SELÇUK ÜNİVERSİTESİ
HUKUK FAKÜLTESİ DERGİSİ
Selçuk Law Review

Araştırma Makalesi
Research Article
Gönderim | Received: 30.10.2019
Kabul | Accepted: 11.02.2020
10.15337/suhfd.640029

ULUSLARARASI HUKUKTA DEĞİŞEN GÜVENLİK ALGISI VE SALDIRI SUÇU BAĞLAMINDA SİBER SALDIRILAR

Arş. Gör. Erdi ŞAFAK*

Öz

Günümüzde teknolojinin gelişmesiyle birlikte kolaylaşan hayatımız, beraberinde bazı sorunları da gündeme getirmiştir. Teknolojinin gelişmesi ile birlikte uluslararası hukukun çalışma alanı ve buna bağlı olarak var olan kurallar bir takım güncellemeler ihtiyacı doğurmuştur. Özellikle silahlı çatışmalar hukukunda var olan mevcut durumda önemli değişikliklerin yaşandığını söyleyebiliriz. Teknolojinin gelişmesiyle birlikte, kara, deniz ve hava kuvvetleri komutanlıklarına, siber savunma komutanlıkları da eklenmiş ve ordular siber saldırı ve siber savaş gibi kavramlar üzerinde senaryolar üretmeye başlamıştır. Devletler açısından güvenlik kavramının önem kazanması ile birlikte savaş algısında yaşanan gelişmeler ve siber saldırı suçunun doğuşu çalışmanın inceleme alanını oluşturacaktır.

Anahtar Kelimeler

Uluslararası Hukuk • Güvenli • Savaş • Siber Saldırı • Siber Savaş.

* Arş. Gör., Yakın Doğu Üniversitesi, Hukuk Fakültesi, Kamu Hukuku Anabilim Dalı, Lefkoşa, KKTC | Asst., Near East University, Faculty of Law, Department of Public Law, Nicosia, TRNC.
erdi.safak@neu.edu.tr • ORCİD 0000-0003-4000-2468

Atıf Şekli | **Cite As**: **ŞAFAK** Erdi, "Uluslararası Hukukta Değişen Güvenlik Algısı ve Saldırı Suçu Bağlamında Siber Saldırılar", *SÜHFD*., C. 28, S. 1, 2020, s. 127-160.

İntihal | **Plagiarism**: Bu makale intihal programında taranmış ve en az iki hakem incelemesinden geçmiştir. | This article has been scanned via a plagiarism software and reviewed by at least two referees.

CHANGING PERCEPTION OF SECURITY IN INTERNATIONAL LAW AND CYBER ATTACKS REGARDING CRIME OF AGGRESSION

Abstract

While improving daily lives, rapid advances in technology have also placed a number of issues on the global agenda. More specifically, with rapid technological change, international law and its principles are now in need of revision. This also applies to the law of armed conflicts which has witnessed a number of important changes. As a result of technological advancement, cyber command is now part of the unified commands alongside naval, air and land components and the armed forces have begun to work on scenarios focusing on cyber attacks and cyber warfare. This article provides a review of the recent developments related to the concept of cyber crime in the context of changes to our understanding of security and of war.

Key Words

International Law • Security • War • Cyber Attacks • Cyber War.

GİRİŞ

Uluslararası ilişkilerin temel çalışma alanlarından olan "Güvenlik" kavramı, uluslararası hukukun da inceleme alanında yer almaktadır. Uluslararası hukukun bir diğer inceleme alanı olan silahlı çatışmalar hukuku kapsamında da, çatışma ya da savaş kuralları belirlenmeye çalışılmıştır. Devlet kavramının ortaya çıktığı 1648 Westphalia düzeninden bu yana, dünyamız birçok savaşa tanıklık etmiş ve bu savaşlar genellikle, kara, hava ve deniz unsurları ile icra edilmiştir. Ancak, günümüzde teknolojinin gelişmesiyle birlikte belirtilen bu üç unsura yakın gelecekte siber alanın da dâhil edileceği ve devletlerin bu alanda da savaşacakları ön görülmektedir. Bu nedenle siber alan ve siber savaş gibi kavramlar, uluslararası hukuk bağlamında incelenmesi ve kurallarının belirlenmesi ihtiyacı her geçe gün artmaktadır.

Siber alan en genel tabiri ile dünyadaki tüm bilgisayar ağları ve onların bağlı olduğu ve kontrol ettiği her şeydir. Bu alanda devletlerin ya da bireylerin birbirlerine karşı gerçekleştirmiş olduğu yasa dışı faaliyetler ise siber saldırı olarak değerlendirilmektedir. Siber savaş ise, yine siber alanda devletlerin birbirlerine karşı yürüttüğü askeri faaliyetler ile aynı etkiye sahip, çatışma biçimidir denilebilir. Güvenliğin insanlık için esas alındığı temel noktadan, savaş kavramının tanımı ve savaşın yeni-

den şekillenmesi süreci aşamasında siber savaş çalışmamızın ana temasını oluşturacaktır.

Savaş olgusunda yeni düşünceleri gündeme getiren siber saldırı ve siber savaş çalışmanın temel inceleme konusu olacaktır. Bu noktadan hareketle, çalışmamız genel olarak 3 bölümden oluşacaktır. Birinci bölümde güvenlik ve savaş kavramları açıklanmaya çalışılacaktır. İkinci bölümde savaş olgusunda yaşanan değişime paralel olarak siber saldırı ve siber savaş kavramları üzerinde durulacaktır. Son bölümde ise, siber saldırı ve siber savaş durumlarında uluslararası hukuk mekanizmasının ne şekilde işleyebileceği irdelenecektir.

