

ULUSLARARASI HUKUK BAĞLAMINDA SİBER SALDIRI VE KKTC ÖRNEĞİ



Yakın
Doğu
Enstitüsü



Yrd. Doç. Dr. Erdi Şafak

ULUSLARARASI HUKUK BAĞLAMINDA SİBER SALDIRI VE KKTC ÖRNEĞİ

Yrd. Doç. Dr. Erdi Şafak

Bu çalışmada yer alan görüşler yazara ait olup Yakın Doğu Üniversitesi'nin kurumsal görüşleri değildir.

Rapor 01 /2021

Yakın Doğu Enstitüsü (YDE)
Near East Institute (NEI)

YDE Rapor 01 / 2021



Editörler:

Yrd. Doç. Dr. Mustafa Çıraklı (Müdür, Yakın Doğu Enstitüsü)
Ercan Çitlioğlu (Başdanışman, Yakın Doğu Enstitüsü)

Copyright @ Yakın Doğu Üniversitesi, 2021

Tüm hakları saklıdır.

Birinci Baskı

ISBN: 978-605-9415-62-0

Kütüphane Katalog Bilgileri

Uluslararası Hukuk Bağlamında Siber Saldırı ve KKTC Örneği

Rapor

Yakın Doğu Enstitüsü Yayınları
Yakın Doğu Üniversitesi Matbaası Lefkoşa/KKTC
Tel: 0392 680 2000 - 321.

Yakın Doğu Enstitüsü (YDE)
Yakın Doğu Üniversitesi Büyük Kütüphanesi, Ofis: 50
Yakın Doğu Bulvarı PK/99138
Lefkoşa/KKTC
Tel: 0392 680 2000 -532.
Email: yde@neu.edu.tr
Web: yde.neu.edu.tr
<http://yde.neu.edu.tr>

Özet

Günümüzde teknolojinin gelişmesiyle birlikte kolaylaşan hayatımız, beraberinde bazı sorunları da gündeme getirmiştir. Özellikle Covid-19 (Coronavirüs) salgını sonrası teknolojiye daha fazla bağımlı hale gelen toplumsal yaşantımız beraberinde hukuksal açıdan bazı konuların tartışılmasına neden olmuştur. Bu bağlamda uluslararası hukukun çalışma alanı ve buna bağlı olarak var olan kurallar da bir takım güncellemeler ihtiyacı hissetmiştir. Özellikle silahlı çatışmalar hukukunda var olan mevcut durumda önemli değişikliklerin yaşandığını söyleyebiliriz. Günümüzde devletler, kara, deniz ve hava kuvvetleri komutanlıklarına, siber savunma komutanlıkları da eklemiş ve ordular siber saldırı ve siber savaş gibi kavramlar üzerinde senaryolar üretmeye başlamıştır. Bu çalışmada olası bir siber savaş senaryosunda uluslararası sistemde tanınmamış bir devlet olan KKTC'nin durumu ve uluslararası hukuk açısından var olan hakları incelenmiştir.

Anahtar Kelimeler: Uluslararası Hukuk, Silahlı Çatışmalar Hukuku, Siber Saldırı, KKTC

Abstract

Technological advances which have brought with them significant advantages to modern life also brought some problems along with them. Especially in the context of the COVID-19 (Coronavirus) epidemic, rendering our lives more dependent on technology, the existing rules of international law regarding technology now require some important updates. This has become more the pertinent with regards to the law of armed conflicts. With technological advances, cyberspace commands have been added to the land, naval and air force commands, and modern armies have started to develop their preparedness relating to scenarios dealing with cyber attacks and cyber warfare. The Turkish Republic of Northern Cyprus as an unrecognized state in the international system offers a unique case study which can contribute to the ongoing discussions on cyber defence and international law. This report examines the existing rights of the TRNC under international law in case of a possible cyber attack.

Keywords: International Law, Law of Armed Conflicts, Cyber Attacks, TRNC

İÇİNDEKİLER

GİRİŞ.....	1
SİBER İLE İLGİLİ GENEL KAVRAMLAR	1
Siber ve Siber Alan.....	1
Siber Saldırı.....	2
Siber Savaş	4
ULUSLARARASI HUKUK BAĞLAMINDA SİBER SALDIRILAR.....	7
Siber Saldırı ve Kuvvet Kullanma Yasağı.....	7
Siber Saldırı Suçu	8
Siber Saldırlara Karşı Meşru Müdafaa Hakkının Kullanımı	10
KKTC'YE YÖNELİK BİR SİBER SALDIRIDA KKTC DEVLETİNİN ULUSLARARASI HUKUK AÇISINDAN DURUMU	11
KKTC'nin Uluslararası Alanda Tanınmama Sorunu.....	11
Siber Saldırıları ile İlgili Uluslararası Antlaşmalara KKTC'nin Taraf Olabilme Durumu	14
Siber Saldırıları ile İlgili KKTC Devleti Mahkemelerince Verilmiş Kararların Tanınması Meselesi	15
SONUÇ	16
KAYNAKÇA.....	17

GİRİŞ

İnternetin kullanımının yaygınlaşması ile birlikte, iletişim imkân ve kabiliyetlerinde görülen gelişim, teknolojik yenilikler ile birlikte internet üzerinden yayılan zararlı yazılımlardaki artış “siber ortam” ve “siber güvenlik” şeklinde tanımlanan yeni kavramların tartışılmasına neden olmuştur.¹ Teknolojinin gelişmesi ile paralel olarak gelişen “siber saldırı” imkânları ise siber ortamda hem bireyler açısından hem de devletler açısından önemli bir sorun haline almıştır. Estonya, Gürcistan ve son olarak İran’da yaşanan “siber saldırı” vakaları, konunun devletlerin ya da bireylerin sorumluluğu, kuvvet kullanma, meşru müdafaa ve saldırı suçu gibi kavramlar çerçevesinde çalışılması ihtiyacını gündeme getirmiştir. Son dönemde birçok devlet kara, hava ve deniz kuvvetleri komutanlıklarına ek olarak, siber komutanlıklar kurma yoluna gitmişlerdir. Kurulan siber ordular çerçevesinde gerçekleşecek bir siber savaş durumunda, uluslararası hukuk kurallarının ne şekilde uygulanacağı önemli bir sorun haline almıştır.

Günümüzde yaşanabilecek olası bir siber savaş durumunda Kuzey Kıbrıs Türk Cumhuriyeti’nin (KKTC) savaşın taraflarından biri olması önemli bir sorun teşkil etmektedir. Başka bir ifadeyle siber savaş ya da siber saldırılar ile ilgili var olan antlaşmalara KKTC’nin taraf olması meselesi de yine günümüz şartlarında bazı sorunları beraberinde getirecektir. Bu çalışma KKTC’ye Devletler ya da Devletlerin desteklediği bireyler tarafından gerçekleştirilecek olası bir siber saldırı durumunda KKTC’nin uluslararası hukuk açısından var olan haklarının irdelenmesi üzerine olacaktır.

SİBER İLE İLGİLİ GENEL KAVRAMLAR

Siber ve Siber Alan

Bilim dünyasındaki gelişme bilgiyi, fiziksel dünyadan elektronik dünyaya doğru hızlı bir şekilde taşımaktadır. Esasen “sibernetik²” (cybernetics) kelimesinin bir ön eki olan “siber” sözcüğü, aynı zamanda kelimeyi kısaltmak amacıyla da kullanılmaktadır.³ “Sibernetik” kavramı Türk Dil Bilgisi sözlüğünde “Güdüm Bilimi” olarak ifade edilmekte olup, “Güdüm Bilimi” ise “Bilişimde, bir olaylar dizisini, bir süreci veya bir aracı yöneltme ve düzenlemeye ilgili işlevlerin bütünü” olarak ifade edilmektedir.⁴

¹ Ali Burak Darcılı, *Siber Uzak ve Siber Güvenlik – ABD ve Rusya Federasyonu’nun Siber Güvenlik Stratejilerinin Karşılaştırılmalı Analizi*, Dora Yayıncılık, Bursa, 2017, s.1.

² “Sibernetik” kelime ve anlam olarak Yunanca da “kübernetes”ten gelmektedir. Eski Yunancada “kübernetes”, “gemiyi yöneten pilot”, yani kısaca “dümenci” demektir. Almanlar ve Avusturyalılar Sibernetik kelimesini “kibernetik” olarak yazıp okumakta, İngilizler ve Amerikalılar ise “cybernetics” olarak yazmakta ve “saybernetiks” olarak okumaktadırlar. Türkçede ise, dilimize daha yakın olan Fransızca okunuş şekli ile “Sibernetik” demektir. Sibernetik kelimesi ile daha detaylı bilgi için bakınız: Toygar Akman, *Sibernetik*, Kaktüs Yayınları, İstanbul, 2003; Norbert, Weiner, *Sibernetik*, Çeviren: İbrahim Keskin, SAY Kitap Pazarlama, İkinci Basım, İstanbul, 1982; Ayhan Songar, *Sibernetik*, Temel Matbaa ve Ambalaj Sanayi, İstanbul, 1980.

³ Haydar/Demir Çakmak, Cenker Korhan, “Siber Dünyadaki Tehditler ve Kavramlar”, *Suç, Terör ve Savaş Üçgeninde Siber Dünya*, Ed. Haydar – Altunok Çakmak, Taner Barış Platin Yayınevi, Ankara, 2009, s.25.

⁴ Detaylı Bilgi İçin Bakınız: Türk Dil Kurumu Sözlüğü, <https://sozluk.gov.tr/>.

