan kötü amaçlı yazılım *'CrashOverride'* olarak adlandırılmış ve fiziksel endüstriyel süreçleri bozmak için tasarlandığı tespit edilmiştir. CrashOverride, Stuxnet'ten sonra mahiyeti ve büyüklüğü itibariyle endüstri sistemlerine etki eden ikinci kötü amaçlı yazılım olarak tanımlanmıştır.[294] Nihayetinde, siber saldırıların giderek daha önemli hale geldiği ve

[291] Kenneth Geers, "Russian Introduction: Cyber War in Perspective", **Cyber War in Perspective: Russian Aggression against Ukraine**, (Ed. Kenneth Geers), NATO CCDCOE Publications, Tallinn, 2015, s. 15.
[292] Güven, ss. 305-307.
[293] Erdem, s. 276.
[294] Kevin Hemsley ve Ronald Fisher, "A History of Cyber Incidents and Threats Involving Industrial Control Systems", **12. International Conference on Critical Infrastructure Protection (ICCIP)**, 2018, s. 230.

yaşam şartlarına müdahale niteliği taşıyabileceği, net bir şekilde tekrar ortaya konmuştur.

2015 ve 2016 yıllarında artarak devam eden ve devletlerin arka plandan destekledikleri siber gruplarla farklı bir anlam kazanan siber saldırılar, hukuki meselelerle birlikte uluslararası ilişkileri ve ekonomiyi ilgilendiren birçok sorunun gündeme gelmesine sebep olmuştur. *'Fancy Bear'* ismiyle anılan ve Rusya tarafından bizzat desteklendiği düşünülen bir grup siber korsan ABD sunucularına saldırmış, başka bir grup *'Sandworm'* ise Ukrayna'nın devlet yapılanmalarına ve özel sektördeki şirketlere bir dizi siber saldırı gerçekleştirmiştir. 2017 yılına gelindiğinde, teknoloji tarihinin küresel çapta etkilere yol açan en yıkıcı saldırılarından biri olan *'NotPetya'* ile durum daha da vahim bir hal almıştır.[295]

Ukrayna menşeili bir yazılım şirketi olan Linkos Grup şirketinin sunucularından başlatılan NotPetya siber saldırısıyla, uluslararası işlemlerde de kullanılan bir muhasebe uygulaması üzerinden saatler içinde tüm dünya geneline, yaklaşık 8000 bilgisayar ağına, yüz binlerce kullanıcıya ve 65 ülkeye, kötü amaçlı yazılım yayılması sağlanmıştır. Birkaç aylık süreçte ortaya çıkan fidye yazılımlarının bir çeşidi olan NotPetya, herhangi bir onaya bağlı kalmaksızın kendiliğinden sistem içinde gezinebilmekte ve sistem dosyalarını şifreleyebilmektedir. Böylece Windows sunucuları erişilemez hale gelmekte ve kullanıcılar bilgisayarlarını kullanamamaktadır. Spesifik olarak Ukrayna'yı öncelikli hedefinde bulunduran bu yazılım, saldırılarının %75'ini Ukrayna'ya yönelik olarak gerçekleştirmiş; devlet bankaları, enerji şirketleri, internet, medya ve haberleşme ağları olmak üzere birçok kuruluş ciddi zarara uğramıştır. Ukrayna Devlet Güvenlik Servisi (Security Service) tarafından NotPetya'nın arkasında Rusya'nın olduğu ileri sürülmüş ancak Rusya tarafından bu iddiaya yanıt verilmemiştir. Çok kısa bir zaman içerisinde büyük ekonomik felaketlere yol açan yazılım sebebiyle küresel mahiyette oluşan zararın 10 milyar doları aştığı düşünülmektedir.[296]

2018 yılından itibaren Ukrayna durumun vahametini kavramış ve bütçe ayırarak siber güvenlik hususunda devlet kurumlarını korumak amacıyla

[295] Erdem, s. 277.

[296] Delerue, ss. 173-177 ve Louis Léonet, **Contextual Cyber Securitisation: A Case Study of Russian Cyberattacks against Ukraine**, (Yayınlanmamış Yüksek Lisans Tezi), Leiden Üniversitesi, Hollanda, s. 16 ve Andrew Coburn, Éireann Leverett, ve Gordon Woo, **Solving Cyber Risk: Protecting Your Company and Society**, Wiley, New Jersey, 2019, ss. 13-14.

geliştirmelere başlamıştır. ABD başta olmak üzere, Ukrayna'nın siber güvenlik projelerine yatırım ve destek sağlanmıştır. Yaşananlar uluslararası işbirliğinin önemini göstermiş ve siber saldırılar konusunda daha çok çalışma yapılması gerektiğini bir kez daha gözler önüne sermiştir.[297]

2021 yılında, Rusya Devlet Başkanı Vladimir Putin, Ukrayna Devlet Başkanı Volodimir Zelenskiy ile görüşmeyi kabul etmemiş ve Ukrayna'yı Rus düşmanlığı ile suçlayıp süreci siyasi olarak çözülemeyecek şekilde çıkmaza sokmuştur. Ukrayna'nın NATO, ABD ve Avrupa Birliği'nden güvenlik maksadıyla destek istemesi Rusya tarafından hoş karşılanmamış ve kriz giderek büyümüştür.[298] 24 Şubat 2022 tarihine gelindiğinde ise Rusya *'Özel Askeri Operasyon'* ismini verdiği bir silahlı saldırıyla Minsk Protokolleri'ni hiçe sayarak iki devlet arasındaki savaşı resmen başlatmıştır. Söz konusu saldırı BM ve Türkiye dahil birçok üye devlet tarafından kabul edilemez bulunmuş, reddedilmiştir.[299] Günümüzde halen etkisi olan bu savaşta, siber saldırılarla yıpratma politikası gücünü artırarak devam etmekte; geleneksel askeri operasyonlar ve savaşlar yerini bilgi savaşına bırakmaktadır.

Ukrayna ve Rusya arasında yaşananları, siber saldırılar ve uluslararası hukuk kapsamında değerlendirerek konumuzu nihayete erdirmek gerekmektedir. Rusya lideri Putin ve Rusya hükümeti, Ukrayna'ya yönelik olarak gerçekleştirdiği tüm saldırıları gerçeklikten yoksun birkaç ana sava dayandırmaktadır. Bu başlıklar şu şekilde özetlenebilmektedir:[300]

- Ukrayna, Rusya için bir silahlı saldırı sorunudur.
- Ukrayna, Donbass bölgesinde soykırım yapmaktadır.
- Ukrayna'da 'Yeni Nazi' rejimi bulunmaktadır.
- Ukrayna, tarihi perspektifte her zaman Rusya'nın parçasıdır.

Söz konusu ifadeler uluslararası arenada kabul görmemiş ve kınanmıştır. Uluslararası hukukta her devletin egemen olduğu ve kendi kaderini tayin hakkı bulunduğu açık bir

---

[297] Erdem, s. 279.

[298] Yağmur Ekim Yılmaz, "Milletlerarası Hukukta Kuvvet Kullanma Yasağı Kapsamında Rusya'nın Ukrayna'ya Müdahalesi", **Uluslararası İlişkiler ve Diplomasi Dergisi**, Cilt:5, Sayı:2, 2022, ss. 60-61.