I. Genel Olarak Güvenlik ve Savaş Kavramlarının Tanımları

A. Güvenlik Kavramı Tanımı

Güvenlik kavramı Latince *se* (olmaksızın) ve *cura* (endişe) kelimelerinin birleşmesinden oluşan *securites* kelimesinden türemiştir. Kavram dikkatli bir biçimde tercüme edildiğinde, *securitas*, "endişeden uzak olma ve sükûnet" anlamına gelmektedir[1]. "

Güvenlik terimini uluslararası ilişkiler literatüründe farklı şekillerde açıklamak mümkündür. Bu tanımlardan hareketle güvenlik kavramı devletlerin, toplumların, grupların ve bireylerin varlıklarını koruma ve sürdürme yolundaki faaliyetleri ile bunları tehdit eden unsurların bertaraf edilmesine yönelik algıları, araçları, uygulamaları ve politikaları kapsamaktadır. Ayrıca güvenlik, değişen ve gelişen dinamiklere göre de her seferinde yeniden şekillenmektedir[2].

Güvenlik, sosyal bilimlerde genel çerçeve ve boyutlara tekabül eden bireylere, konulara, toplumsal adetler ile değişen tarihsel şartlara ve durumlara uyarlanan temel bir kavramdır. Güvenlik kavramı barış ile yakından ilgilidir ve ulus-devlet[3], devlet-üstü ve devlet-dışı aktörler için olağanüstü önlemler gerektiren bir değer ve hareket amacıdır[4].

---

1 **ARENDS J. Frederik**, "Homeros'dan Hobbes ve Ötekine: Avrupa Geleneğinde 'Güvenlik' Kavramı", *Uluslararası İlişkilerde Çatışmadan Güvenliğe*, Derleyenler: AYDIN, Mustafa, BRAUCH, Hans, Günter, ÇELİKPALA, Mitat vd., İstanbul Bilgi Üniversitesi Yayınları, İstanbul, 2012, s.199.

2 **DEDEOĞLU Beril**, "Yeniden Güvenlik Topluluğu: Benzerliklerin Karşılıklı Bağımlılığından Farklılıkların Birlikteliğine", *Uluslararası İlişkilerde Çatışmadan Güvenliğe*, Derleyenler: AYDIN, Mustafa, BRAUCH, Hans, Günter, ÇELİKPALA, Mitat vd., İstanbul Bilgi Üniversitesi Yayınları, İstanbul, 2012, s.369.

3 Ulus düşüncesi, ilk olarak 1689'da İngiltere'de vatandaşlık haklarının kabulü ile ulusal egemenliğe dayalı ve ulus-devletin ortaya çıkmasında zemin oluşturan ana-

Güvenlik tanımlarında kullanılan en önemli kavram tehdit kavramıdır. Güvenlik daha çok güvensizlik ihtimallerinin ortadan kaldırılması durumu olarak değerlendirildiğinde, güvensizlik durumlarının kaynağının tehdit olduğu görülmektedir. Bir güvenlik olgusundan bahsedebilmek için varlığın korunması ve sürdürülmesi açısından bir tehdidin bulunması gerekmektedir. Söz konusu tehdit içsel ya da dışsal olmak üzere bir veya birden fazla olabilir. Tehdidin gerçekten var olmasının yanında, tehdidin varlığına yönelik algılamalar da yeterlidir. Bu yönüyle tehdit, bir taraftan da algı ve tahminlere dayanmaktadır[5].

21. Yüzyılda savaşın bir uluslararası politika seçeneği olarak ortadan kalktığını iddia etmek olası gözükmemektedir. Ancak, saldırı belirgin bir biçimde şekil değiştirmiştir. Günümüzde barışın temel tehdit kaynakları uluslararası çatışmalar değildir. Tehditler ulusların kontrol edemedikleri veya tam anlamıyla kontrol edemedikleri diğer önemli sorunlardır. Bunların başında terörizm, etnik çatışmalar, uluslararası hukuk ihlalleri, kitle imha silahlarının yaygınlaşması, şiddeti artan ekonomik rekabet, siber saldırılar ve siber terörizm gelmektedir. Geleceğin nasıl bir dünya getireceği, yeniden büyük çaplı çatışmaların yaşanıp yaşanmayacağı, ulusların "modern savaşlar"la etkin mücadele edebilme kapasitesine bağlı olacaktır[6].

Güvenlik söylemlerinde güvenlik tehlikeleri için farklı kavramlar kullanılmaya başlanmıştır. Hem sert (askeri) güvenlik, hem de yumuşak (uyuşturucu, insan ticareti, göç) güvenlik konularına ilişkin olarak tehditler, hassasiyetler, çatışma alanları, belirsizlikler ve riskler önem taşımaktadır. Sınırların ortadan kalkması, topluluklaşan diğer konuların

---

yasal monarşinin oluşma süreciyle ortaya çıkmıştır. Daha sonra, Fransız ve Amerikan devrimleriyle ulus düşüncesi, siyasal ve toplumsal örgütlenmede evrensel bir konuma gelmiştir. Detaylı bilgi için bakınız: **ZABUNOĞLU H. Gökçe**, "Günümüzde Ulus Devlet", *Erciyes Üniversitesi Hukuk Fakültesi Dergisi*, Cilt. XIII, 2018, s.1.

4 **BRAUCH, Hans Gunter**, "Güvenliğin Yeniden Kavramsallaştırılması: Barış, Güvenlik, Kalkınma ve Çevre Dörtlüsü, *Uluslararası İlişkilerde Çatışmadan Güvenliğe*, Derleyenler: AYDIN, Mustafa, BRAUCH, Hans, Günter, ÇELİKPALA, Mitat vd., İstanbul Bilgi Üniversitesi Yayınları, 2012, s.168.

5 **DEDEOĞLU, Beril**, Uluslararası Güvenlik ve Strateji, 3. Basım, Yeniyüzyıl Yayınevi, İstanbul, 2008, s.22. / **BAYRAKTAR, Gökhan**, Siber Savaş ve Ulusal Güvenlik Stratejisi, Yeniyüzyıl Yayınevi, İstanbul, 2015, s.27.