Siber alan ise dünyadaki tüm bilgisayar ağları ile onların bağlı olduğu ve kontrol ettiği her şeydir.⁵ Siber alan (cyber space) kelimesi birbiriyle bağlantılı sistem, yazılım, donanım ve insanların iletişim ve/veya etkileşimde bulundukları soyut veya somut alanı tarif etmek için kullanılmaktadır.⁶ 2013 yılında Türkiye'nin Ulusal Siber Güvenlik Stratejisi ve Eylem Planında siber alan: “*Tüm dünyaya ve uzaya yayılmış durumda bulunan bilişim sistemlerinden ve bunları birbirine bağlayan ağlardan oluşan ortam*”, olarak tanımlanmıştır.⁷

Uluslararası hukuk terminolojisinde siber alanın karşılığı tam olarak bulunmamaktadır. Ancak siber alan uluslararası hukuk kurallarının dışındadır denilemez. Zira bir devletin kendi toprakları üzerinde siber altyapıyı ve siber faaliyetleri kontrol edebilme hakkının kaynağı egemenlikten kaynaklanmaktadır. Buradan devamlı, bir devletin karasal topraklarında, iç sularında, deniz yetki alanında (‘deniz yatağı’⁸ dahil) ve ulusal hava sahasında bulunan siber altyapılar o devletin egemenliği altındadır ve devletler siber alandan da sorumludurlar.

Siber Saldırı

Siber alanda, bireylerden geniş çaplı organizasyonlara, terör örgütlerinden devletlere kadar muhtelif kaynaklar tarafından hedef sistemleri bozmaya ve kullanılmaz hale getirmeye yönelik birçok saldırı gerçekleştirilmektedir. İşte bu saldırılar literatürde “*siber saldırı*” olarak ifade edilmektedir. Siber saldırı, “*Siber alanda yer alan bilgileri istismar etmek, bozmak, değiştirmek, sistemlere erişimi engellemek ya da zarar vermek amacıyla siber alanda gerçekleştirilen faaliyetlerdir*”.⁹

⁵ A. Richard, Knake Clarke, Robert K., *Siber Savaş*, İstanbul Kültür Üniversitesi Yayınları, İstanbul, 2011, s.44.

⁶ Fulya Aslay, “Siber Saldırı Yöntemleri ve Türkiye'nin Siber Güvenlik Mevcut Durum Analizi”, *International Journal of Multidisciplinary Studies and Innovative Technologies*, Cilt: 1 No: 1, 2017, s.24. / Nils Melzer, “Cyberwarfare and International Law”, *Ideas For Peace And Security*, <https://unidir.org/files/publications/pdfs/cyberwarfare-and-international-law-382.pdf>. s.5. [Erişim Tarihi: 3 Mart 2021].

⁷ “Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı” Siber Güvenlik Kurulu tarafından 21/12/2012 tarihli toplantıda kabul edilmiş ve Bakanlar Kurulu'nun 20/06/2013 tarihli ve 28683 sayılı kararı ile Resmi Gazetede yayımlanmıştır.

<https://www.btk.gov.tr/uploads/pages/2-1-strateji-eylem-planı-2013-2014-5a3412cf8f45a.pdf>. [Erişim Tarihi: 3 Mart 2021].

⁸ Deniz yatağı devletlerin münhasır ekonomik bölge alanları içerisinde yer almaktadır. Kıyı devleti karasularının ölçülmeye başlandığı hattan itibaren 200 deniz mili içindeki deniz alanlarında, deniz yatağında, toprak altında ayrıca üzerindeki sularda canlı ve canlı olmayan doğal kaynaklar üzerinde bazı ekonomik haklar kullanır.

⁹ Hasan Çifci, *Her Yönüyle Siber Savaş*, TÜBİTAK Yayınları, 2. Basım, Ankara, 2017. s.6; Nils Melzer, “Cyberwarfare and International Law”, *Ideas For Peace And Security*, <https://unidir.org/files/publications/pdfs/cyberwarfare-and-international-law-382.pdf>. s.5 – 6. [Erişim Tarihi: 3 Mart 2021].

Başka bir tanımda ise siber saldırı, “Saldırganlar tarafından bilgi sistemlerinin çalışamaz hale getirilmesi, bilgi sistemlerinin güvenliğinin veya güvenilirliğinin riske atılması, bozulması ve çalınması şeklinde de ifade edilmektedir”.¹⁰

Siber saldırılar verilere ya da kontrol sistemlerine yönelik olmak üzere iki şekilde meydana gelmektedir. Bilginin çalınması ya da bozulması sıklıkla karşılaşılan verilere yönelik eylem türlerindendir. Kontrol sistemleriyle ilgili olanlar ise bir fiziksel alt yapıyı kullanılmaz hale getirme ya da manipüle etmeyi kapsamaktadır. Örneğin 2000 yılında Avustralya’da atık kontrol sistemine giren eski bir çalışan, bir milyon litre katı atığın bir şehrin nehir ve sahil sularına yayılmasına sebep olmuştur. Böylelikle eylemi gerçekleştiren kişi sistemi bilmesinin avantajından faydalanarak belediyedeki amirlerinden “intikamını” almıştır.¹¹

Siber saldırılarda farklı araçlar kullanılmaktadır. Siber saldırıda kinetik güç (yumruk, kılıç, bomba, silah vb.) kullanmak yerine dijital araçlar (bir çeşit bilgisayar hareketi) kullanılır. Bu nokta önemlidir, bir siber saldırı geleneksel saldırıların olağan fiziki ile sınırlı değildir. Siber uzayda bir saldırı, coğrafya ve siyasi sınırla kısıtlanmadan gerçek manada ışık hızıyla hareket edebilmektedir. Fizikten bağımsız olması aynı zamanda, aynı anda birçok yerde olabileceği anlamına gelen birden çok hedefi bir kerede aynı saldırının vurması anlamına da gelmektedir.¹²



Uluslararası sistemde kaydedilen ilk siber saldırılardan biri, Soğuk Savaş sırasında Amerika Birleşik Devletleri (ABD) Başkanı Ronald Reagan’ın 1982 yılında Sibiryadaki Rus boru hattı sistemine yönelik bir SCADA (Supervisory Control and Data Acquisition) saldırısını onaylamasıyla gerçekleşmiştir. Soğuk Savaş gerilimleri bağlamında, boru hattı saldırısı, Sovyetler Birliği’nin gaz arzını bozmak ve Rus ekonomisine ve Batı’dan gelen

¹⁰ Mustafa Canlı, “Siber Güvenlik”, Ankara Siyasal ve Ekonomik Araştırmalar Merkezi Raporu, Ankara, 2013, s.8; Nezir, Akyeşilman, *Disiplinlerarası Bir Yaklaşımla Siber Politika & Güvenlik*, ORION Yayınları, 1. Baskı, Ankara, 2018, s.93 – 94.

¹¹ Demir Çakmak, a.g.e., s.30.; Çifçi, a.g.e., s.6; Akyeşilman, a.g.e., s.93 -95.

¹² Peter Warren ve Friedman Singer, Allan, *Siber Güvenlik ve Siber Savaş*, Buzdağı Yayınları, Ankara, 2015, s.101.

gaz gelirlerine zarar vermek ve böylece gücünü zayıflatmak için özel olarak tasarlanmıştır.¹³

Günümüzde ordu birimleri arasında her türlü bilgi alış-verişi internetten bağımsız, kapalı sistem olan bilgi sistemleri üzerinden yapılmaktadır. Buna ilaveten, uçak, gemi, füze, mühimmat gibi birçok yüksek teknolojiye sahip harp silah ve araçları, koruma kontrol sistemleri, kontrol ihbar ve hava savunma sistemleri bilgisayarlara ve yazılımlara bağımlı olarak çalışmaktadır. Bu durum, askeri sistemleri ve ülke savunmalarını siber saldırılara karşı hassas hale getirmektedir. Bilgi sistemlerine yönelik gerçekleştirilen siber saldırı, bilgisayar ağına girilerek, sistemde istenilen değişiklikleri yapmak suretiyle sistemin çalışma şeklini değiştirmek ya da sistemi tamamen çöktürmek amacıyla yapılmaktadır.¹⁴

Siber Savaş

Uluslararası hukukta savaş kavramı ile ilgili yapılan farklı tanımlar, siber savaş tanımı için de geçerlidir. Siber savaş en genel tanımı ile “devletlerin siber alanda birbirine karşı yürüttüğü siber saldırı faaliyetleridir”.¹⁵ Siber savaş, “kara, hava, deniz ve uzay savaşlarından sonra beşinci savaş alanı” olarak açıklanmaktadır.¹⁶ Siber savaş ile ilgili yapılan tanımlarda dikkat edilecek iki husus vardır; Bunlardan ilki siber savaşın devletler arasında cereyan etmesi; diğeri ise karşı tarafın sistemlerine hasar vermeye veya sistemlerde kesinti yapmaya yönelik eylemlerin siber savaş olarak nitelendirilmesidir. Bu tanıma göre karşı tarafın sistemlerine zarar vermeden bilgi çalmak siber savaş olarak kabul edilmemektedir.¹⁷

Uluslararası literatürde “siber savaş” ile doğrudan ilgili olmamakla birlikte “bilgi savaşı”¹⁸ şeklinde bir tanım Şanghay İşbirliği Örgütü tarafından yapılmıştır. Söz konusu tanım şu şekildedir: “bilgi alanındaki bilgi sistemlerine, süreçlerine ve kaynaklarına, eleştirel ve diğer yapılara zarar vermeyi, politik, ekonomik ve sosyal sistemleri zedelemeyi, toplumu ve devleti istikrarsızlaştırmak için toplu psikolojik [beyin] yıkamayı

¹³ Paul Livingstone, David Clemente Cornish, Dave Yorke Claire, *On Cyber Warfare*, Chatham House Report, Kasım 2010, s.7.