[299] T.C. Dışişleri Bakanlığı, **24 Şubat 2022, Rusya Federasyonu Tarafından Ukrayna'ya Yönelik Başlatılan Askeri Operasyon Hk.**, 62 Numaralı Resmî Açıklama, Ankara, 2022.

[300] Hakkı Hakan Erkiner, "Rusya-Ukrayna Savaşı Dairesinde Uluslararası Hukuk Meseleleri", **Uluslararası Akdeniz Hukuku Kongresi 2022: Akdeniz Üniversitesi Hukuk Fakültesi'nin Kuruluşunun 30. Yılı Anısına**, Adalet Yayınevi, Ankara, 2022, s. 347.

şekilde düzenlenmektedir. Bu sebeple Ukrayna'nın ulusal kararları ve iç işleyişine müdahale edilmesi haksız ve hukuka aykırıdır.

2014 seçimlerindeki baskılar, 2015 yılındaki enerji sistemlerine yönelik saldırılar ve 2017'deki NotPetya olayları göz önüne alındığında siber sorunlar birçok endişeyi beraberinde getirmiş, uluslararası hukukta birçok tartışmaya yol açmıştır. Siber saldırıların kuvvet kullanma olarak değerlendirilmesi hususundaki eşik henüz tem olarak netlik kazanmasa da egemenliğin ihlali ve müdahale yasağı kavramlarının ihlali açık ve net bir şekilde ortaya koyularak, bu durumun ayrıntılı bir şekilde değerlendirilmesi önemli hale gelmiştir.

Schmitt'e göre birçok devlet, fiziki olarak zarar ve hasar meydana getirmediği sürece, siber saldırıları kuvvet kullanma eylemi olarak ele almamaktadır. Sorumluluk bakımından değerlendirildiğinde, söz konusu siber saldırıların Rusya yahut Rusya'nın desteklediği siber gruplar aracılığıyla gerçekleştiği büyük oranda kabul görmekte fakat somut olarak isnat edilebilme meselesi tartışmalı halini sürdürmektedir. İlk aşamada yoğunluk ve etki kıstasları düşünüldüğünde kuvvet kullanmadan ziyade müdahale yasağının ihlal edebileceği mümkün görülmektedir. Ancak silahlı saldırılar nezdinde siber saldırıların destekleyici yapısı da göz ardı edilmemelidir. Benzer bir mantık, meşru müdafaa hakkı için de kurulabilecektir. Nihayetinde, tüm bunları konuşabilmek için, söz konusu saldırıların somut bir şekilde Rusya'ya isnat edilmesi gerektiği unutulmamalıdır. Kuvvet kullanma yasağı, yalnızca devletler için geçerli bir uluslararası hukuk ilkesidir. Bu sebeple devlet dışı aktörlerin gerçekleştirdiği siber saldırılar, iç hukuku ihlal etse de uluslararası arenada sonuç doğurmayacaktır. Söz konusu hususlar siber uzayın doğası gereği gizemini ve belirsizliğini korumaya devam etmektedir.[301]

Nihayetinde, mevcut durumun isnadiyet koşullarını sağladığı varsayıldığında ve Ukrayna'ya yönelik gerçekleştirilen eylemlerin hepsi birlikte değerlendirildiğinde kuvvet kullanma eşiğinin aşılmış ve meşru müdafaa hakkının ortaya çıkmış olduğu savunulabilecektir. Rusya bizzat gerçekleştirdiği ve desteklediği siber saldırılarla, bu konuda uzmanlaştığını ve uluslararası mahiyette tehdit oluşturabileceğini kamuoyuna göstermiştir. Siber stratejilerde kendini sürekli geliştiren Rusya, Estonya örneğinde

[301] Michael N. Schmitt, "Russian Cyber Operations And Ukraine: The Legal Framework", **Lieber Institute West Point**, 2022, https://lieber.westpoint.edu/russian-cyber-operations-ukraine-legal-framework/ (09.10.2023).

yalnızca siber saldırılar gerçekleştirmiş, Gürcistan örneğinde askeri operasyonları desteklemek amacıyla siber saldırıları kullanmıştır. Ukrayna örneğinde ise siber saldırıları hibrit savaş ortamında kullanmış ve Ukrayna'yı iç savaşa sürükleyerek stratejik hedefi olan Kırım'ı ilhak edip süreci kendi lehine çevirmiştir. Nitekim petrol ve doğalgazın aktarımı ve Avrupa bölgesindeki ekonomik ilişkilerde Kırım'ın konumu yadsınamaz bir değere sahiptir.

Rusya'nın düşmanca tutum ve eylemlerinin uluslararası hukuka birçok açıdan çeşitli sonuçları bulunmaktadır. 2014'ten günümüze değin Rusya, birçok temel ilkeyi çiğneyerek bir devletin egemenliğini hiçe saymış, müdahale yasağını ihlal etmiş ve kuvvet kullanma eşiğini aşmıştır. Bununla birlikte 2022 yılından itibaren doğrudan bir askeri operasyonla saldırıya girişmiş, süreç artık uluslararası insancıl hukuk ve silahlı çatışmalar hukuku kurallarının uygulanması gereken ayrı bir duruma evrilmiştir. Önemle hatırlatmak gerekir ki; tüm devletler uluslararası hukuka tabidir ve söz konusu kurallar somut olaylar ışığında uygulanmaya devam edecektir.

SONUÇ

Egemenlik, ortaya çıktığı zamandan günümüze değin, çeşitli tartışmalara konu olmuş ve gündemde yerini koruyan bir kavram olarak karşımıza çıkmaktadır. Egemenlik, devletler tarafından gerçekleştirilen yahut devletlere atfedilebilen eylemlerle ihlal edilebilir. Bununla birlikte devlet dışı aktörler ve kişisel eylemlerin de egemenliğe zarar vermesi ihtimali bulunmaktadır. Devlet dışı aktörlere ve kişilere karşı yargı yetkisi kullanmak devletlerin en temel haklarından biri olmakla birlikte uluslararası hukuk kurallarına da riayet edilmelidir. Siber uzay, siber güvenlik ve siber saldırılar bu hususstaki yeni tartışma alanlarından birini oluşturmaktadır.

Siber saldırılar, devletlerin egemenlik alanını tehdit edebilecek ve uluslararası hukukta sorunlara yol açabilecek yeni bir güvenlik açığıdır. Siber uzay kapsamında birçok yöntem ve aktörle siber saldırılar gerçekleştirilebilmekte, devletler anonim ve sınır aşan teknolojiye sahip bir tehditle karşı karşıya kalmaktadır. Devletler bu alanı uluslararası teamül kuralları ve andlaşmalar çerçevesinde bağlayıcı düzenlemelere tabi tutana dek mevcut kuralların somut olaylara uygulanması gerekmektedir. Bu noktada ise iç işlere müdahale ve kuvvet kullanma yasağı hususları gündeme gelmektedir.

Siber tehditlerin siber saldırı boyutuna ulaşması, teknolojik gelişmelerle birlikte büyük sorunlara yol açabilecek fiillerin ilk adımı olarak karşımıza çıkmaktadır. Devletlerin siber tehditlere karşı yetkilerini kullanabilmesi için, siber uzayda faaliyet gösteren kişi ve kişilerin, ilgili devletin ulusal yetki alanlarında etkili olması yeterlidir. Bazı durumlarda ise yetki alanını aşan tehditler söz konusu olabilmekte ve uluslararası hukuk kurallarına başvurmak önemli hale gelmektedir. Bu durumda ise siber saldırıların mahiyeti, niteliği itibariyle hangi kural ve ilkeleri ihlal ettiği hususu önem arz etmekte, her bir somut olay için ayrı ayrı değerlendirme yapılması gerekmektedir.