6 **YILMAZ Muzaffer Ercan**, "Westphalia'dan Günümüze Savaş", *Uluslararası İlişkilerde Çatışmadan Güvenliğe*, Derleyenler: AYDIN, Mustafa, BRAUCH, Hans, Günter, ÇELİKPALA, Mitat vd., İstanbul Bilgi Üniversitesi Yayınları, İstanbul, 2012, s.87.

aksine hükümetler – arası yapılara dayanan iki güvenlikleştirme stratejisiyle tanımlanmıştır. Uluslararası örgütler bağlamında da artık çevresel güvenlik, gıda güvenliği, siber güvenlik, enerji güvenliği ve geçim güvenliği gibi sektöre özel güvenlik kavramları yaygın olarak kullanılmaktadır[7].

Güvenlik kavramı yukarıda da açıkladığımız üzere, genellikle askeri bir kavram olarak düşünülmüş ve güç unsuru ile birlikte değerlendirilmiştir. Güvenliğin olmadığı durumlarda ise çatışma ya da savaş durumlarından bahsedilebilir. Biz de bu noktadan hareketle konumuz ile ilgili olarak savaş kavramını ve tarihsel süreç içerisinde savaş olgusunda yaşanan değişimi açıklamaya çalışacağız.

B. Güvenlik ve Barış Kavramlarının Karşıtı Savaş Kavramı

Savaş bir zamanlar pragmatik bir eylem olduğu kadar, bir ritüel olarak da tasvir edilmiştir. Avlanma, insan öldürme ve kendini feda etme, yani savaşın ataları başlangıçta tamamen dinsel etkinliklerdi. Bu pratiklerin çoğu olan savaş, bu mantığın bir ürünü olarak maddi ve manevi etkinlikle etkili ve kutsal gösteriyi bağdaştırmaktaydı. Savaş, sivilleşmeye başladıkça, şov artık giderek daha az kader, Tanrılar ve Tanrıçalar için ve daha çok iki tarafın da savaşçılarının morali için yapılır olmuştur[8].

Uluslararası hukuk belgelerinde savaşın genel bir tanımı yapılmamaktadır. Uluslararası Sürekli Hakemlik Mahkemesi "Osmanlı Savaş Zarar – Giderimi Davası"[9]ndaki 11.11.1912 tarihli kararında savaşı "*uluslararası bir olay"* olarak tanımlamak suretiyle savaşın yalnızca devletler arasında gerçekleşen silahlı çatışma yanını vurgulamıştır[10].

Kuvvet kullanmayı ve şiddeti içeren bir çatı kavram olan savaş, genellikle devletler tarafından icra edilmektedir[11]**.** Muharebe veya çar-

---

7 **BRAUCH**, s.177.

8 **GRAY Chris Hables**, Postmodern Savaş – Yeni Çatışma Politikası, (Çeviren: Derya Kömürcü), Alfa Yayınları, İstanbul, 2000, s.58.

9 "Osmanlı Savaş Zarar – Giderimi Davası" hakkında detaylı bilgi için bakınız: **MERAY Seha L**., Lozan Barış Konferansı – Tutanaklar – Belgeler, Takım 1, Cilt:3, Ankara Üniversitesi Siyasal Bilgiler Fakültesi Yayınları, No:320.

10 **PAZARCI Hüseyin**, Uluslararası Hukuk, 15. Basım, Turhan Kitabevi, Ankara, 2016, s.538.

11 Savaş sadece devletler arasında icra edilmemektedir. Devletlerin terör unsurları ile mücadelesi de zaman zaman terörle savaş şeklinde değerlendirilebilmektedir. Ancak biz konumuzun alanını genişletmemek adına "savaş" kavramı ile devletler arasında icra edilen silahlı çatışmaları ifade edeceğiz.

pışma ise savaşa nazaran daha dar bir kavramdır. Savaş sırasında silahlı çatışmanın gerçekleşmediği durumlarda bile askerî faaliyetlerin ve/veya millî gücün diğer unsurlarının güç vasıtası olarak kullanılması söz konusudur. Muharebede ise mutlak surette askerî gücün silahlı mücadelesi gerçekleşir. Savaş doğrudan devlet eliyle yürütülürken muharebe ve askerî harekât silahlı kuvvetler tarafından icra edilir. Uygulamada çarpışma sözcüğü, çatışmadan daha büyük seviyedeki birliklerin yakın muharebesi anlamında kullanılmaktadır. Askerî doktrinde ise "çatışma" sözcüğünün, çatışmanın özel niteliğinin belirtildiği, etnik çatışma, kültürel çatışma, menfaat çatışması vb. bir gerginlik durumunu açıklayan anlamı dışında tek başına kullanıldığında "silahlı çatışma" hâli anlaşılmaktadır[12].

Çağımızın savaşları, cephelerden siber ortama taşınmış olup bilgi güvenliğinin önemi ve devlet kurumlarının gizliliği, halkın devlete olan güveni siber dünyada sözü geçen kişilere/devletlere bağlı belirlenmektedir. İşte bu nedenler, ülkelerin fiziksel askeri yatırımlarının yanı sıra bilişim alanına da yansımış olup sözün tam anlamıyla "siber ordu"lar kurulmaya başlamıştır[13]. 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, kara, hava ya da deniz alanları gibi değildir. Siber alanda bir muharebe alanının ve sınırlarının kesin olmayışı, siber alanın savaş ortamından çok bir mücadele ortamı olarak düşünülmesine neden olmuştur[14].

Geleneksel savaşlara baktığımızda genellikle bir "ilan ediliş" görülmektedir. Bir ülke, bir başka ülkeye böylelikle savaşını başlatmış olmaktadır. Oysa siber dünyada sözü edilen savaş bu şekilde gerçekleşmemektedir. Dahası, tam tersi olarak bir ülke, bir ülkeye siber saldırı düzenlediğinde bunu dahi kabul etmez, etmek istemez. Esasen bu durum siber saldırının bir "savaş" olarak açıklanmasından kaçınılması olarak kabul edilebilir. Zira savaş sözcüğü ağırlığı olan bir konumdadır ve ülkelerin müttefiklerinin de bu savaşa dâhil olması da pek muhtemeldir. Ülke çapında yapılan siber saldırılardan sonra yapılan açıklama-

---

12 **VARLIK Ali Bilgin,** Savaşı Tanımlamak: Terminolojik Bir Yaklaşım, Avrasya Terim Dergisi, Cilt: 1, Sayı: 2, 2013, s. 126.