¹⁴ Gökhan Bayraktar, *Siber Savaş ve Ulusal Güvenlik Stratejisi*, Yeni Yüzyıl Yayınevi, İstanbul, 2015, s.137.

¹⁵ Nils Melzer, “Cyberwarfare and International Law”, *Ideas For Peace And Security*, <https://unidir.org/files/publications/pdfs/cyberwarfare-and-international-law-382.pdf>, s.4. [Erişim Tarihi: 3 Mart 2021].

¹⁶ Angelyn Flowers, “Cyberwar: The What, When, Why and How”, *IEEE Technology And Society Magazine*, Güz 2014, s.14. [file:///C:/Users/NewTech/Downloads/Cyberwar The What When Why and How Commentary%20\(1\).pdf](file:///C:/Users/NewTech/Downloads/Cyberwar%20The%20What%20When%20Why%20and%20How%20Commentary%20(1).pdf) [Erişim Tarihi: 3 Mart 2021].

¹⁷ Çifçi, a.g.e., s.7; Şeyda Türkay, “Siber Savaş Hukuku ve Uygulanma Sorunsalı”, *İÜHFİM*, Cilt: LXXI, Sayı:1, 2013, s.1179-1180; Lionel Alford Jr., “Cyber Warfare: A New Doctrine and Taxonomy”, *The Journal of Defense Software Engineering*, Bahar 2001, s.27 – 30; Bayraktar, a.g.e., s.47 – 50.

¹⁸ Bilgi savaşı ile ilgili herhangi bir doktrin bulunmamasına ve üzerinde anlaşılmış inanç/kavram topluluğu olmamasına rağmen, bilgi savaşları çok kısa manada “ulusal ve bu amaçla çatışmaların gerçekleştirilmesi için bilginin kullanılması” olarak tanımlanmaktadır. Mustafa, Sağsan, “Bilgi Savaşı: Siberlerden Klavyelere Taşınan Bir Harekâtın Anatomisi”, *Avrasya Dosyası: İstihbarat Özel*, 2002, Cilt 9, Sayı 2, s.217.

amaçlayan iki veya daha fazla devlet arasındaki çatışmanın yanı sıra devletin çıkarına karar vermeye zorlamak".¹⁹

Siber savaş veya internet üzerinden yürütülen bilgi savaşı, temel olarak bir düşmanın bilgisayar ağlarına ve veri tabanlarına, genellikle "virüsler"²⁰, "solucanlar"²¹, "Truva atları"²² gibi silahların kullanılmasıyla sızmayı ve bozmayı amaçlamaktadır.²³

İçerik ve unsurların açısından siber suç ve siber terörden farklı yönleri bulunan siber savaş "devletlere/hükümetlere bağlı meşru organize gruplar arasındaki büyük ölçekli çatışma" olarak tanımlanmaktadır. Bu nedenle siber savaş, çıkar elde etmeyi ve maddi kazanç sağlamayı amaç edinen siber suç ile siyasi-ideolojik amaçlarla girişilen siber terörle temelde ayrılmaktadır.²⁴

¹⁹ Annex I to the Agreement between the Governments of the Member States of the Shanghai Cooperation Organization on Cooperation in the Field of International Information Security of 16 June 2009. <http://eng.sectesco.org/load/207508/> [Erişim Tarihi: 3 Mart 2021].

²⁰ Bilgisayar virüsleri, "çalıştığında bilgisayara değişik şekillerde zarar verebilen" bilgisayar programlarıdır. Eğer bu programlar (ya da virüs kodları) herhangi bir şekilde çalıştırılırsa, programlanma şekline göre bilgisayarınıza zarar vermeye başlar.

<https://www.sabah.com.tr/egitim/2017/02/02/bilgisayar-virusu-nedir>. [Erişim Tarihi: 3 Mart 2021].

²¹ Solucanlar, daha karmaşık yapıya sahip olan zararlı yazılımlardır. Genellikle e-posta ile gönderilen ekler, çeşitli web siteleri ve ağ üzerinde paylaşılan dosyaları kullanarak yayılırlar. Solucanlar, bir sistemi ele geçirdiklerinde, kullanıcının başka bir eylemine ihtiyaç duymadan, kullanıcının veri kaynaklarını kullanarak (e-posta adres listesi gibi) kendi kaynak dosyalarını hızlı bir şekilde diğer kullanıcılara da ulaştırmayı denerler ve bu yolla kendilerini çok fazla sayıda çoğaltabilirler. Solucanlar bunu yaparken kullanıcıların bant genişliklerini ve ağ kaynaklarını kullandıklarından ağların kilitlenmesine, e-posta sunucularının aşırı yüklenmesine veya Web kaynaklarına erişim hızının düşmesine sebep olabilmektedirler. <https://bidb.itu.edu.tr/sevir-defteri/blog/2013/09/07/vir%C3%BCs-solucan-ve-truva-at%C4%B1> [Erişim Tarihi: 3 Mart 2021].

²² Truva atı adı verilen zararlı yazılımlar kendilerini kullanıcılara faydalı bir program gibi göstererek karıştan yüklenmelerini sağlarlar. Temelde iki farklı dosya içerirler. Bunlardan birincisi kullanıcıya yollanılan dosyadır. Bu dosya kullanıcının kendisini bilerek veya bilmeyerek çalıştırması durumunda bilgisayarın bir portunu kendisi için açarak, programcısına kullanıcının bilgisayarına erişebilme imkânı sunar. Programcı ise ikinci dosyayı çalıştırarak kullanıcının bilgisayarına ulaşabilmektedir. Truva atı programcılar ulaştıkları bilgisayardaki kullanıcıların kişisel bilgilerini (şifre, kredi kartı bilgileri, önemli dokümanlar) elde etmek amaçlı kullanılmaktadır ve bu durum kullanıcılara virüs ve solucanlardan daha fazla zarar vermektedir. Ayrıca Truva atları sistemde bilinmeyen açık bir kapı bıraktıklarından programcılarının bilgisayara kolayca başka kötü amaçlı yazılımlar yükleyebilmesine imkan vermektedir. <https://bidb.itu.edu.tr/sevir-defteri/blog/2013/09/07/vir%C3%BCs-solucan-ve-truva-at%C4%B1> [Erişim Tarihi: 3 Mart 2021].

²³ Ahmad Kamal, *The Law of Cyber – Space*, United Nations Institute of Training and Research, Cenevre, 2005, s.76; Angelyn Flowers, a.g.e., s.14 – 20; Bayraktar, a.g.e., s.47 – 50; Can Kasapoğlu, "Siber Savaş: Geleceğin Askeri Gerçekliği ve Günümüzün Bilimkurgusu Arasında", *EDAM Siber Politikalar Kağıtları Serisi*, 2017/2, s. – 14.

[file:///C:/Users/NewTech/Downloads/Cyberwar The What When Why and How Commentary%20\(1\).pdf](file:///C:/Users/NewTech/Downloads/Cyberwar%20The%20What%20When%20Why%20and%20How%20Commentary%20(1).pdf) [Erişim Tarihi: 3 Mart 2021].

²⁴ Ercan Çitlioglu, *İnsanı Dünyayı ve Terörizmi Anlamak*, Destek Yayınevi, İstanbul, 2011, s.104; Türkay, a.g.e. s.1180; Bayraktar, a.g.e., s.47 – 50.

Siber savaşın temelleri Soğuk Savaş döneminde atılmıştır ve teknolojik gelişmeler de birçok siber tehdit araçlarını²⁵, saldırı tekniklerini ve ülkelerin beşinci caydırıcı güç olarak öngördükleri siber orduları ortaya çıkarmıştır.²⁶

Günümüz savaşları, cephelerden siber ortama taşınmış olup bilgi güvenliğinin önemi ve devlet kurumlarının gizliliği önemli bir hal almıştır. Halkın devlete olan güveni siber dünyada sözü geçen kişilere/devletlere bağlı ilerlemektedir. İşte bu nedenler, ülkelerin fiziksel askeri yatırımlarının yanı sıra bilişim alanına da yansımış olup “siber ordu”lar kurulmaya başlamıştır.²⁷ Yeni savaş alanı olarak kabul edilen siber alanda yalnızca bilgiye erişim değil, bunun yanı sıra, bilgiyi değiştirme, manipüle etme, siber istihbarata karşı koyma, bilgiyi çarpıtma ve koruma gibi tam manasıyla bir mücadele söz konusudur. Siber alan, kendisinden önceki savaşlar gibi olur biter vaziyette değildir. Bir muharebe alanının ve sınırlarının olmayışı, siber alanın savaş ortamından çok bir mücadele ortamı olarak ortaya çıkmasını zorunlu kılmıştır.²⁸

Sonuç olarak siber savaş, bir ülkenin başka bir ülkenin bilişim ve iletişim sistemlerine zarar vermek veya onları kullanım dışı bırakmak amacıyla internet veya iletişim ağları ve bilgisayarları kullanarak müdahale etmek olarak tanımlanabilir. Geleneksel kara, deniz, hava savaşlarında olduğu gibi siber savaşta da uygun yetkinlik ve teçhizata sahip ordular kullanılmaktadır.²⁹



²⁵ Siber tehdit araçları çalışmamızın “Siber Saldırı Türleri” başlıklı bölümde detaylı olarak incelenmiştir.

²⁶ Abdulkemir Alkan, Oğuzhan, “Dünyada ve Türkiye’de Siber Savaşlar”, *CyberMag Dergisi*, Sayı:27, Nisan, 2018, s.17; Bayraktar, a.g.e., s.47 – 50.

²⁷ Kolektif Yazarlar, *Siber Güvenliğe Giriş*, 1.Baskı, İstanbul, 2017, s.58; Bayraktar, a.g.e., s.47 – 50.

²⁸ Siber Güvenliğe Giriş, a.g.e., s.58.