BM Andlaşması m. 2/1, 2/4 ve 2/7 hükümleri çerçevesinde devletlerin egemen eşitliği ilkesi vurgulanmış, kuvvet kullanma yahut tehdidinde bulunma yasaklanmış, devletlerin iç işlerine karışmama ilkesi benimsenmiştir. Kuvvet kullanmaya dair getirilen istisnalardan biri ise BM Andlaşması m. 51'de düzenlenen meşru müdafaa hakkı olarak düzenlenmiştir.

Siber saldırıların egemenlik, iç işlere karışmama ilkesi, müdahale yasağı, kuvvet kullanma yasağı ve meşru müdafaa hakkı çerçevesinde değerlendirilmesi, ilk

olarak Tallinn Kılavuzu'nda gündeme gelmiştir. Bu bağlamda bir siber saldırının, devletler tarafından gerçekleştirildiğinin kuvvetli delillerle ispat edilmesi ve silahlı kuvvet eşiğinin aşılması halinde; kuvvet kullanma yasağı ihlal edilmiş olacaktır. Saldırının ağırlığına ve Schmitt ölçütlerini karşılayan niteliği haiz olmasına göre; saldırıya uğrayan devletin meşru müdafaa hakkı da gündeme gelebilecektir.

Uluslararası hukukta hâkim olan görüş, BM Andlaşması m. 2/4 hükmü ve teamül uyarınca, "kuvvet kullanma" eylemlerinin "silahlı saldırı" niteliğindeki eylemlerden daha düşük bir eşik olduğu yönündedir. Tüm silahlı saldırılar kuvvet kullanımıdır ancak bunun tam tersi doğru olmayacaktır. Tallinn Kılavuzu kapsamında Uluslararası Uzmanlar Grubu görüşlerine göre, siber uzayda da ilgili temel prensiplerin ihlaline ilişkin net bir ayrım yapılamamış, somut olaylar üzerinde değerlendirme yapmak önemli hale gelmiştir.

Tallinn Kılavuzu'nu hazırlayan Uluslararası Uzmanlar Grubu'na göre, siber operasyonların, özellikle ciddi yaralanma veya fiziksel hasara yol açtığı durumlarda, silahlı saldırı eşiğinin aşılmasının tek başına yeterli olabileceği konusunda oybirliğiyle mutabakata varılmıştır. Grubun bazı üyeleri daha da ileri giderek neden olunan zararın niteliğine değil ciddiyetine odaklanmıştır.

Bir devletin ekonomik çöküşüyle sonuçlanan, yeterince ciddi, zarar verici veya yıkıcı olmayan siber operasyonları da silahlı saldırı olarak nitelendirmek mümkündür. Bu çerçevede siber saldırılar, bir başka kuvvet kullanma eylemine denk büyüklükte zararlar meydana getirirse, kuvvet kullanma yasağı ihlal edilmiş olacak ve devletler zorlayıcı karşı önlemlere başvurabilecektir. Siber saldırının silahlı saldırı koşullarını sağlaması halinde ise, saldırıyı bertaraf etmek amacıyla meşru müdafaa hakkı kullanılabilecektir. Bu durumda devletlerin meşru müdafaa hakkının orantılılık ilkesine bağlı kalmak suretiyle, geleneksel yahut siber yöntemlerle, karşılık verme hakkı doğacaktır.

Devletler, genelde siber saldırıları açık bir şekilde gerçekleştirmeyip saldırıların kaynağını devlet dışı aktörler üzerinden yahut teknik yollarla gizlemeye çalışmaktadır. Bu nedenle devletlerin siber saldırı faaliyetlerinin kuvvet kullanma yasağı çerçevesinde değerlendirilebilmesi için, saldırının doğrudan veya dolaylı olarak söz konusu devlet tarafından gerçekleştirildiği kanıtlanmalıdır. Siber saldırıların

anonim olabilme özelliğinden dolayı, bir saldırının devlete atfedilmesi sürecinin çeşitli zorluklar içerdiği unutulmamalıdır.

Belirtmek gerekir ki; devletlerin uluslararası arenadaki güç ve dünyanın ortak menfaatleri dengesini koruyarak uzlaşı sağlaması, uzun bir süreç gerektirebilmektedir. Bu süreçte ulusal düzenlemeler ve uluslararası hukukun temel kurallarıyla siber uzaya ilişkin uygulamalar geliştirilmeli; büyük çapta yıkımlar oluşmasının önüne geçilmelidir. Nitekim devletler tarafından kuvvet kullanma yasağına ilişkin silahlı saldırı eşiğinin karşılıklı olarak aşılması halinde, uluslararası insancıl hukuk ve silahlı çatışmalar hukuku kurallarının uygulama alanı bulabileceği unutulmamalıdır.

Geçmişte karşılaşılan ve günümüzde halen etkisini sürdüren örneklerde de görüldüğü üzere, siber saldırılar stratejik fikirlerle desteklendiğinde büyük yıkımlara sebep olabilmektedir. Gelecekte daha büyük sorunlarla karşılaşmamak adına, siber uzay alanına ilişkin uluslararası hukukta caydırıcı düzenlemeler oluşturulmalı ve devletlerin bu düzenlemelere uyması için gerekli tedbirler alınmalıdır. Önemle vurgulamak gerekir ki; uluslararası işbirliği, uluslararası hukukun uygulanabilirliğini koruyan bir mihenk taşıdır. İşbirliği için devletlerden hakiki adımlar atılmadığı takdirde, uluslararası hukuk gücünü yitirmektedir.

KAYNAKÇA

12 Ağustos 1949 Tarihli Cenevre Sözleşmeleri ve Ek Protokolleri, (Yayına Hazırlayanlar: Melike Batur Yamaner, A. Emre Öktem, Bleda Kurtdarcan, Mehmet C. Uzun), Galatasaray Üniversitesi Yayınları, İstanbul, 2008.

Ada, Mehmet ve Hüseyin Çakır. "Kuzey Atlantik Antlaşma Örgütü'nün (NATO) Siber Güvenlik Stratejisinin İncelenmesi", **Düzce Üniversitesi Bilim ve Teknoloji Dergisi**, Cilt:5, Sayı:2, 2017, ss. 632-656.

Ahronheim, Anna. "Liberman: Squabbling over credit for strike on Syrian reactor an 'embarrassment'", **The Jerusalem Post,** https://www.jpost.com/Israel-News/Liberman-praises-Israels-strike-on-Syrian-reactor-Livni-recalls-events-546640 (02.07.2023).

Akın, Murat ve Şeref Sağıroğlu. "Gelişmiş Sürekli Tehditler", **Türkiye Bilişim Vakfı Bilgisayar Bilimleri ve Mühendisliği Dergisi**, Cilt:10, Sayı:1, 2017, ss. 1-10.

Akman, Toygar. **Sibernetik "Dünü Bugünü Yarını"**, Kaknüs Yayınları, İstanbul, 2003.

Anand, R. P.. "Sovereign Equality of States in International Law", **International Studies**, Cilt:8, Sayı:3, 1966, ss. 213-241.