13 **Kolektif Yazarlar**, Siber Güvenliğe Giriş, Kutlu Yayınevi, İstanbul, 2017, 1.Bası, s.58.

14 **Siber Güvenliğe Giriş**, s.58.

lar ağırlıklı olarak olayı, "milli duygular kapsamında kabiliyetlerini kullanan bir gruba" aksettirir. Esasen de ortada bir savaş yoktur, zira tarafların karşılaşmasından ziyade birbirlerine siber uzayda zarar verme, bilgi manipüle etme, sosyal medyada propaganda yapma, bilişim sistemlerini aksatma gibi sabotaj eksenli siber ataklar söz konusudur[15].

II. Değişen Güvenlik Algısı Bağlamında Siber Saldırı, Siber Savaş ve Siber Terörizm

Siber alan, kara, hava, deniz ve uzay alanlarından aktörler, kurallar, sınırlar, boyutlar, süreçler ve ilişkiler açısından oldukça farklı olduğundan, siber alanı anlayabilmek için geleneksel araçlardan ve teorilerden farklı kavramsal ve kuramsal bir çerçeveye ihtiyaç duymaktadır. Uluslararası ilişkiler ve siber alanın birbirini şekillendirmeye başladığı günümüzde, bu karşılıklı etkileşim ve bağımlılığı okuyabilmek, anlayabilmek ve anlamlandırabilmek için mevcut durumda oldukça az ve etkin olmayan kavramsal ve kuramsal araçlar mevcuttur. Siber teknolojisindeki gelişmeler son yıllarda dünya politikasında meydana gelen askeri, sosyal, ekonomik ve siyasal faaliyetleri derinden etkilemektedir[16]. Bu noktadan hareketle çalışmamızın bu bölümünde siber saldırı, siber savaş ve siber terörizm kavramlarını açıklamaya çalışacağız.

A. Siber Saldırı ve Siber Savaş

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 tür eylemler literatürde "siber saldırı" olarak ifade edilmektedir[17]**.** Siber saldırı, siber alanda yer alan bilgileri istismar etmek, bozmak, değiştirmek, sistemlere erişimi engellemek ya da zarar vermek amacıyla siber alanda gerçekleştirilen faaliyetlerdir[18]. Başka bir tanımda ise siber saldırı, saldırganlar tarafından bilgi sistemlerinin çalışılamaz hale getirilmesi, bilgi sistemlerinin güvenliğinin veya güvenirli-

---

15 **Siber Güvenliğe Giriş**, s.105.

16 **AKYEŞİLMAN Nezir**, Disiplinlerarası Bir Yaklaşımla Siber Politika & Güvenlik, Orion Kitabevi, Ankara, 2018, s.180.

17 **ÇİFCİ Hasan**, Her Yönüyle Siber Savaş, İkinci Basım, TÜBİTAK Yayınları, Ankara, 2017, s.6.

18 **ÇİFCİ,** s.6.

ğinin riske atılması, bozulması veya çalınması şeklinde ifade edilmektedir[19].

Siber saldırıların ne olduğunun anlaşılması noktasında öncelikle yapılması gereken, konunun geleneksel saldırılardan ayırt edilmesi gerektiği ile ilgilidir. İlk olarak siber saldırılarda genellikle farklı araçlar kullanılmaktadır. Siber saldırıda kinetik güç (yumruk, kılıç, bomba, silah vb.) kullanmak yerine, dijital araçlar (bir çeşit bilgisayar hareketi) kullanılır. Bu nokta önemlidir çünkü bir siber saldırı geleneksel saldırıların olağan fiziği 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[20].

Bir siber saldırının farklılaştığı ikinci yön hedeftedir. Doğrudan fiziksel hasara sebep olmak yerine bir siber saldırı daima ilk olarak bilgisayarı ve ondaki bilgiyi hedef almaktadır. Niyet edilen saldırının sonucu fiziksel bir şeye hasar vermek olabilir ancak hasar daima ilk olarak dijital âlemdeki bir olaydan doğmaktadır[21].

Günümüzde ordu birimleri arasında her türlü bilgi alış-verişi genel olarak 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 çökertmek amacıyla yapılmaktadır[22].

---

19 **CANLI Mustafa**, "Siber Güvenlik", *Ankara Siyasal ve Ekonomik Araştırmalar Merkezi Raporu*, Ankara, 2013, s.8.

20 **SINGER Peter / FRIEDMAN Warren Allan**, *Siber Güvenlik ve Siber Savaş*, Buzdağı Yayınevi, Ankara, 2015, s.101.

21 **SINGER/FRIEDMAN**, s.101.

22 **BAYRAKTAR**, s.137.

Bu bilgiler doğrultusunda siber savaş en genel tanımı ile *"devletlerin birbirine karşı yürüttüğü siber saldırı faaliyetleridir*[23]*"*. Bu tanımda dikkat edilecek iki husus bulunmaktadır; Bunlardan ilki siber savaşın devletler arasında cereyan etmesi; diğeri ise karşı tarafın sistemlerine hasar vermeye veya sistemlerinde kesinti yapmaya yönelik eylemlerin siber savaş olarak nitelendirilmesidir. Bu tanıma göre karşı tarafın sistemlerine zarar vermeden bilgi çalmak siber savaş olarak kabul edilmemektedir[24].

Siber savaş sadece devletlerin birbirlerine karşı yürüttüğü siber saldırı faaliyetleri olarak tanımlanmamaktır. Uluslararası hukuka göre, bir devletin hükümetine karşı silahlı mücadele veren güçlere de savaşan statüsü tanınabilmektedir[25]. Bu durumda silahlı mücadelenin siber ekipmanlar aracılığı ile gerçekleştirilmesi neticesinde meydana gelen çatışmalar siber savaş olarak değerlendirilebilecektir.