²⁹ Oğuzhan Abdulkemir Alkan, “Siber Güvenlik ve Siber Savaşlar”, *CyberMag Dergisi*, Sayı:12, Ocak 2017, s.22.

ULUSLARARASI HUKUK BAĞLAMINDA SİBER SALDIRILAR

Siber Saldırı ve Kuvvet Kullanma Yasağı

Uluslararası hukukta kuvvet kullanılmasının yasaklanmasına ilişkin temel düzenlemeyi, BM Antlaşması madde 2/4'de düzenlemektedir. Söz konusu madde; *"Tüm üyeler, uluslararası ilişkilerinde gerek herhangi bir başka devletin toprak bütünlüğüne ya da siyasal bağımsızlığa karşı, gerek Birleşmiş Milletler'in amaçları ile bağdaşmayacak herhangi bir biçimde kuvvet kullanma tehdidine ya da kuvvet kullanılmasına başvurmaktan kaçınırlar"*³⁰ şeklinde düzenlenmiştir.

Madde metninden de anlaşılacağı üzere, kuvvet kullanma yasağı uluslararası ilişkiler çerçevesinde düşünülmüş olup, devletin ülkesi içinde meydana gelen ayaklanma veya iç savaş gibi durumlarda kuvvet kullanılması, anılan yasağın dışında kalmaktadır. Dolayısıyla, bir devletin ülkesinde devam eden isyanı bastırmak veya terör hareketlerini önlemek amacıyla kuvvet kullanması hükmün kapsamına girmemektedir.³¹

Siber faaliyetler, yukarıda açıklamış olduğumuz tanımlar çerçevesinde BM Şartı'nın 2 (4) maddesi ve uluslararası teamül hukuku anlamında güç kullanımını oluşturabilirler. Bir siber operasyonun bir güç kullanımı oluşturup oluşturmadığını analiz ederken, çoğu yorumcu, siber olaydan kaynaklanan doğrudan fiziksel yaralanma ve maddi hasarın kinetik silahlar tarafından üretilmesi üzerine odaklanıp, siber saldırıların güç kullanımı olarak kabul edilip edilmeyeceğine odaklanmaktadır. Örneğin, ölüm, yaralanma veya önemli ölçüde tahribatla sonuçlanan siber faaliyetler büyük olasılıkla güç kullanımı olarak görülecektir. Bir olayın siber alanda güç kullanımını oluşturup oluşturmadığını değerlendirirken, olayın bağlamı, eylemi sürdüren aktör, hedef ve yer, etkiler, niyet ve diğer olası konular önem teşkil etmektedir. Güç kullanımını oluşturacak siber faaliyet örnekleri olarak, örneğin, (1) nükleer santral tesislerinin reaktörlerinin erimesini tetikleyen operasyonlar, (2) nüfusun yoğun olduğu bir alanın üzerinde imhaya neden olan bir baraj kapaklarını açan operasyon veya (3) uçak kazalarına neden olan hava trafik kontrolünü devre dışı bırakan siber saldırıları verebiliriz. Kısaca açıklamak gerekirse eğer bir siber saldırının fiziksel sonuçları bir bomba atmak veya bir füze ateşlemek gibi bir tür fiziksel hasara neden olursa, siber saldırı eşit derecede bir kuvvet kullanımı olarak düşünülebilecektir.³²

BM Antlaşması madde 2/4 çerçevesinde siber saldırıların, fiziksel hasar, fonksiyonel zarar veya her ikisinin bir kombinasyonunu içerip içermediğine bakılmaksızın, insanlarda ölüme veya yaralanmaya ya da nesnelerin ve altyapının tahribatına neden olmak için tasarlanmış saldırgan veya savunma amaçlı bir araç olarak kullanılması kuvvet kullanımı

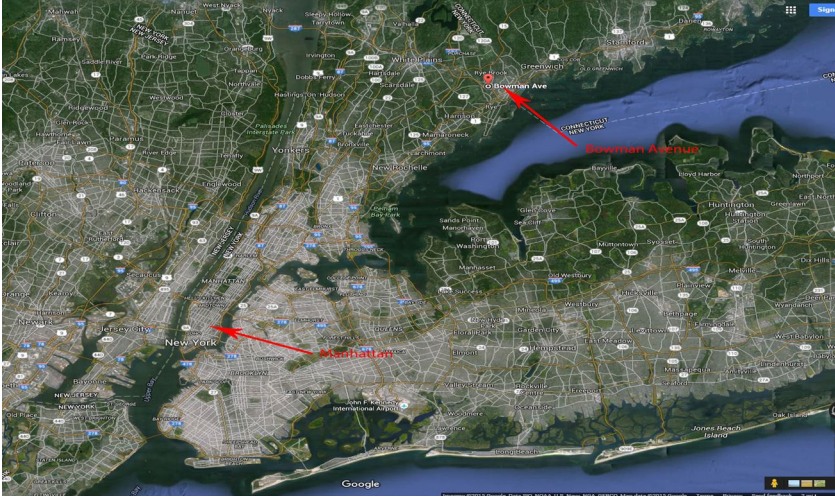
30 Birleşmiş Milletler Antlaşması için bakınız:

<https://www.tbmm.gov.tr/komisyon/insanhaklari/pdf01/3-30.pdf> [Erişim Tarihi: 3 Mart 2021].

31, Ahmet Hamdi Topal, *Uluslararası Terörizm ve Terörist Eylemlere Karşı Kuvvet Kullanma*, Beta Yayınları, İstanbul, 2005, s.86; Sertaç Hami Başeren, *Uluslararası Hukukta Devletlerin Münferiden Kuvvet Kullanmalarının Sınırları*, Ankara Üniversitesi Basımevi, Ankara, 2003, s.47 – 51; Cem, Ü. Beyoğlu, *Kuvvet Kullanma Yasağı Kapsamında Devletlerin Bireysel Meşru Müdafaa Hakkı*, Seçkin Yayınları, Ankara, 2018, s.40 – 44; İbrahim Kayra, *Terörle Mücadele ve Uluslararası Hukuk*, USAK Yayınları, Ankara, 2005, s.24.-25.

32 Harold H. Koh, "International Law in Cyber Space", *Harvard International Law Journal*, Cilt 54, 2012, s.3 – 4.

olarak değerlendirilebilecektir. Dolayısıyla, BM Antlaşması'nın 2/4. maddesi anlamında "kuvvet" kullanımının göze çarpan örnekleri, bir nükleer güç istasyonunda erimeye neden olacak veya taşkın kapılarını açacak şekilde hedef bilgisayar sistemlerini manipüle eden siber işlemler olacaktır. Yoğun nüfuslu bir alanın üzerindeki bir baraj veya kötü hava koşullarında yoğun bir havaalanının hava trafik kontrolünü devre dışı bırakmak, her biri ölüm, yaralanma ve imha açısından potansiyel olarak korkunç sonuçlara yol açabilecektir.³³



Kaynak: "Iranian Hackers Claim Cyber Attack on New York Dam", *NBC News*, 23 Aralık 2015.

Siber Saldırı Suçu

Devletlerin saldırı suçu ile ilgili çalışmalar II. Dünya Savaşı'ndan sonra Birleşmiş Milletler Genel Kurulu'nun 12.12.1974 tarihli 3314 (XXIX) sayılı kararı ile sonuçlanmış ve saldırı kavramının anlamı açıklanmıştır. Bu tanımın yapılış amacı, kararın giriş kısmında açıklanmış ve bunun muhtemel bir saldırganın cesaretini kırmak olduğu belirtilmiştir.³⁴ 3314 sayılı kararda saldırı tanımı, şu şekilde ifade edilmektedir:

³³ Nils Melzer, "Cyberwarfare and International Law", *Ideas For Peace And Security*, <https://unidir.org/files/publications/pdfs/cyberwarfare-and-international-law-382.pdf>, s.7. [Erişim Tarihi: 3 Mart 2021].

³⁴ Durmuş Tezcan, "Saldırgan Savaş ve Devletlerarası Ceza Hukuku", *Ankara Üniversitesi Siyasal Bilgiler Fakültesi Dergisi*, Sayı:1, Cilt:49, 1994, s.358; Malcolm N. Shaw, *Uluslararası Hukuk*, Türkiye Bilimler Akademisi Yayınları, Ankara, 2017, s. 313; Melda Sur, *Uluslararası Hukukun Esasları*, Dokuz Eylül Üniversitesi Yayınları, İzmir, 2000, s.265; Cengiz Başak, *Uluslararası Ceza Mahkemeleri ve Uluslararası Suçlar*, Turhan Kitabevi, Ankara, 2003, s.249 – 254.

*"Madde 1- Saldırı, bir Devletin diğer bir Devletin egemenliğine, ülke bütünlüğüne veya siyasi bağımsızlığına karşı veya işbu Tanımda belirtildiği üzere, Birleşmiş Milletler Antlaşması ile bağdaşmayan diğer herhangi bir tarzda silahlı kuvvet kullanılmasıdır."*³⁵

3314 sayılı kararın 1.maddesi saldırı tanımında belirtildiği üzere, 'herhangi bir tarzda silahlı kuvvet kullanılması' çalışmamız açısından önemli bir ayrıntı teşkil etmektedir. İlgili maddede de belirtildiği üzere silahlı saldırıdan ne anlaşılması gerektiği açık bir şekilde belirtilmemiş olup, saldırı ile ilgili önemli kısmın, devletin egemenliğine veya siyasi bağımsızlığına karşı gerçekleştirilmesi yönünde olduğudur. Bu bağlamda siber enstrümanlar vasıtasıyla gerçekleştirilecek eylemler, etkileri çerçevesinde 3314 sayılı kararın 1.maddesi ile ilgili olarak devletler açısından saldırı suçu şeklinde değerlendirilebilecektir.