Andress, Jason ve Steve Winterfeld. **Cyber Warfare: Techniques, Tactics and Tools for Security Practitioners**, Second Edition, Elsevier Inc., 2014.

Arasan, Murat Can. **Uluslararası Hukukta Devletlerin Egemen Eşitliği İlkesi**, (Yayınlanmamış Yüksek Lisans Tezi), Ankara Üniversitesi Sosyal Bilimler Enstitüsü, Ankara, 2017.

Ataş, İsmail. **Otonom Silah Sistemlerinin ve Siber Saldırıların Uluslararası İnsancıl Hukukun Temel Prensiplerine Uygunluğu**, Adalet Yayınevi, Ankara, 2023.

Avrupa Konseyi Sanal Ortamda İşlenen Suçlar Sözleşmesi. RG 09.08.2014, Sayı:29083.

Bağcı, Hasan. "Sosyal Mühendislik ve Denetim", **Denetişim**, Sayı:1, 2009, ss. 42-51.

Bal, Ali. **Devletin Uluslararası Sorumluluğunun Doğması**, (Yayınlanmamış Yüksek Lisans Tezi), Dokuz Eylül Üniversitesi Sosyal Bilimler Enstitüsü, 2006.

Balık, Gürcan. "Anayasa'da "Milletlerarası Hukukun Meşru Saydığı Haller" Sorunu", **Uluslararası İlişkiler Dergisi**, Cilt:12, Sayı:47, 2015, ss. 47-71.

Bass, Warren. **A Surprise Out of Zion?**, RAND Corporation, Santa Monica, 2015.

Benedikt, Michael. "Cyberspace: Some Proposals", **Cyberspace: First Steps**, Ed. Michael Benedikt, 3. Baskı, MIT Press, London, 1992, ss. 119-224.

Beriş, H. Emrah. "Egemenlik Kavramının Tarihsel Gelişimi ve Geleceği Üzerine Bir Değerlendirme", **Ankara Üniversitesi SBF Dergisi**, Cilt:63, Sayı:1, 2008, ss. 55-80.

Bıçakcı, Salih. "NATO'nun Gelişen Tehdit Algısı: 21. Yüzyılda Siber Güvenlik", **Uluslararası İlişkiler**, Cilt:10, Sayı:40, 2014, ss. 101-130.

Bıçakçı, Salih. "Yeni Savaş ve Siber Güvenlik Arasında NATO'nun Yeniden Doğuşu", **Uluslararası İlişkiler**, Cilt:9, Sayı:34, 2012, ss. 205-226.

Bilen, Abdulkadir. **Akıllı Yöntemler ile Siber Saldırı Tespit Sistemi Geliştirilmesi**, (Yayınlanmamış Yüksek Lisans Tezi), Fırat Üniversitesi Fen Bilimleri Enstitüsü, Elazığ, 2021.

Birleşmiş Milletler Andlaşması. RG 24.08.1945, Sayı:6092.

Bodin, Jean. **On Sovereignty: Four chapters from The Six Books of the Commonwealth**, Ed. ve Çev. Julian H. Franklin, Cambridge University Press, United Kingdom, 1992.

Bolat, Can. **Siber Saldırılara Karşı Meşru Müdafaa Hakkının Uluslararası Hukuk Açısından İncelenmesi**, (Yayınlanmamış Yüksek Lisans Tezi), İstanbul Üniversitesi Sosyal Bilimler Enstitüsü, İstanbul, 2020.

Buchan, Russell. "Cyber Attacks: Unlawful Uses of Force or Prohibited Interventions?", **Journal of Conflict & Security Law**, Cilt:17, Sayı:2, 2012, s. 211-227.

Buyuran, Abdullah Ahmet. **Devlet Başarısızlığı, Egemen Eşitlik ve Uluslararası Hukukta Müdahale**, (Yayınlanmamış Doktora Tezi), Millî Savunma Üniversitesi Atatürk Stratejik Araştırmalar ve Lisansüstü Eğitim Enstitüsü, İstanbul, 2023.

Carr, Jeffrey. **Inside Cyber Warfare: Mapping the Cyber Underworld**, O'Reilly Media, 2012.

Cerf, Vinton G. ve Robert E. Kahn. "A Protocol for Packet Network Intercommunication", **IEEE Transactions on Communications**, Cilt:22, Sayı:5, 1974, ss. 637-648.

Choucri, Nazli. **Cyberpolitics in International Relations**, MIT Press, London, 2012.

Cin, Gökhan ve Hasan Hüseyin Tekin. "Rusya'nın Hibrit Savaş Kapasitesinin Kırım ve Donbas Vakaları Üzerinden Analizi", **Güvenlik Stratejileri Dergisi**, Cilt:17, Sayı:37, 2021, ss. 203-246.

Civelek, Mustafa Emre. **İnternet Çağı Dinamikleri**, Beta Yayıncılık, İstanbul, 2009.

Clark, David D. ve Susan Landau. "Untangling Attribution", **Harvard National Security Journal**, Cilt:2, Sayı:2, 2011, ss. 323-352.

Clark, David. "Characterizing Cyberspace: Past, Present and Future", **MIT CSAIL**, Version 1.2, 2010.

Clarke, Richard A. ve Robert K. Kanke. **Siber Savaş (Cyber War)**, Çev. Murat Erduran, İstanbul Kültür Üniversitesi Yayınları, 2011.

Coburn, Andrew, Éireann Leverett ve Gordon Woo. **Solving Cyber Risk: Protecting Your Company and Society**, Wiley, New Jersey, 2019.

Cohen-Almagor, Raphael. "Internet History", **International Journal of Technoethics**, Cilt:2, Sayı:2, 2011, ss. 45-64.

Collins, Sean ve Stephen McCombie. "Stuxnet: The Emergence of A New Cyber Weapon and Its Implications", **Journal of Policing, Intelligence and Counter Terrorism**, Cilt:7, Sayı:1, 2012, ss. 80-91.

Çakmak, Cenap. **Uluslararası Hukuk: Giriş, Teori ve Uygulama**, Ekin Yayınevi, Bursa, 2014.

Çelik, Soner ve Barış Çeliktaş. "Güncel Siber Güvenlik Tehditleri: Fidye Yazılımlar", **Cyberpolitik Journal**, Cilt:3, Sayı:5, 2018, ss. 105-132.

Çelik, Şener. "Stuxnet Saldırısı ve ABD'nin Siber Savaş Stratejisi: Uluslararası Hukukta Kuvvet Kullanmaktan Kaçınma İlkesi Çerçevesinde Bir Değerlendirme, **Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi**, Cilt:15, Sayı:1, 2013, ss. 137-175.

Çırak, Bekir ve Abdülkadir Yörük. "Mekatronik Biliminin Öncüsü İsmail El - Cezeri", **Siirt Üniversitesi Sosyal Bilimler Enstitüsü Dergisi**, Sayı:4, 2015, ss. 175-194.

Çifci, Hasan. **Her Yönüyle Siber Savaş**, 2. Basım, TÜBİTAK Yayınları, Ankara, 2017.

Çölgeçen, Mutlu. **Siber Savaş: Kıyametin İlk Halkası**, Arşiv Kitapları, Ankara, 2002.

Darıcılı, A. Burak. "Rusya Federasyonu Kaynaklı Olduğu İddia Edilen Siber Saldırıların Analizi", **U. Ü. Sosyal Bilimler Enstitüsü Dergisi,** Cilt:7, Sayı:2, 2014, ss. 1-16.