Siber savaşlar stratejik, operatif ve taktik olmak üzere her seviyede uygulanabilir olma özelliğine sahiptir. Bu nedenle her seviyede istenen etki elde edilebilmektedir. Hedef olarak ise siber savaşlar, temel olarak ülkelerin kritik bilgi sistem altyapılarını hedef almaktadır. Siber savaş sayesinde bu altyapıların hizmet dışı bırakılmasının yanı sıra ülkelerin sivil ve askeri hassas ve kıymetli bilgilerine ulaşılabilmektedir. Söz konusu bilgiler çalınabilmekte hatta silinebilmektedir. Ayrıca saldırıya maruz kalan ülke halkını ve yönetimini, siber ortamda dezenformasyon ile psikolojik olarak etkilemek de mümkün olabilmektedir. Bu nedenle siber savaşlar toplumun her kesimini etkileyebilmekte, çatışma ve rekabet ortamı yaratabilmektedir[26].

B. Siber Terörizm

Terör[27] ile ilgili günümüzdeki literatüre bakıldığında, bu tür olaylara ilişkin tanım ve açıklamaların odak noktasını "siyasi amaçlı şiddet eylemi" vurgusunun oluşturduğu görülmektedir[28].

---

23 **FLOWERS, Angelyn**, "Cyberwar: The What, When, Why and How", *IEEE Technology And Society Magazıne*, 2014, s.14.
file:///C:/Users/NewTech/Downloads/Cyberwar_The_What_When_Why_and_How_Commentary%20(1).pdf

24 **ÇİFCİ**, s.7.

25 **PAZARCI**, s.537-540.

26 **BAYRAKTAR**, 49.

27 Terör Türk Dil Kurumu sözlüğünde "Yıldırı" anlamında kullanılmakta olup, uluslararası ilişkiler literatüründe değişik birçok farklı tanıma sahiptir. Terör ile ilgili

Terörizm modern bir olgu olmayıp, her çağda var olmuştur. Ancak terörizm açısından Soğuk Savaşın sona ermesinin yanı sıra özellikle 11 Eylül saldırıları[29] bir milat olarak kabul edilmektedir. Esasen 1990'lı yılların ortasından itibaren kendinden önceki terör uygulamalarından önemli bir farklılık göstermeye başlayan terörizm, değişen organizasyon yapısı ve benimsediği yeni yöntemlerle "yeni terörizm" olarak adlandırılmaya başlamıştır[30].

11 Eylül 2001 İkiz Kule saldırılarından sonra terörizm ve güvenlik söylemleri, terörü ve dolaylı olarak siber terörizm tehdidi endişelerini arttırmıştır. Bu çerçevede uzman politik ve psikolojik birimler bir araya gelerek siber terörizm tehdidini araştırmaktadırlar. Psikolojik perspektife göre modern dönemlerin en büyük korkularından biri de, "siber terörizm" olmuştur. Modern araçlardan ve alışkanlıklardan kaynaklanan mağduriyet korkusu, bilgisayar teknolojilerine olan güvensizlik ve endişe ile birleşerek siber terörizm korkusunu yaratmıştır. Buna rağmen siber terörizm doğrudan bir şiddet tehdidi sunmamaktadır; fakat tedirgin toplumlarca yapacağı psikolojik darbe, terörist bir bombanın etkisi kadar zarar verici olabilir. Daha da ötesi siber saldırılara karşı mücadele çalışmaları, en büyük ve gerçek tehdidin bilinmezlikten, bilgi eksikliğinden ve daha da kötüsü yanlış bilgilerden kaynaklandığı ortaya çıkmıştır[31].

Siber terörizme odaklanmanın birde politik boyutu vardır. Siber terörizm ile ilgili güvenlik tartışmaları her zaman için siyasi aktörlerin

---

detaylı bilgi için bakınız: **TOPAL, Ahmet Hamdi**, Uluslararası Terörizm ve Terörist Eylemlere Karşı Kuvvet Kullanımı, Beta Yayınları, İstanbul, 2005.

28 **KÜÇÜKCAN Talip**, "Terörün Sosyolojisi: Toplumsal Kökenleri Anlama İmkanı", *Uluslararası İlişkilerde Çatışmadan Güvenliğe*, Derleyenler: AYDIN Mustafa, BRAUCH Hans Günter, ÇELİKPALA, Mitat vd., İstanbul Bilgi Üniversitesi Yayınları, İstanbul, 2012, s.102.

29 11 Eylül 2001 tarihinde Amerika Birleşik Devletleri Washington ve New York'ta kaçırılan uçaklarla düzenlenen terör saldırılarında, 2 bin 977 kişi hayatını kaybetmiştir. Ayrıca uçakları kaçıran 19 hava korsanı ölmüş, Saldırılarda 6 binden fazla kişi ise yaralanmıştır. Konu ile ilgili detaylı bilgi için bakınız: "11 Eylül saldırıları: 2001'de neler yaşandı, 18 yılda neler değişti?",
https://www.bbc.com/turkce/haberler-dunya-49653233. E.T. 12.10.2019.

30 **KURT Selim**, "Yeni Terörizmin Geleceğin Güvenlik Ortamına Etkileri: DAEŞ Örneği," *Geleceğin Güvenliği*, Editör: Ahmet Yıldız, TASAM Yayınları, İstanbul, 2019, s.209.

31 **SANDIKLI Atilla/ YİVCİVER Gökhan**,Siber Terörizm Stratejik Rapor, TASAM Yayınları, İstanbul, 2014, s.2.

ilgisini çekmiş ve indirgemeci bir yaklaşımla değerlendirilmiştir. Bu açıdan bakıldığında siber terörizm zaman zaman küresel siyasetin ve "güç" unsurunun önemli bir parçası haline gelmiştir[32].