Geleneksel kara, deniz, hava savaşlarında olduğu gibi siber savaşta da uygun yetkinlik ve teçhizata sahip ordular kullanılmaktadır. Bu ordular, 3314 Sayılı Karar da belirtildiği üzere Devletin kara, deniz veya hava kuvvetlerine veya deniz veya hava filolarına siber saldırılar düzenleyebilir. Bu noktada kanaatimiz "siber saldırıların" silahlı bir saldırı sonucu teşkil etmesi ya da başka bir deyişle silahlı bir saldırının yaratacağı boyutta zarar vermesi durumunda, 3314 Sayılı Kararın 3.maddesi çerçevesinde de değerlendirilip, saldırı suçu teşkil edebileceği yönündedir.

3314 Sayılı Karar bir devletin ülkesine fiziki olarak bir tecavüz olmadan da saldırı eyleminin gerçekleştirilebileceğini belirtmektedir. Bir ülkenin silahlı kuvvetleri vasıtası ile bir başka ülkenin limanlarının ya da kıyılarının abluka altına alınması da bir saldırı eylemi örneği olarak değerlendirilmiştir. Abluka, mutlaka hedef devletin egemenliği altındaki ülke topraklarının ihlali gerektirmemektedir. Zira abluka, açık denizlerden de yapılabilmektedir³⁶. Yine bu noktada da "siber saldırıların" belirtilen abluka gibi, bir devletin askeri unsurlarınca karşı devletin, internet ağının kesilip kontrol altına alınması, devlet imkânlarının işlemez hale gelmesi ya da bilgilerin silinip değiştirilmesi, devletin egemenliğine ya da ülke bütünlüğüne bir saldırı olarak düşünülüp, saldırı suçu kapsamında değerlendirilebilecektir.



³⁵ Saldırı'nın Tanımı: Birleşmiş Milletler Genel Kurulu'nun 3314 (XXIX) sayılı ve 1974 Tarihli Kararı: Detaylı Bilgi için bakınız: http://www.unicankara.org.tr/doc_pdf/3814.pdf. [Erişim Tarihi: 3 Mart 2021].

³⁶ Yücel Acer, *Uluslararası Hukukta Saldırı Suçu*, Roma Yayınları, Ankara, 2004, s.106-107.

Siber saldırıları saldırı suçu bağlamında değerlendirecek olursak, iki veya daha fazla ülke arasında mevcut olan bir çatışma ya da çatışma potansiyelinin açık olması durumunda taraflardan birinin karşı tarafta kesin olarak ölümler, yaralanmalar ya da fiziki zararlar sonuçlanabilecek bir siber tehditte bulunması, siber saldırı olarak değerlendirilmektedir. Örneğin, ABD-Rusya arasında cereyan eden büyük bir siyasi ya da askerî kriz sonrasında, ABD'nin Rusya'daki bir nükleer santrale yönelik doğrudan zarar verici siber saldırı yapacağını yetkili birimlerce aleni ya da zımni olarak açıklaması durumunda olası sonuçların klasik anlamda bir bombardımandan farklı olmayacağı için saldırı olarak değerlendirilecektir. Klasik uygulamaya benzer şekilde, muhtemel saldırı durumu dışında sadece bir tarafın diğer tarafa tehditte bulunması bu kapsamda değerlendirilemez. Ayrıca, uluslararası hukuka uygun olarak meşru müdafaa hakkına sahip ya da Güvenlik Konseyi kararına istinaden güç kullanmaya hak kazanan tarafların tehditte bulunması meşru sayılmaktadır.³⁷

Siber Saldırlara Karşı Meşru Müdafaa Hakkının Kullanımı

Uluslararası hukuk bakımından kuvvet kullanımı ve saldırı yasağı ile yakından ilgili bir konu da meşru müdafaa hakkıdır. İç hukuklarda birey nasıl ki, kendisine veya bir başkasına yönelik ağır ve haksız bir saldırıdan doğan tehlikeyi uzaklaştırmak amacıyla saldırıyla orantılı bir koruma hakkına sahipse; uluslararası hukuk bakımından da devletlerin ülkesel bütünlüğüne, bağımsızlığına yönelik bir saldırı olması halinde, saldırıya uğrayan devletin saldırıyı def etmek amacıyla kuvvet kullanma hakkı kabul edilmektedir.³⁸

BM Antlaşmasının kuvvet kullanılmasına izin verdiği durumlar BM Antlaşması 51.madde çerçevesinde "meşru müdafaa" hakkı ve BM Güvenlik Konseyi kararları uyarınca kuvvet kullanılmasıdır. BM Antlaşması'nın meşru müdafaa hakkı ile ilgili 51.maddesi şu şekildedir; *"Bu Antlaşma'nın hiçbir hükmü, Birleşmiş Milletler üyelerinden birinin silahlı bir saldırıya hedef olması halinde, Güvenlik Konseyi uluslararası barış ve güvenliğin korunması için gerekli önlemleri alıncaya dek, bu üyenin doğal olan bireysel ya da ortak meşru savunma hakkına halel getirmez."*³⁹

BM Antlaşması'nın 51.maddesiyle savaş yasağına getirilen doğal bir hak şeklindeki bu istisna, sadece silahlı bir saldırıya cevap vermek için ve BM Güvenlik Konseyi'nce gerekli önlemler alınıncaya kadar başvurulabilecek bir yol olmaktadır. Bu durumda Güvenlik Konseyi'ne hemen bilgi vermek gerektiği gibi, Güvenlik Konseyi de her an olaya kendisi el koyabilmektedir.⁴⁰

Siber saldırıya karşı meşru müdafaa hakkının kullanımı ile ilgili en önemli tartışmalı husus, siber saldırının kaynağının tespit edilmesinin zorluğuna ilişkindir. Buna göre, siber saldırıya karşı meşru müdafaa hakkının kullanılabilmesi için, siber saldırının bir devlet tarafından ya da devlet destekli bir grup tarafından gerçekleştirilmesi ve bunun tespit edilmesi gerekmektedir.

³⁷ Ramazan Güreşçi, "Siber Saldırıların Uluslararası Hukuktaki Güç Kullanımı Kapsamında Değerlendirilmesi", *Savunma Bilimleri Dergisi*, Mayıs 2019, Cilt:18, Sayı:1, s.88.

³⁸ Poyraz Bozkurt Kütükçü, a.g.e., s.318; İlyas Doğan, *Devletler Hukuku*, Seçkin Yayıncılık, Ankara, 2008, s.156; Bozkurt, a.g.e., s.57 – 62.

³⁹ BM Antlaşması 51.Madde için bakınız: <https://www.tbmm.gov.tr/komisyon/insanhaklari/pdf01/3-30.pdf>. [Erişim Tarihi: 3 Mart 2021].

⁴⁰ Tezcan, a.g.e., s.351; Doğan, a.g.e., s.156 – 157..

Meşru müdafaa hakkının kapsamı ile ilgili önemli tartışma konularından biri de, hiç şüphesiz devletlerin önleyici meşru müdafaa (*self defence/ Bush doctrine*) hakkının olup olmadığıdır. Bu çerçevede karşılaşılan sorun, BM Antlaşması 51.madde hükmünün sadece silahlı bir saldırının başlamasından sonra mı meşru müdafaa hakkının varlığını tanımakta olduğu veya çok yakın bir tehlike veya saldırı gerçekleşmeden meşru müdafaa amaçlı kuvvet kullanmanın olup olmadığıdır.⁴¹

Önleyici meşru müdafaa doktrini, uluslararası hukukta net bir biçimde çözümlenmiş bir konu değildir. Eğer, uluslararası hukuk kuralları geniş şekilde yorumlanır ise, önleyici meşru müdafaa hukukidir. Aksine, dar yorum benimsenirse hiçbir şekilde önleyici meşru müdafaa hakkı uygulama alanı bulamayacaktır.⁴²

Sonuç olarak silahlı saldırı seviyesine gelmiş bir siber hareketin hedefi, doğal olarak meşru müdafaa hakkını kullanabilir. Meşru müdafaa hakkını kullanan bir devlet tarafından gerçekleşen güç kullanımı, gerekli ve orantılı olmalıdır. Meşru müdafaa kuvvet kullanımı hakkı, bir siber silahlı saldırı gerçekleşirse veya kaçınılmaz ise ortaya çıkmaktadır. Bu husus aynı zamanda acil bir gereksinime bağlıdır. Meşru müdafaa hakkı müşterek hareket olarak da kullanılabilir. Silahlı saldırı seviyesine gelmiş bir siber harekate karşı müşterek meşru müdafaa hakkı yalnızca mağdur ülkenin talebi ile ve talep kapsamı doğrultusunda kullanılabilir.⁴³

KKTC'YE YÖNELİK BİR SİBER SALDIRIDA KKTC DEVLETİNİN ULUSLARARASI HUKUK AÇISINDAN DURUMU

KKTC'nin Uluslararası Alanda Tanınmama Sorunu

Çalışmamızın bu bölümünde KKTC (Kuzey Kıbrıs Türk Cumhuriyeti)'ye yönelik Devlet tarafından ya da Devlet destekli olası bir siber saldırı durumunda, uluslararası hukuk açısından KKTC'nin var olabilecek haklarını irdelleyeceğiz.

KKTC'ye yönelik olası bir siber saldırının Devletlerin askeri unsurları ya da Devletlerin desteklediği diğer kişiler tarafından gerçekleştirilmesi durumunda uluslararası hukuk açısından, saldırıyı gerçekleştiren ya da destekleyen devletin uluslararası sorumluluğu gündeme gelecektir. Uluslararası hukuk açısından uluslararası sorumluluğun gündeme gelebilmesi için, uluslararası hukuk kişinin hukuka aykırı eylemi ya da hukuka uygun faaliyetlerinden kaynaklanan zararı önem arz etmektedir. Bu noktadan hareketle siber saldırılar neticesinde devletlerin zarar görmesi durumunda, eylem uluslararası hukuka aykırı bir nitelik olarak değerlendirilebilecek ve eylemi gerçekleştiren devletin sorumluluğu konusunu gündeme gelebilecektir.