Delerue, François. **Cyber Operations and International Law**, Cambridge University Press, United Kingdom, 2020.

DeSimone, Antonio ve Nicholas Horton. **Sony's Nightmare Before Christmas: The 2014 North Korean Cyber Attack on Sony and Lessons for US Government Actions in Cyberspace**, The Johns Hopkins University Applied Physics Laboratory LLC, Laurel, 2017.

Dinstein, Yoram. **War, Aggression and Self-Defence**, 4. Baskı, Cambridge University Press, United Kingdom, 2005.

DOD Dictionary of Military and Associated Terms.

Dörr, Oliver ve Kirsten Schmalenbach (Ed.). **Vienna Convention on the Law of Treaties: A Commentary**, 2. Baskı, Springer, Germany, 2018.

Durmaz, Didem. "İnsancıl Hukukun Orantılılık İlkesi Çerçevesinde Tali Hasar Doktrinine Genel Bir Bakış", **Antalya Bilim Üniversitesi Hukuk Fakültesi Dergisi**, Cilt:10, Sayı:20, 2022, ss. 213-238.

Emir, Buğrahan. **Uluslararası İlişkilerin Kuramsal Çerçevesi ve Siber Güvenlik Kavramının Analizi**, (Yayınlanmamış Yüksek Lisans Tezi), Karadeniz Teknik Üniversitesi Sosyal Bilimler Enstitüsü, Trabzon, 2020.

Endicott, Timothy. "The Logic of Freedom and Power", **The Philosophy of International Law**, Ed. Samantha Besson ve John Tasioulas, Oxford University Press, Oxford, 2010, ss. 245-260.

Erdem, Tolga. **21. Yüzyılda Uluslararası İlişkilerde Yeni Güç Rekabet Sahası: Siber Uzay**, (Yayınlanmamış Doktora Tezi), Trakya Üniversitesi Sosyal Bilimler Enstitüsü, Edirne, 2020.

Ereker, Fulya A.. "İlkçağlardan Günümüze Haklı Savaş Kavramı, **Uluslararası İlişkiler Dergisi**, Cilt:1, Sayı:3, 2004, ss. 1-36.

Eren, M. Yusuf. "Uluslararası Hukukta Savaşa Varmayan Kuvvet Kullanma Yolları", **İnönü Üniversitesi Hukuk Fakültesi Dergisi**, Cilt:3, Sayı:2, 2012, ss. 229-259.

Erkiner, Hakkı Hakan. "Rusya-Ukrayna Savaşı Dairesinde Uluslararası Hukuk Meseleleri", **Uluslararası Akdeniz Hukuku Kongresi 2022: Akdeniz Üniversitesi Hukuk Fakültesi'nin Kuruluşunun 30. Yılı Anısına**, Adalet Yayınevi, Ankara, 2022, ss. 347-398.

FBI National Press Office. **Update on Sony Investigation**, 2014, https://www.fbi.gov/news/press-releases/update-on-sony-investigation (08.09.2023).

Garber, Lee. "Melissa Virus Creates a New Type of Threat", **Computer**, Cilt:32, Sayı:6, 1999, ss. 16-19.

Geers, Kenneth. “Russian Introduction: Cyber War in Perspective”, **Cyber War in Perspective: Russian Aggression against Ukraine**, Ed. Kenneth Geers, NATO CCDCOE Publications, Tallinn, 2015, ss. 13-18.

Geray, Haluk. **İletişim ve Teknoloji**, Ütopya Yayınları, Ankara, 2002.

Gibson, William. **Burning Chrome**, Yeniden Baskı, HarperCollins Publishers, Scotland, 2003.

Gibson, William. **Neuromancer**, Elektronik Baskı, ACE Books by ACE Publishing Group – Penguin Putnam Inc., Newyork, 2003.

Goodman, Marc. **Future Crimes**, Penguin Random House, London, Great Britain, 2015.

Graham, James Richard Howard ve Ryan Olson (Ed.). **Cyber Security Essentials**, CRC Press, 2011.

Green, James. **The International Court of Justice and Self-Defence in International Law**, Hart Publishing, Oregon, 2009, s. 61.

Gündüz, Aslan. **Milletlerarası Hukuk**, Ed. Reşat Volkan Günel, 11. Baskı, Savaş Yayınevi, Ankara, 2021.

Güneş, Mustafa ve Ahmet Alabacak. “Bilgisayar Virüsleri”, **D.E.Ü. İ.İ.B.F. Dergisi**, Cilt:11, Sayı:2, 1996, ss. 239-248.

Güntay, Vahit. “Siber Güvenliğin Uluslararası Politikada Etki Aracına Dönüşmesi ve Uluslararası Aktörler”, **Güvenlik Stratejileri Dergisi**, Cilt:14, Sayı:27, 2018, ss. 79-113.

Güreşci, Ramazan. “Siber Saldırıların Uluslararası Hukuktaki Güç Kullanımı Kapsamında Değerlendirmesi”, **Savunma Bilimleri Dergisi**, Cilt:18, Sayı:1, 2019, ss. 75-98.

Güven, Ferit. **Siber Saldırılar ve Türk Kamu Yönetiminin Çözümleri**, (Yayınlanmamış Doktora Tezi), Süleyman Demirel Üniversitesi Sosyal Bilimler Enstitüsü, Isparta, 2022.

Haggard, Stephan ve Jon R. Lindsay. “North Korea and the Sony Hack: Exporting Instability Through Cyberspace”, **Asia Pacific Issues**, Sayı:117, 2015, ss. 1-8.

Hearn, Kay, Patricia A. H. Williams ve Rachel J. Mahncke. “International Relations and Cyber Attacks: Official and Unofficial Discourse”, **11th Australian Information Warfare and Security Conference**, Edith Cowan University, Perth Western Australia, 2010, ss. 7-12.

Hemsley, Kevin ve Ronald Fisher. “A History of Cyber Incidents and Threats Involving Industrial Control Systems”, **12. International Conference on Critical Infrastructure Protection (ICCIP)**, 2018, ss. 215-242.

Herzog, Stephen. “Ten Years After the Estonian Cyberattacks: Defense and Adaptation in the Age of Digital Insecurity”, **Georgetown Journal of International Affairs,** Cilt:18, Sayı:3, 2017, ss. 67-78.

Hobbes, Thomas. **Leviathan**, Çev. Semih Lim, 6. Baskı, Yapı Kredi Yayınları, İstanbul, 2007.

Hollis, Duncan B.. “An e-SOS for Cyberspace”, **Harvard International Law Journal**, Cilt:52, Sayı:2, 2011, ss. 373-432.

Independent International Fact-Finding Mission on the Conflict in Georgia, Report, Volume II, 2009, https://www.mpil.de/files/pdf4/IIFFMCG_Volume_II1.pdf (03.09.2023).

International Committee of the Red Cross. **International Humanitarian Law: Answers to your Questions**, ICRC Press, Switzerland, 2023.

International Committee of the Red Cross. **The Geneva Conventions of 12 August 1949**, https://www.icrc.org/en/doc/assets/files/publications/icrc-002-0173.pdf (03.02.2024).