Siber terörizm, siber boşluk ve terörizm bileşimidir. Siber terörizm, siyasi ve sosyal mercilere ve kişilere gözdağı vermek, baskı oluşturmak maksadıyla resmi birimlerin bilgisayarlarına, network sistemlerine, bilgi veri tabanlarına yapılan yasadışı tehdit ve zarar verici saldırılardır. Daha da ötesi, bir saldırının siber terörizm olarak tanımlanması için bireye ya da mala karşı şiddet içermesi gerekmektedir. En azından "korku yaratacak kadar hasara" yol açmalıdır. Siber terörü ölümcül olan ya da fiziki hasara yok açan, şiddetli ekonomik kayba neden olan saldırılar olarak örneklenebilir[33]. Kritik altyapı odaklarına yapılan ciddi saldırılar yarattığı etkiye göre siber terörizm olarak tanımlanabilir. Önemli olmayan servislere verilen rahatsızlıklar siber terörizm olarak tanımlanamaz[34].

C. Yeni Konsept Savaş Alanında Kullanılan Siber Saldırı Türleri

II. Dünya Savaşı'nın ardından başlayan Soğuk Savaş Dönemi boyunca devletler silahlanma yarışından bir an olsun geride durmamışlardır. Bu süreçte üretilen konvansiyonel silahların yanı sıra kitle imha silahı türleri ve miktarlarında da kontrolsüz bir artış meydana gelmiştir. Bunun sonucunda ise, dünya her geçen gün daha da güvensiz bir yer haline gelmiştir[35].

Dünyanın yaşamakta olduğu güvenliksiz haline son olarak siber saldırı türleri de eklenmiştir diyebiliriz. Siber saldırı türleri ile ilgili literatürde çok fazla farklı kavramlar bulunmaktadır. Bu türler arasında amaç ve yöntemleri ile failler ve sonuçlar yönünden birbirleri ile örtüşenleri olduğu gibi, ayrışanları da bulunmaktadır. Bu nedenle bu bölümde daha çok uluslararası saldırı neticesi oluşturabilecek eylemlerde kullanılan siber saldırı türleri ve örnek olaylar üzerinde durulacaktır.

---

32 **SANDIKLI/YİVCİVER**, s.3.

33 **BRENNER Susan W. / CLARKE Leo L**., "Conscription and Cyber Conflict: Legal Issues", *CCD COE Publications,* 2011. https://ccdcoe.org/uploads/2018/10/ConscriptionAndCyberConflictLeaglIssues-Brenner-Clarke.pdf.

34 **SANDIKLI/YİVCİVER**, s.3.

35 **KARATAŞ Salih**, Uluslararası Hukukta Silahsızlanma ve Kimyasal Silahların Yasaklanması Örgütü (OPCW), Yüksek Lisans Tezi, Selçuk Üniversitesi Sosyal Bilimler Enstitüsü Kamu Hukuku Anabilim Dalı, Konya, 2014, s.3.

a. Virüsler ve Solucanlar

Virüsler bir programın içerisinde gömülü olarak bulunan, mevcut sistem içerisinde çoğalabilen, bir dosyadan veya programdan diğerine yayılabilen, dosyalar kopyalandığı ve paylaşıldığı zaman diğer bir bilgisayara da bulaşabilen ve dosyalara zarar veren bilgisayar programıdır[36]. Virüs terimi, bir bilgisayarı zararlı yazılımlarca saldırıya maruz bırakacak tüm değişik yöntemleri belirtmekte kullanılan genel bir terim halini almıştır[37]. Bir virüs ile bilgisayar takip edilebilir, şifre çalınabilir, reklam gösterme ya da sistemi çökertme gibi fonksiyonlar yerine getirebilir. Virüslerin en önemli özelliği yayılma yöntemleridir. Örneğin, bir taşınabilir USB bellek üzerinde bir dosyaya virüs bulaşmışsa, o bellek bir bilgisayarda çalıştırıldığında virüs o bilgisayardaki dosyalara bulaşır. Bellek başka bir bilgisayara takıldığında ona da bulaşır ve bu yolla çoğalmaktadır[38].

Solucanlar ise virüslere benzerler fakat farklı şekilde yayılırlar. Solucanlar bir dosyaya bulaşıp insan hareketiyle yayılmak yerine, ağ üzerinden kendi kendine yayılır ve bulaşırlar. Virüs gibi, solucanlar da bir bilgisayara bulaştıktan sonra bir dizi zarar verebilir[39]. Solucanlar çok hızlı ve büyük sayılarda çoğalabilen, e-postalar veya dosyalar ile diğer bilgisayarlara bulaşmakta ve hedef bilgisayarın kilitlenmesine ve internet sayfaları açılırken de uzun süre beklemesine neden olmaktadır[40].

Virüsler ya da solucanlar ile ilgili gerçekleşen örnek olay, 2010 yılında İran'da yaşanan "*Stuxnet Saldırısı*"dır. Stuxnet saldırısı, İran'ın nükleer tesislerini hedef alan Amerika Birleşik Devletleri (ABD) ve İsrail uzmanları tarafından üretildiği tahmin edilen ve zarara neden olan bir koddur. Stuxnet bulaştığı hedef sisteme "*ortadaki adam*" yazılımını yerleştirerek makine ile kontrol bilgisayar arasındaki bağı koparmaktadır. İkinci olarak ana bilgisayara bir sorun göndermeyerek, sistemdeki hatayı kamufle etmektedir[41]. Saldırı neticesinde İran'ın nükleer çalışmaları sekteye uğramış ve 30 bin bilgisayar bu virüsten etkilenmiştir. Stuxnet

---

36 **YILMAZ Abdullah Batuhan**, "Siber Ağ Güvenlik kavramının Gelişimi", *CyberMag Deregisi*, Sayı:32, Ankara, 2018, s.15.

37 **BÜLBÜL İsmail – BİNGÖL Poyraz Emre**, Etik Hackerlığa Giriş – Ofansif Siber Güvenliğin ABC'si, Hayy Kitap, İstanbul, 2018, 5. Baskı, s.33.