Bir devletin uluslararası sorumlu tutulabilmesi için bu devlet organlarının uluslararası hukuka aykırı bir fiili doğrudan işlemiş olmaları ya da uluslararası sorumluluk doğuracağı kabul edilen faaliyeti kendi adlarına yürütmeleri gerekmektedir. Bununla birlikte, özel kişilerin bir devletçe işledikleri fiillerin kimi koşullarda bu devletin sorumluluğunu dolaylı olarak ortaya koyması söz konusu olabilmektedir. Yine, bir devlet ülkesinde ayaklanmalar

⁴¹ Yusuf Aksar, *Teori ve Uygulamada Uluslararası Hukuk – II*, Seçkin Yayınları, Ankara, 2019, s.131.

⁴² Aksar, a.g.e. s.131.

⁴³ M. Yasin Aslan, "Savaş Hukukunun Temel Prensipleri", *Türkiye Barolar Birliği Dergisi*, Sayı 79, 2008, s.200.

ya da iç savaşlar sonucu meydana gelen zararlardan kimi koşullarda bu devletin sorumlu tutulması durumlarıyla karşılaşmaktadır.⁴⁴

Devletlerin uluslararası sorumluluğu çerçevesinde, KKTC'ye yönelik gerçekleştirilecek olası bir siber saldırı durumunda KKTC'nin uluslararası hukukun bazı haklarından yararlanması söz konusu olabilecektir. KKTC'nin uluslararası sistemde devlet olarak tanınmıyor olması bazı ise bu durumun ayrıca açıklanmasını gerektirecektir.



Kıbrıslı Türklerin 15.11.1983'de Kuzey Kıbrıs Türk Cumhuriyeti'ni ilanı üzerine BM Güvenlik Konseyi 18.11.1983 tarih ve 541 sayılı kararı ile bu ilanı 1960 Anayasasına aykırı bulmuş ve KKTC'yi geçersiz saymıştır. Anılan karar Bağımsızlık Bildirisini bölücülük olarak değerlendirmiş ve bütün Devletlere Kıbrıs Cumhuriyeti'nden başka bir Kıbrıs Devletini tanımama çağrısında bulunmuştur. BM'nin bu yaklaşımına rağmen, bir tek Türkiye ilan edildiği gün KKTC'yi tanımış ve o günden bu zamana Türkiye dışında hiçbir ülke KKTC'yi tanımamıştır.⁴⁵

BM'in 541 sayılı kararına uluslararası toplumda genel bir biçimde uyularak KKTC'nin tanınmadığı ve Kıbrıs Cumhuriyeti'nin, Kıbrıs'ta tek Devlet olduğu yolunda birçok kararın alındığı görülmektedir. Ancak bu durum, KKTC'nin uluslararası hukuk açısından haklarının olmadığı ve zarar görmesi durumunda haklarını savunamayacağı anlamına gelmemelidir.

KKTC'ye yönelik olası bir siber saldırı durumunda ilk olarak belirlenmesi gereken, eylemin hangi Devlet tarafından gerçekleştirildiği ya da Devlet desteğinin olup olmadığıdır. Eylemi gerçekleştiren ya da destek veren Devletin tespit edilmesi sonrasında, KKTC saldırı ile ilgili meşru müdafaa hakkını kullanabilecek ya da BM Antlaşması'nda da belirtildiği üzere sorunu barışçıl yollarla çözme yoluna gidebilecektir.

Bu noktadan hareketle KKTC'ye yönelik gerçekleştirilecek olası bir siber saldırı durumunda ilk olarak meşru müdafaa hakkı ne şekilde gerçekleşecektir? İkinci olarak eylemi gerçekleştiren Devletin KKTC'yi Devlet olarak tanımıyor olması ve herhangi bir

⁴⁴ Hüseyin Pazarcı, *Uluslararası Hukuk Dersleri 3. Kitap*, Turhan Kitabevi, Ankara, 2019, s.162.

⁴⁵ Hüseyin Pazarcı, *Türk Dış Politikasının Başlıca Sorunları*, Turhan Kitabevi, Ankara, 2015, s.161.

diplomatik temasının bulunmaması, barışçıl yollara gidilmesi durumunda, tanımaya sebep olabilir mi?

Çalışmamızın ilgili bölümünde de belirttiğimiz üzere, meşru müdafaa hakkı BM Antlaşması çerçevesinde kuvvet kullanılmasını meşru kılmış ve her devlet kendisine yönelik gerçekleştirilen saldırılara, saldırıyla orantılı olarak cevap verebilme hakkına sahip kılınmıştır. KKTC'ye yönelik gerçekleştirilecek olası bir siber saldırıda, KKTC vatandaşlarının yaralanması, ölmesi ya da Devletin itibarının zarar görmesi durumunda, KKTC BM Antlaşması'nda belirtilen meşru müdafaa hakkını kullanabilecektir. KKTC'nin uluslararası sistemde Devlet olarak tanınmıyor olması meşru müdafaa hakkının kullanılmasına engel teşkil etmemektedir. Meşru müdafaa hakkının kullanılması ile ilgili en önemli mesele, siber saldırılara karşı, siber enstrümanlar aracılığıyla cevap verilmesidir. Başka bir ifadeyle, olası bir siber saldırı durumunda, diğer askeri teçhizatları (füze, balistik füze, uçak, tank) kullanmak, meşru müdafaa hakkı bağlamında bazı sorunlara neden olabilecektir.

Yine KKTC'ye yönelik olası bir saldırı durumunda, sorunu barışçıl yollarla çözme yoluna gidilmesi konusu ise BM çatısı altında mümkün olabilecektir. Bilindiği üzere BM'nin temel kuruluş amacı uluslararası barış ve güvenliği sağlamaktır. Bu çerçevede BM Antlaşması'nın 35.maddesinin 2.fıkrası; *"Birleşmiş Milletler üyesi olmayan bir devlet, taraf olduğu herhangi bir uyuşmazlık konusunda, işbu Antlaşmada öngörülen barışı yollarla çözme yükümlülüğünü, bu uyuşmazlık için önceden kabul etmek koşuluyla, Güvenlik Konseyi'nin ya da Genel Kurul'un dikkatini çekebilir"* diyerek, BM tarafından tanınmayan Devletlerin de BM Güvenlik Konseyi ya da Genel Kurul'a konuyu getirebileceğini belirtmektedir.

Siber saldırıdan ötürü yaşanacak bir uyuşmazlık durumunda konunun BM önüne taşınması, ya da uyuşmazlığa taraf diğer Devletin KKTC'yi muhatap alması, KKTC'yi tanıma olarak değerlendirilebilir mi sorusu ise yine önemli bir ayrıntıdır. Uluslararası hukukta tanıma, bir uluslararası hukuk kişinin kendi dışında oluşan belli bir olayı, durumu, belgeyi ya da iddiayı kendisi bakımından yasal kabul ettiğini ve hukuksal ilişkilerini bu veriler üzerine kuracağını bildiren tek-tarafli hukuksal işlemdir. Devletlerin tanımaya uygulamada iki değişik nitelikli tanıma biçimine yer vermektedir: bunlardan birincisi de jure tanıma, ikincisi ise de facto tanımadır. De jure tanıma bir devleti tam olarak tanımının sağladığı bütün hukuksal etkileri ile tanımayı belirtmektedir. Buna karşılık, de facto tanıma geçici ve sınırlı nitelikli bir tanımayı belirtmektedir. De facto tanımda genellikle tanıyan devletin tanınan devletin bağımsızlığı, ülke üzerindeki otoritesi ve ülkedeki istikrara ilişkin olarak kuşkuları bulunduğu ve bu nedenle tam bir tanımaya gitmediği görülmektedir. Böylece tanımaya atfedilen bu de jure ve de facto sıfatları tanınan devletin durumu ile ilgili olup, tanıma işleminin bizzat nitelendirilmesi değildir.⁴⁶

Öte yandan, de facto tanıma işlemi ile bir devletin başka bir devletin fiilen varlığını kabul etmesi olgusunu ayırmak gerekmektedir. Bunlardan ilki bir hukuksal işlemin gerçekleşmesini gerektirirken, ikinci durumda yalnızca bir fiili durum teyid edilmekte, fakat bu fiili duruma tanımadan kaynaklanan herhangi bir hukuksal etki tanımamaktadır. Örneğin, 1978 yılında Hesperides Hotels Ltd. V Aegean Turkish Holidays Ltd. davasında

⁴⁶ Hüseyin Pazarcı, *Uluslararası Hukuk*, Turhan Kitabevi, 18. Baskı, Ankara, 2019, s.344.

ilgili İngiliz Mahkemesine görüşünü bildiren İngiliz Dışişleri ve Commonwealth Bakanlığı Kıbrıs'ta adada fiilen iki yönetimin varlığını kabul etmesine rağmen KKTC'yi de facto tanımadığını bildirmiştir.⁴⁷

Böylece KKTC'ye yönelik olası bir siber saldırı gerçekleştiren Devletin tespit edilmesi ile birlikte, oluşan zararın barışçıl yollarla çözülmesi isteği, KKTC'nin de facto olarak tanınması ile gerçekleşebilir. Başka bir ifadeyle yukarıda Hesperides Hotels Ltd. V Aegean Turkish Holidays Ltd. davasında da İngiliz Dışişleri Bakanlığı'nın belirttiği üzere, siber saldırı neticesinde de, KKTC'nin tanınmadığının bir şerh ile belirtilmesi neticesinde sorun, barışçıl yollarla çözülebilecektir.