International Law Commision. **Responsibility of States for Internationally Wrongful Acts**, A/56/49, 2001, https://legal.un.org/ilc/texts/instruments/english/draft_articles/9_6_2001.pdf (11.01.2022).

Jaitner, Margarita Levin. "Russian Information Warfare: Lessons from Ukraine", **Cyber War in Perspective: Russian Aggression against Ukraine**, Ed. Kenneth Geers, NATO CCDCOE Publications, Tallinn, 2015, ss. 87-94.

Jensen, Eric Talbot. "The Tallinn Manual 2.0: Highlights and Insights", **Georgetown Journal of International Law**, Cilt:48, 2017, ss. 735-778.

Kafadar, Muhammed Fatih. "Uluslararası Hukukta Devletlerin Sorumluluğu Bağlamında Siber Saldırıların Atfedilebilirliği Meselesi", **Galatasaray Üniversitesi Hukuk Fakültesi Dergisi**, Sayı:2, 2020, ss. 1027-1054.

Kanburoğlu, Ömer Lütfi. "Önleyici Harekât Stratejileri ve ABD", 2012, http://www.kanburoglu.com/makale153.htm (05.01.2022).

Kara, Mahruze. **Siber Saldırılar – Siber Savaşlar ve Etkileri**, (Yayınlanmamış Yüksek Lisans Tezi), İstanbul Bilgi Üniversitesi Sosyal Bilimler Enstitüsü, İstanbul, 2013.

Karagiannis, Emmanuel. "The 2008 Russian-Georgian War via the Lens of Offensive Realism", **European Security**, Cilt:22, 2013, ss. 74-93.

Keleştemur, Saim Atalay. **Siber İstihbaratın Kamu Güvenliği İçin Rolü ve Önemi**, (Yayınlanmamış Yüksek Lisans Tezi), İstanbul Gedik Üniversitesi Sosyal Bilimler Enstitüsü, İstanbul, 2018.

Kılınç, Doğan. "Türk Hukukunda ve Mukayeseli Hukukta İnternet Sitelerine Erişimin Engellenmesi ve İfade Hürriyeti", **Gazi Üniversitesi Hukuk Fakültesi Dergisi**, Cilt:14, Sayı:2, 2010, ss. 407-454.

Klimburg, Alexander. "Mobilising Cyber Power", **Survival**, Cilt:53, Sayı:1, 2011, ss. 41-60.

Knapp, Eric D. ve Joel Thomas Langill. **Industrial Network Security**, Second Edition, Elsevier Inc., Waltham, 2015.

Kocabay, Hüseyin. **Uluslararası Hukukta Kuvvet Kullanımı**, (Yayınlanmamış Yüksek Lisans Tezi), Abant İzzet Baysal Üniversitesi Sosyal Bilimler Enstitüsü, Bolu, 2014.

Kofman, Michael, Katya Migacheva, Brian Nichiporuk, Andrew Radin, Olesya Tkacheva ve Jenny Oberholtzer. **Lessons from Russia's Operations in Crimea and Eastern Ukraine**, RAND Corporation, California, 2017.

Korhan, Sevda. "Siber Uzayda Aktör - Güç İlişkisi", **Cyberpolitik Journal**, Cilt:2, Sayı:4, 2018, ss. 75-103 (Aktör - Güç İlişkisi).

Korhan, Sevda. **Siber Uzayda Uluslararası İlişkilerin Değişen Parametreleri**, (Yayınlanmamış Yüksek Lisans Tezi), Selçuk Üniversitesi Sosyal Bilimler Enstitüsü, Konya, 2018 (Parametreler).

Krishna-Hensel, Sai Felicia. "Preface", **Power and Security in the Information Age: Investigating the Role of the State in Cyberspace**, Ed. Myriam Dunn Cavelty, Victor Mauer ve Sai Felicia Krishna-Hensel, Ashgate Publishing, 2007, ss. ix-xiv.

Lakomy, Miron. "The Significance of Cyberspace in Canadian Security Policy", **Central European Journal of International and Security Studies**, Cilt:7, Sayı:2, 2013, ss. 102-119.

League of Nations. **General Treaty for Renunciation of War as an Instrument of National Policy**, 1929, https://treaties.un.org/doc/Publication/UNTS/LON/Volume%2094/v94.pdf (12.10.2023).

Léonet, Louis. **Contextual Cyber Securitisation: A Case Study of Russian Cyberattacks against Ukraine**, (Yayınlanmamış Yüksek Lisans Tezi), Leiden Üniversitesi, Hollanda.

Li, Sheng. "When Does Internet Denial Trigger the Right of Armed Self-Defense?", **Yale Journal of International Law,** Sayı:38, 2013, ss. 179-216.

Libicki, Martin C.. **Cyberdeterrence and Cyberwar**, RAND Corporation, Santa Monica, 2009.

Mandel, Robert. **Optimizing Cyberdeterrence: A Comprehensive Strategy for Preventing Foreign Cyberattacks**, Georgetown University Press, Washington, 2017.

Mares, Miroslav ve Veronika Netolicka. "Georgia 2008: Conflict Dynamics in the Cyber Domain, **Strategic Analysis,** Cilt:44, 2020, ss. 224-240.

Markoff, John. “A Silent Attack but Not a Subtle One”, **The New York Times,** 2010, https://www.nytimes.com/2010/09/27/technology/27virus.html (28.12.2022).

Medvedev, Sergei A.. **Offense–Defense Theory Analysis of Russian Cyber Capability**, Calhoun: The Naval Postgraduate School (NPS) Institutional Archive, California, 2015.

Moynihan, Harriet. “The Application of International Law to State Cyberattacks: Sovereignty and Non-intervention”, **Chatham House**, 2019, ss. 1-60.

Mumcu, Şinasi Özgür. “Barış Zamanı Siber Operasyonların Egemenlik İlkesi Bakımından Hukuki Rejimi”, **Bahçeşehir Üniversitesi Hukuk Fakültesi Dergisi**, Cilt:16, Sayı:201-202, 2021, ss. 995-1012.

Nguyen, Reese. “Navigating Jus Ad Bellum in the Age of Cyber Warfare”, **California Law Review**, Cilt:101, Sayı:4, 2013, ss. 1079-1130.

Nourian, Arash ve Stuart Madnick. “A Systems Theoretic Approach to the Security Threats in Cyber Physical Systems Applied to Stuxnet”, **IEEE Transactions on Dependable and Secure Computing**, Cilt:15, Sayı:1, 2018, ss. 2-13.

Orallı, Levent Ersin. “Uluslararası Hukukta Ve BM Sisteminde Askeri Müdahale Olgusu”, **Tesam Akademi Dergisi**, Cilt:1, Sayı:1, 2014, ss. 102-127.

OSCE. Комплекс мер по выполнению Минских соглашений, Minsk, 2015, https://www.osce.org/ru/cio/140221 (12.10.2023).

OSCE. Протокол о результатах консультаций Трехсторонней контактной группы, Минск, 5 сентября 2014 г., Minsk, 2014, https://www.osce.org/ru/home/123258 (12.10.2023).

Ottis, Rain. “Analysis of the 2007 Cyber Attacks Against Estonia from the Information Warfare Perspective”, **Proceedings of the 7th European Conference on Information Warfare and Security**, Plymouth, Reading: Academic Publishing Limited, 2008, ss. 163-168.

Ottis, Rain. “Proactive Defense Tactics Against On-Line Cyber Militia”, **Proceedings of the 9th European Conference on Information Warfare and Security (ECIW 2010)**, 2010, ss. 233-237.