38 **AKYEŞİLMAN**, s.76. / **BÜLBÜL – BİNGÖL**, s.33-37.

39 **AKYEŞİLMAN**, s.77. / **BÜLBÜL – BİNGÖL**, s.45.

40 **YILMAZ**, s.15 / **BÜLBÜL – BİNGÖL**, s.45.

41 **AKYEŞİLMAN**, s.243.

virüsünün (ya solucanının), Çernobil benzeri bir nükleer felakete yol açabileceği iddia edilmiştir[42].

b. Hizmet Engelleme (Dos/Dos) Saldırısı

Siber saldırı türleri arasında en yaygın olanı "*Hizmet Dışı Bırakma"* (Dos/Dos -Denial of Service) saldırılarıdır. Bu saldırı türünde amaç hedef sistemini veya bilgisayarını kullanıcıların taleplerine cevap veremez hale getirmektir. Hizmet engelleme saldırıları tek bir kaynaktan gelmektedir ve hedefin başka sistemlerle iletişim kurmasını engellemeyi amaçlar. Bu saldırı türüne örnek olarak, kullandığımız sisteme doğrudan bir saldırı yapılmak yerine saldırının Domain Name System (DNS) sunucusuna yöneltilmesi verilebilir. Bu durumda Internet Protokol (IP) çözümlemesi yapılamayacağından internet bağlantısı da çalışmayacaktır[43].

Hizmet engelleme saldırıları ile ilgili örnek olayımız 2007 yılında Estonya'da gerçekleşmiştir. Estonya hükümetinin başkent Tallinn'in merkezinde bulunan 2.Dünya Savaşı'nda Sovyetlerin, Nazilere karşı zaferini temsil eden Bronz asker heykelini şehrin kıyısında bir mezarlığa taşımaya karar vermesiyle, önce ülkede bulunan Rus azınlığı protesto gösterileri düzenlemiş, ardından ülkeye siber saldırı gerçekleştirilmişti. Yüzbinlerce bilgisayar üzerinden botnetler[44] kullanılarak yapılan "Hizmet Dışı Bırakma" saldırıları sonucu bir ay boyunca onlarca resmi, özel, kurum ve kuruluş, ticari, finans ve kritik altyapı sitelerinin hizmetleri yavaşlatılmış ya da tamamen durdurulmuştu. Bütün hükümet websiteleri, iki büyük banka, gazeteler, parlamento e-mail servisleri, para çekme makinaları ve çok sayıda özel ticari site hizmet veremez duruma gelmişti[45].

c. Truva Atları

Truva atları içlerinde kötü amaçlı yazılımlar bulunduran yazılımlardır. Bunlar genellikle kullanıcının isteyeceği özellikleri sunar ve çoğu zaman kurban bunları kendi isteğiyle indirip kurmaktadır[46]. Truva atı, başlangıçta kullanıcıya iyi niyetli ve zararsızmış gibi gözüken ancak

---

42 **ÇİFCİ**, s.190-191.

43 **BAŞARAN Alper**, Siber Savaş Cephesinden Notlar, Arion Yayınevi, İstanbul, 2016, s.29.

44 Botnet sözcüğü, "robot" ve "network" (ağ) sözcüklerinin birleşiminden türetilmiştir.

45 **AKYEŞİLMAN**, s.239.

46 **BAŞARAN**, s.31-32. / **YILMAZ**, s.16.

gizli bir şekilde yerleştiği bilgisayarın arka planında zarar vermeye yönelik faaliyetler icra eden programlardır[47].

Truva atı farklı amaçlarla yüklenebilmektedir. Bilgisayarda yapılanları izlemek, bilgisayarı gerektiğinde bir takım suçlarda kullanmak üzere zombileştirmek, bilgisayar üzerinden hizmet engelleme saldırıları gerçekleştirmek, diğer siber suçlar gerçekleştirmek ya da bu yolla bilgisayarlara farklı programlar yüklenebilir[48].

D. Siber Saldırılardan Ötürü Devletlerin Sorumluluğu ve İsnat Edilebilirlik Meselesi

Uluslararası hukuka göre, bir siber saldırı neticesinde uluslararası hukukun kurallarının çiğnemesi durumunda, bu fiilin sahibinin uluslararası sorumluluğu gündeme gelmektedir. Böylece eğer kuralları çiğneyen bir devletse bu devletin uluslararası sorumluluğu söz konusu olmaktadır. Bu bölümde siber saldırılar ile ilgili devletlerin sorumluluğunu ve siber saldırı eylemlerinin isnat edilmesi meselesini inceleyeceğiz.

I. Siber Saldırlar ile İlgili Devletlerin Sorumluluğu

Birinci Dünya Savaşı sonrasında uluslararası sorumluluğun kapsamı daha geniş bir şekilde ele alınmaya ve tartışılmaya başlanmıştır. Bu dönemde uluslararası hukuk literatüründe "devletlerin işlediği suç" ve "tüm devletlere karşı sorumluluk" gibi kavramlar girmiştir. Uluslararası hukukta bazı kuralların emredici nitelikte olduğunun ve bu kuralların ihlalinin uluslararası topluluğu bir bütün olarak ilgilendirdiğinin, dolayısıyla da doğrudan zarar görmese bile başka devletlerin de bu kuralların ihlali durumunda uluslararası sorumluluk mekanizmalarını harekete geçirme hakkının bulunduğunun kabulü, söz konusu iki taraflı sorumluluk düşüncesini değiştirmiştir. Bunun yanında, teknolojik gelişmeler, çevreye verilen zararlarda olduğu gibi, uluslararası sorumluluğun doğuşunun sadece hukuka aykırı eylemlerden doğması koşulunu da işlevsiz hale getirmiştir[49].