Siber Saldırı ile İlgili Uluslararası Antlaşmalara KKTC'nin Taraf Olabilme Durumu

Siber uzayın tartışılmaya başlandığı ve siber güvenliğin ciddi tehditler ürettiği 2000'li yıllardan itibaren bölgesel düzeyde, etkin olmasa bile önemli bazı düzenlemeler yapılmıştır. Bu çerçevede şu ana kadar yapılmış en önemli Antlaşma, "Avrupa Konseyi Siber Suçlar Sözleşmesi (2001)"dir.

KKTC, bağımsız bir devlet olarak tanınmadığı için Avrupa Konseyi'ne üye olamadığı gibi, Avrupa Siber Suçlar Sözleşmesi'ne de taraf değildir⁴⁸. Avrupa Konseyi organları Konsey'e üye ve Sözleşmeye taraf olarak Kıbrıs Cumhuriyeti'ni tanımaktadır. Bu nedenle KKTC'nin belirtilen antlaşmaya taraf olması Kıbrıs sorunun çözümü sonrasında ele alınabilecektir.

Avrupa Siber Suçlar Sözleşmesi'nin en önemli bölümü siber saldırı suçuyla mücadelede adli yardımlaşma hükümlerini içeren 3.bölümüdür.⁴⁹ Zira sınır tanımayan bir özelliğe sahip, birçok ülke üzerinde aynı anda işlenebilen, soruşturulması ve kovuşturulması çok teknik ve zorlu bir süreç olmasını gerektiren ve delillerin çabuk kaybolabileceği bu suç türleriyle mücadelede etkin ve çok hızlı bir uluslararası işbirliği olması gerekmektedir.⁵⁰ Ayrıca yine Avrupa Siber Suçlar Sözleşmesi Madde 24 uyarınca siber saldırı suçu işleyen bireylerin iadesi neticesinde devletler, vatandaşlarını yargılayıp söz konusu suç çerçevesinde yaptırımlar uygulayabilecekler.⁵¹

⁴⁷ Pazarıcı, a.g.e., s.345.

⁴⁸ Murat Metin Hakkı, "Property Wars in Cyprus: The Turkish Position According to International Law", *Ankara Bar Review*, 2010/2, 43-56, s. 44.

⁴⁹ Avrupa Siber Suçlar Sözleşmesi, III. Bölüm, Madde 23 – Uluslararası İşbirliğine İlişkin Esaslar, Madde 24 – Suçluların İadesi, Madde 25 – Karşılıklı Yardımlaşmaya İlişkin Genel İlkeler, Madde 26 – Kendiliğinden Bilgi Verme, Madde 27 – Uluslararası Anlaşmaların Yürürlükte Olmadığı Hallerde Yapılan Karşılıklı Yardımlaşma Taleplerine İlişkin Usuller, Madde – 28 Gizlilik ve Kullanımın Sınırlandırılması.

⁵⁰ Aliusta - Benzer, a.g.e., s.40.

⁵¹ Avrupa Siber Suçlar Sözleşmesi Madde 24: "Suçluların İadesi" – Bu madde, Taraflar arasında suçluların iadesi için işbu Sözleşme'nin 2 ila 11.maddelerinde tanımlanmış cezai suçlara ilişkin olarak söz konusu suçluların her iki tarafın yasaları çerçevesinde, en az bir yıl süreyle özgürlükten mahrum bırakma cezası veya daha ağır bir ceza ile cezalandırılabilir olması durumunda geçerli olacaktır."

Siber saldırıyı gerçekleştiren Devletlerin tespit edilmesi noktasında Avrupa Siber Suçlar Sözleşmesi önemli bir işbirliği içermektedir. İlerleyen teknoloji ile savaşların siber alana taşınacağı yönünde belirtilen görüşler, yıllarda siber saldırganların tespit edilmesi noktasında yardımı daha fazla önemli hale getirecektir. Bu bağlamda KKTC'nin sözleşmeye taraf olmadan da sözleşmede belirtilen adli yardımlaşma konusunda, Konsey'e katkısı olabilecektir. Bu durum yine KKTC'yi de facto olarak tanıyıp, kesin olarak tanıma anlamına gelmeyecektir.

Genel olarak, bir devletin politik varoluşu, diğer devletlerin tanınmasından bağımsızdır. Diğer devletler saldırgan davranışlardan kaçınmak zorundadır. Uluslararası antlaşmalar imzalayan devletler, aynı antlaşmayı imzalayan tanınmamış devletlerin de antlaşma ile bağlı olduğunu varsayarlar. Örneğin Birleşik Krallık tanımadığı Alman Demokratik Cumhuriyeti'nin 1963 tarihli Nükleer Denemelerin Önlenmesi Antlaşması ile bağlı olduğunu kabul etmiştir. Diplomatik ilişkilerin olmaması devletin hakları ve borçlarını etkilerse de, bu durum hak ve borçların varlığına engel teşkil etmemektedir.⁵²

Siber Saldırıları ile İlgili KKTC Devleti Mahkemelerince Verilmiş Kararların Tanınması Meselesi

Bir devletin mahkemesince verilmiş bir kararın, başka bir devletin ülkesinde kendiliğinden ve doğrudan doğruya etkili olması, sonuç doğurması söz konusu değildir. ancak uluslararası özel hukuk alanında "tanıma ve tenfiz" denilen belli usullerle, bu durum olanaklı hale gelebilmektedir.

Yabancı bir devlet mahkemesince verilmiş bir kararın "tanıma ve tenfiz" konusu olabilmesi için, kararın verildiği devletin "tanınmış" bir devlet olması gerekir mi? öğretide bu konuda çeşitli görüşler bulunmaktadır. Birinci görüşe göre, bir mahkemenin, yabancı bir devlet mahkemesince verilmiş kararıyla ilgili olarak, kendisine yapılan "tanıma ve tenfiz" başvurusunu, önce kararın verildiği ülke devletinin, kendi devletince tanınmış olup olmadığını incelemesi gerekir. Tanıma ya da tenfiz kararı verebilmesi için birinci koşul, tanıma ya da tenfiz istemine konu kararın "tanıma ve tenfiz" incelemesi yapan mahkemenin bağlı olduğu devletçe "tanınmış" olmasıdır. Bu görüşün gerekçesi şöyle özetlenebilir; Tanıma ve tenfiz işlemleri, sadece uluslararası topluluğun üyesi olarak kabul edilmiş devletler arasında söz konusu olabilir. Mahkeme, kendi devletince tanınmış olmayan yani uluslararası topluluğun üyesi sayılmayan bir devletin yargı organınca verilmiş kararlar ile ilgili olarak tanıma ve tenfize ilişkin karar vererek, kendi devletiyle çelişkiye düşmemelidir.⁵³

Buna karşı görüş ise, tanıma tenfiz konusunda karar verecek ulusal mahkemenin, başvuru konusu kararı veren devletin "tanıma" durumuyla ilgilenmemesi gerektiğini; yasal açıdan gerekli teknik koşullar varsa, tanıma ya da tenfiz kararı verilmesi gerektiğini savunur. Bu görüşün gerekçesi de şöyledir; "Tanıma ve tenfiz" konusunda karar verecek mahkemenin işlevi ile hükümetin işlevleri farklıdır. Mahkeme, bir yargı organı olarak, tanıma ya da tenfiz başvurusuna konu olan kararı veren mahkemenin dayandığı

⁵² Işıl Özkan, *Tanınmamış Devletlerin Yasa, Hukuki İşlem ve Kararlarının Tanınması*, Onikilevha Yayınları, İstanbul, 2017, s.107.

⁵³ Rona Aybay ve Elif Oral, *Kamusal Uluslararası Hukuk*, İstanbul Bilgi Üniversitesi Yayınları, İstanbul, s.286.

otoritenin, ülke üzerinde tartışmasız biçimde denetim kurmuş olup olmadığıyla ilgilenmelidir. Kendi hükümetinin, yabancı bir devleti tanıyıp tanımaması ayrı bir konudur. Mahkemenin devletin yabancı bir devleti tanıyıp tanımama konusunda vereceği karar, karmaşık birtakım politik hesaplara dayanmış olabilir. Tanıma, tenfiz konusunu inceleyen mahkemenin, bu değerlendirmelerle ilgilenmesi gerekmez.

KKTC mahkemelerinin vereceği kararlarda da yine tanıma meselesi önem taşımaktadır. KKTC'de yaşayan Türk vatandaşları açısından, Türkiye KKTC'yi tanıyan bir ülke olduğu için şuan "tanıma ve tenfiz" davaları Türkiye mahkemelerinde görülmektedir. Ancak, KKTC'de bulunan diğer ülke vatandaşları açısından, adli konularda söz konusu ülkenin vatandaşları açısından durum büyük bir sorun teşkil etmektedir.



SONUÇ

Uluslararası hukukta tanıma konusu, gerek uluslararası politika gerek hukuk açısından türlü sorunlar yaratabilen, oldukça karmaşık yönleri olan bir konudur. Ancak yine uluslararası hukukta var olan görüşlere göre, tanıma konusu devlet olmanın ana unsurlarından birisi değildir. Bu bağlamda tanınmayan bir devletin herhangi bir saldırıya maruz kalması durumunda meşru müdafaa hakkını kullanması ya da uluslararası antlaşmalara taraf olması konusunu, uluslararası hukukun üzerinde anlaşılmadığı konulardandır.