Owolabi, Kudirat Magaji W.. “The Principle of The Common Heritage of Mankind”, **Nnamdi Azikiwe University Journal of International Law and Jurisprudence**, Cilt:4, 2013, ss. 51-56.

Öğün, Mehmet Nesip ve Adem Kaya. “Siber Güvenliğin Milli Güvenlik Açısından Önemi ve Alınabilecek Tedbirler”, **Güvenlik Stratejileri Dergisi**, Y. 9, Sayı:18, 2013, ss. 145-181.

Özman, M. Aydoğan. “Devletlerin Egemenliği ve Milletlerarası Teşekküller”, **Ankara Üniversitesi Hukuk Fakültesi Dergisi**, Cilt:21, Sayı:1, 1964, ss. 53-121.

Pazarcı, Hüseyin. **Uluslararası Hukuk**, 15. Baskı, Turhan Kitabevi, Ankara, 2016.

Polat, Doğan Şafak. “Nato’nun Yeni Operasyon Alanı: Siber Uzay”, **Güvenlik Bilimleri Dergisi**, UGK Özel Sayısı, 2020, ss. 135-158.

Richet, Jean-Loup. **Cybersecurity Policies and Strategies for Cyberwarfare Prevention**, Information Science Reference, Pennsylvania, 2015.

Roscini, Marco. “Cyber Operations as a Use of Force”, **Research Handbook on International Law and Cyberspace**, Ed. Nicholas Tsagourias and Russell Buchan, Edward Elgar Publishing, United Kingdom, 2015, ss. 233-254.

Rousseau, Jean-Jacques. **Toplum Sözleşmesi**, Çev. Vedat Günyol, 9. Basım, Türkiye İş Bankası Kültür Yayınları, İstanbul, 2012.

Schmitt, Michael N. ve Liis Vihul. "Respect for Sovereignty in Cyberspace", **Texas Law Review**, Cilt:95, Sayı:7, 2017, ss. 1639-1671.

Schmitt, Michael N.. "Russian Cyber Operations And Ukraine: The Legal Framework", **Lieber Institute West Point**, 2022, https://lieber.westpoint.edu/russian-cyber-operations-ukraine-legal-framework/ (09.10.2023).

Schmitt, Michael N.. "The Law of Cyber Warfare: Quo vadis?", **Stanford Law & Policy Review**, Sayı:25, 2014, ss. 269-300.

Schmitt, Michael N.. **Computer Network Attack and The Use of Force in International Law: Thoughts on A Normative Framework**, Research Publication 1 Information Series, Institute for Information Technology Applications, USAF Academy, Colorado, 1999.

Schmitt, Michael. "International Law and Cyber Attacks: Sony v. North Korea", **Just Security**, 2014, https://www.justsecurity.org/18460/international-humanitarian-law-cyber-attacks-sony-v-north-korea/ (08.09.2023).

Sertçelik, Aşır. "Siber Olaylar Ekseninde Siber Güvenliği Anlamak", **Medeniyet Araştırmaları Dergisi**, Cilt:2, Sayı:3, 2015, ss. 25-42.

Shanghai Cooperation Organization. **Agreement on Cooperation in Ensuring International Information Security between the Member States of the Shanghai Cooperation Organization**, 2009.

Shanghai Cooperation Organization. **Agreement on Cooperation in Ensuring International Information Security between the Member States of the Shanghai Cooperation Organization, ANNEX 1 to the Agreement on Cooperation in the**

Field of Ensuring International Information Security among the Member States of the Shanghai Cooperation Organization, ss. 9-10, 2009. (ANNEX 1).

Sharp, Walter Gary. "The Past, Present, and Future of Cybersecurity", Journal Of National Security Law & Policy, Cilt:4, Sayı:13, 2010, ss. 13-26.

Shaw, Malcolm N.. **International Law**, 8. Baskı, Cambridge University Press, United Kingdom, 2017.

Sigholm, Johan. "Non-State Actors in Cyberspace Operations", **Journal of Military Studies**, Cilt:4, Sayı:1, 2016, ss. 1-37.

Slevin, James. **The Internet and Society**, Polity Press, Oxford, 2000.

Springer, Paul J.. **Encyclopedia of Cyber Warfare**, ABC-CLIO, California, 2017.

Steed, Brian L.. **Piercing the Fog of War: Recognizing Change on the Battlefield: Lessons from Military History 216 BC through Today**, Zenith Press, Mineneapolis, 2009.

Stinissen, Jan. "A Legal Framework for Cyber Operations in Ukraine", **Cyber War in Perspective: Russian Aggression against Ukraine**, Ed. Kenneth Geers, NATO CCDCOE Publications, Tallinn, 2015, ss. 123-134.

Sullivan, Clare. "The 2014 Sony Hack and the Role of International Law", **Journal of National Security Law & Policy**, Sayı:8, 2016, ss. 437-468.

Sur, Melda. **Uluslararası Hukukun Esasları**, 15. Baskı, Beta Yayıncılık, İstanbul, 2021.

Süleymanova Rafael, Günay. **A Comparative Analysis of Major Russian Cyber Attacks in the Post-Cold War Era**, (Yayınlanmamış Yüksek Lisans Tezi), Bahçeşehir Üniversitesi Lisansüstü Eğitim Enstitüsü, İstanbul, 2022.

Şafak, Erdi. "Uluslararası Hukukta Değişen Güvenlik Algısı Ve Saldırı Suçu Bağlamında Siber Saldırılar", **Selçuk Üniversitesi Hukuk Fakültesi Dergisi,** Cilt:28, Sayı:1, 2020, ss. 127-160.

T. C. Dışişleri Bakanlığı. **Şanhay İşbirliği Örgütü (ŞİÖ)**, https://www.mfa.gov.tr/sanghay-isbirligi-orgutu.tr.mfa, (02.12.2021).

T.C. Dışişleri Bakanlığı. **24 Şubat 2022, Rusya Federasyonu Tarafından Ukrayna'ya Yönelik Başlatılan Askeri Operasyon Hk.**, 62 Numaralı Resmî Açıklama, Ankara, 2022.

T.C. Ulaştırma ve Altyapı Bakanlığı. **Ulusal Siber Güvenlik Stratejisi ve Eylem Planı 2020-2023**, Ankara, 2020.

Tabansky, Lior ve Isaac Ben Israel. **Cybersecurity in Israel**, Springer, Switzerland, 2015.

Taşdemir, Fatma. "Uluslararası Anarşiye Giden Yol: Uluslararası Hukuk Açısından Önleyici Meşru Müdafaa Hakkı", **Uluslararası Hukuk ve Politika Dergisi**, Cilt:2, Sayı:5, 2006, ss. 75-89.

Tezcan, Durmuş. "Bozkurt-Lotus Davasının Uluslararası Hukuktaki Önemi ve Yeri, **Çağdaş Türkiye Tarihi Araştırmaları Dergisi**, Cilt:2, Sayı:4, 1994, ss. 267-274.

The International Group of Experts at the Invitation of The NATO Cooperative Cyber Defence Centre of Excellence. **Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations**, Ed. Michael N. Schmitt ve Liis Vihul, 2. Baskı, Cambridge University Press, 2017 (Tallinn Kılavuzu).

The United States Army's. **Cyberspace Operations Concept Capability Plan 2016-2028**, United States, 2010.

Thornburgh, Tim. "Social Engineering: The "Dark Art"", **1st Annual Conference on Information Security Curriculum Development**, 2004, ss. 133-135.

Tikk, Eneken, Kadri Kaska ve Liis Vihul. **International Cyber Incidents: Legal Considerations**, Cooperative Cyber Defense Centre of Excellence, Tallinn, 2010.

Tokdaş, Abdullah. **Siber Güvenlik ve Uluslararası İlişkiler**, (Yayınlanmamış Yüksek Lisans Tezi), Selçuk Üniversitesi Sosyal Bilimler Enstitüsü, Konya, 2018.

Trautman, Lawrence J. ve Peter C. Ormerod. "Industrial Cyber Vulnerabilities: Lessons from Stuxnet and the Internet of Things", **University of Miami Law Review**, Cilt:72, Sayı:3, 2018, ss. 761-826.

Tsagourias, Nicolas. "The Tallinn Manual on the International Law Applicable to Cyber Warfare: A Commentary on Chapter II - The Use of Force", **Yearbook of International Humanitarian Law**, Ed. Terry D Gill, Cilt:15, 2014, ss. 19-43.

Uluslararası Adalet Divanı, **Kongo Demokratik Cumhuriyeti'ndeki Silahlı Faaliyetler Davası**, 2005, https://www.icj-cij.org/public/files/case-related/116/116-20051219-JUD-01-00-EN.pdf (03.12.2023).

Uluslararası Adalet Divanı, **Nükleer Silah Tehdidinin veya Kullanımının Yasallığı Hakkında Danışma Görüşü**, 1996, https://www.icj-cij.org/public/files/case-related/95/095-19960708-ADV-01-00-EN.pdf (10.01.2022).

Uluslararası Adalet Divanı. **Korfu Boğazı Davası**, 1949, (Korfu Boğazı Kararı) https://www.icj-cij.org/public/files/case-related/1/001-19490409-JUD-01-00-EN.pdf (05.01.2022).

Uluslararası Adalet Divanı. **Nikaragua'ya Karşı Askeri ve Bölgesel Faaliyetler Davası**, 1986, (Nikaragua Kararı), https://www.icj-cij.org/public/files/case-related/70/070-19860627-JUD-01-00-EN.pdf (31.12.2021).

United Nations General Assembly Security Council. **Letter dated 27 June 2014 from the Permanent Representative of the Democratic People's Republic of Korea to the United Nations addressed to the Secretary-General**, A/68/934–S/2014/451, 2014.

United Nations General Assembly, **Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security**, A/70/174, 2015, s. 12, https://digitallibrary.un.org/record/799853/files/A_70_174-EN.pdf (11.01.2022).

United Nations General Assembly. **Declaration on Principles of International Law concerning Friendly Relations and Cooperation among States in accordance with the Charter of the United Nations**, 2625(XXV), 1970, https://digitallibrary.un.org/record/202170/files/A_RES_2625%28XXV%29-EN.pdf (31.12.2021).

United Nations General Assembly. **Declaration on the Inadmissibility of Intervention in the Domestic Affairs of States and the Protection of Their Independence and Sovereignty**, 2131(XX), 1965, https://digitallibrary.un.org/record/203886/files/A_RES_2131%28XX%29-EN.pdf (31.12.2021).

United Nations General Assembly. **Declaration on the Inadmissibility of Intervention and Interference in the Internal Affairs of States**, 36/103, 1981, https://digitallibrary.un.org/record/27066/files/A_RES_36_103-EN.pdf (31.12.2021).

United Nations General Assembly. Definition of Aggression, 3314(XXIX), 1974, https://digitallibrary.un.org/record/190983/files/A_RES_3314%28XXIX%29-EN.pdf (05.01.2022).

United Nations General Assembly. **Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security**, A/68/98, 2013, s. 8, https://digitallibrary.un.org/record/753055/files/A_68_98-EN.pdf (31.12.2021).

United Nations General Assembly. **Territorial integrity of Ukraine**, 68/262, 2014, https://documents-dds-ny.un.org/doc/UNDOC/GEN/N13/455/17/PDF/N1345517.pdf?OpenElement (03.10.2023).

United Nations. **Summaries of Judgments, Advisory Opinions and Orders of the Permanent Court of International Justice**, 2012, (USAD Kararları), https://legal.un.org/PCIJsummaries/documents/english/PCIJ_FinalText.pdf (03.12.2023).

United Nations. **United Nations Charter**, https://www.un.org/en/about-us/un-charter/full-text (03.12.2023).

Uzun, Elif. "Haklı Savaş Düşüncesinin Batılı Kökleri: İlk Çağlardan Yirminci Yüzyıla Jus Ad Bellum Kavramı", **Uluslararası Hukuk ve Politika Dergisi**, Cilt:6, Sayı:21, 2010, ss. 19-33.

Weimann, Gabriel. "Cyberterrorism: How Real is the Threat?" **United States Institute of Peace**, Special Report 119, 2004, ss. 1-12.

Whyte, Christopher ve Brian Mazanec. **Understanding Cyber Warfare: Politics, Policy and Strategy**, Routledge, New York, 2018.

Wiener, Norbert. **Cybernetics or Control and Communication in the Animal and Machine**, 2. Baskı, MIT Press, London, 2019.

Williams, Martyn. "Analysis: Why North Korea might not be to blame for the Sony Pictures hack", **The Guardian**, https://www.theguardian.com/world/2014/dec/02/-sp-north-korea-hack-sony (08.09.2023).

Wilson, Clay. "Cyber Crime", **Cyberpower and National Security**, (Ed. Franklin D. Kramer, Stuart H. Starr ve Larry Wentz), National Defense University Press, Washington, 2009, ss. 415-437.

Yaşın, Abdullah. "Ebul-İz'in Bilime Katkıları", **Bilim Düşünce ve Sanatta Cizre (Uluslararası Bilim Düşünce ve Sanatta Cizre Sempozyumu Bildirileri)**, 2012, ss. 201-204.

Yayla, Mehmet. "Siber Savaş ve Siber Ortamdaki Kötü Niyetli Hareketlerden Farkı", **Hacettepe Hukuk Fakültesi Dergisi**, Cilt:4, Sayı:2, 2014, ss. 181-200.

Yayla, Mehmet. "Uluslararası Hukukta Siber Saldırılara Karşı Kuvvet Kullanma", **Türkiye Barolar Birliği Dergisi**, Sayı:107, 2013, ss. 199-220.

Yazıcı, Merve. "İlk Modern Siber-Atak: Estonya, **TUİÇ Akademi,** 2015, https://www.tuicakademi.org/ilk-modern-siber-atak-estonya (27.12.2022).

Yener, Yavuz. "8. Yılında Estonya Saldırılarına Çok Boyutlu Bir Bakış", **SiberBülten,** 2014, https://siberbulten.com/siber-saldirilar-2/8-yilinda-estonya-saldirilarina-cok-boyutlu-bir-bakis (27.12.2022).

Yılmaz, Yağmur Ekim. "Milletlerarası Hukukta Kuvvet Kullanma Yasağı Kapsamında Rusya'nın Ukrayna'ya Müdahalesi", **Uluslararası İlişkiler ve Diplomasi Dergisi**, Cilt:5, Sayı:2, 2022, ss. 58-80.