Türkiye dışında başka bir devlet tarafından tanınmayan KKTC bugün, devlet olabilmenin temel koşulları olan ülke, insan ve egemenlik kriterlerine sahiptir. BM Güvenlik Konseyi kararları neticesinde Türkiye dışında başka bir ülkenin KKTC'yi tanıma yoluna gitmemiş olması, KKTC'nin bir devlet olduğu gerçeğini değiştirmemektedir. Bu noktada KKTC'nin uluslararası sistemde tanınmıyor olması olası bir siber saldırıya maruz kalması durumunda meşru müdafaa hakkını kullanmasına engel teşkil etmeyecektir. Yine başka bir ifadeyle olası bir siber saldırı durumunda oluşacak uyuşmazlıkta, KKTC ile sorunu barışçıl yollarla çözmeye yoluna gidilmesi her zaman KKTC'nin tanınması anlamına gelmeyecektir.

Sonuç olarak KKTC'ye yönelik olası bir siber saldırı durumunda KKTC Devleti, uluslararası hukukun var olan bazı haklarından faydalanabilecek ve Devlet halkının korunması konusunda adımlar atabilecektir:

KAYNAKÇA

- Richard A. Clarke ve Robert K. Knake, *Siber Savaş*, İstanbul Kültür Üniversitesi Yayınları, İstanbul, 2011.
- Abdulkrim Oğuzhan Alkan, "Dünyada ve Türkiye'de Siber Savaşlar", *CyberMag Dergisi*, Sayı: 27, Nisan 2018.
- Ahmad Kamal, *The Law of Cyber – Space*, *United Nations Institute of Training and Research*, Cenevre, 2005.
- Ahmet Hamdi Topal, *Uluslararası Terörizm ve Terörist Eylemlere Karşı Kuvvet Kullanımı*, Beta Yayınları, İstanbul, 2005.
- Lionel D. Alford Jr., "Cyber Warfare: A New Doctrine and Taxonomy", *The Journal of Defense Software Engineering*, Nisan 2001.
- Ali Burak Darıcılı, *Siber Uzay ve Siber Güvenlik – ABD VE Rusya Federasyonu'nun Siber Güvenlik Stratejilerinin Karşılaştırılmalı Analizi*, Dora Yayıncılık, Bursa, 2017.
- Angelyn Flowers, "Cyberwar: The What, When, Why and How", *IEEE Technology and Society Magazine*, Güz 2014.
- Ayhan Songar, *Sibernetik*, Temel Matbaa ve Ambalaj Sanayi, İstanbul, 1980.
- Berdal Aral, *Uluslararası Hukukta Meşru Müdafaa Hakkı*, Siyasal Kitabevi, Kırıkkale, 1999.
- Can Kasapoğlu, "Siber Savaş: Geleceğin Askeri Gerçekliği ve Günümüzün Bilimkurgusu Arasında", *EDAM Siber Politikalar Kağıtları Serisi*, 2017/2.
- Cem Beyoğlu, *Kuvvet Kullanma Yasağı Kapsamında Devletlerin Bireysel Meşru Müdafaa Hakkı*, Seçkin Yayınları Ankara, 2018,
- Cengiz Başak, *Uluslararası Ceza Mahkemeleri ve Uluslararası Suçlar*, Turhan Kitabevi, Ankara, 2003.
- Durmuş Tezcan, "Saldırgan Savaş ve Devletlerarası Ceza Hukuku", *Ankara Üniversitesi Siyasal Bilgiler Fakültesi Dergisi*, Sayı:1, Cilt:49, 1994.
- Ercan Çitlioğlu, *İnsanı Dünyayı ve Terörizmi Anlamak*, Destek Yayınevi, İstanbul, 2011.
- Fahrettin Demirdağ, "Uluslararası Ceza Divanı, Savaş Suçları – Saldırı Suçu, Mevzuatımıza Göre Savaş Hali", *Uluslararası Ceza Divanı*, Yayına Hazırlayan, Feridun Yenisey, Arıkan Basım Yayım, İstanbul, 2007.
- Fulya Aslay, "Siber Saldırı Yöntemleri ve Türkiye'nin Siber Güvenlik Mevcut Durum Analizi", *International Journal of Multidisciplinary Studies and Innovative Technologies*, Cilt: 1, No: 1, 2017.
- Gökhan Bayraktar, *Siber Savaş ve Ulusal Güvenlik Stratejisi*, Yeni Yüzyıl Yayınevi, İstanbul, 2015.
- Halis Ayhan, "Terör Kavramı, Güvenlik Konseyi ve Genel Kurul Özelinde Birleşmiş Milletler'in 2001 Sonrası Terör Yaklaşımı", *Güvenlik Stratejileri Dergisi*, Cilt:11, Sayı:21, 2015.
- Harold, H. Koh, "International Law in Cyber Space", *Harvard International Law Journal*, Cilt:54, 2012.

- Hasan Çifçi, *Her Yönüyle Siber Savaş*, TUBİTAK Yayınları, 2. Basım, Ankara, 2017.
- Haydar Demir Çakmak ve Korhan Cenker, "Siber Dünyadaki Tehditler ve Kavramlar", *Suç, Terör ve Savaş Üçgeninde Siber Dünya*, Haydar D. Çakmak ve Taner Altunok (Der.), Barış Platin Kitabevi, Ankara, 2009.
- Hüseyin Pazarıcı, *Uluslararası Hukuk Dersleri 3. Kitap*, Turhan Kitabevi, Ankara, 2019.
- Hüseyin Pazarıcı, *Türk Dış Politikasının Başlıca Sorunları*, Turhan Kitabevi, Ankara, 2015.
- Hüseyin Pazarıcı, *Uluslararası Hukuk*, Turhan Kitabevi, 18. Baskı, Ankara, 2019.
- Işıl Özkan, *Tanınmamış Devletlerin Yasa, Hukuki İşlem ve Kararlarının Tanınması*, Onikilevha Yayınları, İstanbul, 2017.
- İbrahim Kaya, *Terörle Mücadele ve Uluslararası Hukuk*, USAK Yayınları, Ankara, 2005.
- İlyas Doğan, *Devletler Hukuku*, Seçkin Yayıncılık, Ankara, 2008.
- Kolektif Yazarlar, *Siber Güvenliğe Giriş*, 1.Baskı, İstanbul, 2017.
- M. Yasin Aslan, "Savaş Hukukunun Temel Prensipleri", *Türkiye Barolar Birliği Dergisi*, Sayı 79, 2008.
- Malcolm, N. Shaw, *Uluslararası Hukuk*, Türkiye Bilimler Akademisi Yayınları, Ankara, 2017.
- Melda Sur, *Uluslararası Hukukun Esasları*, Dokuz Eylül Üniversitesi Yayınları, İzmir, 2000.
- Murat Metin Hakkı, "Property Wars in Cyprus: The Turkish Position according to International Law", *Ankara Bar Review*, 2010/2, s. 43-56.
- Mustafa Canlı, "Siber Güvenlik", Ankara Siyasal ve Ekonomik Araştırmalar Merkezi Raporu, Ankara, 2013.
- Nezir Akyeşilman, *Disiplinlerarası Bir Yaklaşımla Siber Politika & Güvenlik*, Orion Yayınları, 1. Baskı, Ankara, 2018.
- Nils Melzer, "Cyberwarfare and International Law", Ideas For Peace And Security, <https://unidir.org/files/publications/pdfs/cyberwarfare-and-international-law-382.pdf>. [Erişim Tarihi: 1 Mart 2021]
- Peter Warren Singer ve Allan Friedman, *Siber Güvenlik ve Siber Savaş*, Buzdağı Yayınları, Ankara, 2015.
- Ramazan Güreşçi, "Siber Saldırıların Uluslararası Hukuktaki Güç Kullanımı Kapsamında Değerlendirilmesi", *Savunma Bilimleri Dergisi*, Mayıs 2019, Cilt:18, Sayı:1.
- Rona Aybay ve Elif Oral, *Kamusal Uluslararası Hukuk*, İstanbul Üniversitesi Bilgi Üniversitesi Yayınları, 2016.
- Sertaç Hami Başeren, *Uluslararası Hukukta Devletlerin Münferiden Kuvvet Kullanmalarının Sınırları*, Ankara Üniversitesi Basımevi, Ankara, 2003.
- İbrahim Keskin, *Sibernetik*, SAY Kitap Pazarlama, İstanbul, 1982.
- Şeyda Türkay, "Siber Savaş Hukuku ve Uygulanma Sorunsalı", İÜHFM, Cilt: LXXI, Sayı:1, 2013.
- Talip Küçükcan, "Terörün Sosyolojisi: Toplumsal Kökenleri Anlama İmkanı". Mustafa Aydın, Hans Brauch, Günter Çelikpala, Mitat vd. (Der.), *Uluslararası İlişkilerde Çatışmadan Güvenliğe*, İstanbul Bilgi Üniversitesi Yayınları, İstanbul, 2012.
- Taner Sökmen Altunok ve Aşkın İnci, "Dünya'da Siber Terör Örnekleri". Haydar Çakmak ve Taner Altunok (Der.), *Suç, Terör ve Savaş Üçgeninde Siber Dünya*, Barış Platin Kitabevi, Ankara, 2009.

Toygar Akman, *Sibernetik*, Kaktüs Yayınları, İstanbul, 2003.

Yusuf Aksar, *Teori ve Uygulamada Uluslararası Hukuk – II*, Seçkin Yayınları, Ankara, 2019.

Yücel Acer, *Uluslararası Hukukta Saldırı Suçu*, Roma Yayınları, Ankara, 2004.

ULUSLARARASI HUKUK BAĞLAMINDA SİBER SALDIRI VE KKTC ÖRNEĞİ



Yakın
Doğu
Enstitüsü



YAKIN DOĞU ÜNİVERSİTESİ

www.neu.edu.tr

ISBN: 978-605-9415-62-0