Uluslararası hukukta devletlerin işlemiş olduğu eylemlerden sorumlu tutulabilmesi bazı koşullara bağlıdır. Devletin sorumluluğunu doğuran olay, devlete yüklenebilen, milletlerarası hukuka aykırı bir ey-

---

47 **YILMAZ**, s.15.

48 **AKYEŞİLMAN**, s.239.

49 **UZUN Elif**, Milletlerarası Hukuka Aykırı Eylemlerinden Dolayı Devletin Sorumluluğu, 1. Basım, Seçkin Yayınları, Ankara, 2017, s.40.

lemin varlığıdır. Dolayısıyla, en genel şekliyle, devletin sorumluluğunun ortaya çıkması için iki koşulun bulunduğunu söylemek mümkündür. Bunlar; 1) Bir devletin uluslararası hukuk uyarınca sahip olduğu bir yükümlülüğü ihlal eden bir eylemin varlığı ve 2) bu eylemin o devlete yüklenebilmesidir. Doğrusu, eylemin uluslararası hukuka aykırı olması ile devlete yüklenebilmesi, birbirinden ayrılması güç iki niteliktir[50].

Kuzey Atlantik Antlaşması Örgütü (NATO) tarafından, siber saldırılar ile ilgili uluslararası hukuk uzmanlarına hazırlatılan Tallinn Kitapçığı'nın 6.maddesi "Devletlerin Yasal Sorumluluğu" başlığı ile devletlerin sorumluluğu ile ilgili önemli detaylar içermektedir. İlgili maddeye göre; *"Bir Devlet, kendisine atfedilebilen ve uluslararası bir yükümlülüğün ihlali oluşturan bir siber operasyon için uluslararası yasal sorumluluk taşımaktadır[51]."*

Tallinn Kitapçığının 6.madde 2.fıkrası siber saldırılar ile devletlerin sorumluluğunu bazı şartlara bağlamıştır. Bunlar; (i) söz konusu fiil uluslararası hukuka göre Devlete atfedilebilir olmalı ve (ii) eylem Devlet için geçerli olan uluslararası bir yasal yükümlülüğün ihlali anlamına gelmelidir[52].

II. Siber Saldırıların İsnat Edilebilirlik Meselesi

Bir devletin uluslararası haksız bir fiilden dolayı sorumlu tutulabilmesi ve saldırıya uğrayan devletin meşru müdafaa hakkını ya da görmüş olduğu zarardan ötürü yargı yollarına başvurabilmesi için, saldırının saldırıyı gerçekleştiren devlete isnat edilebilmesi gerekmektedir. Bu kural esas olarak Uluslararası Hukuk Komisyonu'nun hazırladığı "*Uluslararası Haksız Bir Fiilden Ötürü Devletin Uluslararası Sorumluluğu Üzerine Taslak Maddeler'in* ilk maddesinde düzenlenmiş olup, uluslararası teamül hukukunun bir parçası olmuştur[53].

---

50 **UZUN**, s.45.

51 Tallinn Manual On The International Law Applicable To Cyber Warfare, General editor, Michael N. Schmitt, Cambridge University Press 2013, Sectıon 2: State Responsıbılıty Rule 6 – Legal responsibility of States.

52 Tallinn Manual On The International Law Applicable To Cyber Warfare, , Sectıon 2: State Responsıbılıty Rule 6/2.

53 **GÜMÜŞBAŞ Ahmet**,"Siber Savaş Hukukunda Meşru Müdafaa Hakkı ve İsnat Edilebilirlik: Stuxnet ve Aramco Saldırıları", Türk-Arap İlişkileri: Çok Boyutlu Güvenlik İnşası "Karşılıklı Bağımlılık İçin Sektörel ve Finansal Derinleşme" TASAM Yayınları Uluslararası İlişkiler Serisi, İstanbul, 2016, s.188.

Siber alana yönelik gerçekleştirilen ya da siber silah sistemleri vasıta kılınarak işlenmiş suçların araştırılması, soruşturulması ve yargılanması aşamasında birçok güçlükler bulunmaktadır. Özellikle internet ortamının sınır ve mesafe tanımayan nitelikte olması sebebiyle faillerin bulunmasında zorluk olması, fail bulunsa dahi devletler arasında farklı usul uygulamaları bulunması suçun kovuşturulmasını çoğu zaman olanaksız kılmaktadır. Suçun işlendiği zamanın ve yerin tespitinde de zorluklar yaşandığı gibi, mahkemelerin yargı yetkisi problemi ayrıca çözülmeye muhtaç kalmıştır[54]**.**

Bir siber saldırı karşısında, istenilen düzey ve isabet oranıyla tespit yapılabilmesi için gerekli kanıt miktarı ve niteliği birçok devlete hatta aynı devletin içindeki farklı kurumlara göre değişebilmektedir. Burada iyi anlaşılması gereken konu, teknik tespit ile söz konusu tespitin siyasi olarak deklere edilmesi arasında ciddi bir fark olduğudur. Özellikle başka bir devleti bir siber saldırıdan sorumlu tutmak düşünüldüğünden daha komplike bir olaydır. Hatta, saldırgan devlete böyle bir sorumluluk yükledikten sonra diplomatik retorik ötesine geçen bir adım atılmaması halinde, saldırıya uğrayan devletin caydırıcılık kapasitesinin zarar görmesi dahi olasıdır[55]**.**

Teknik olarak, siber alanda tespit ve ilişkilendirme kavramı, siber saldırgan(lar)ın kimliklerinin (identity), yerlerinin (location) ve aracılarının (intermediary) belirlenmesi anlamına gelmektedir. Yapılan çalışmalar sonucu henüz emekleme evresinde olan literatür ve siber saldırılardan öğrenilen dersler, birkaç temel noktaya işaret etmektedir. Öncelikle, bir siber saldırı sonrası tespit / isnat çalışması, mevcut imkanlar dahilinde, gerçekten zordur. Özellikle, profesyonellik dereceler yüksek saldırganlar için birçok saklanma ve yanıltıcı yöntemlerden yararlanma imkanı vardır. Öte yandan, eğer saldırılan kurum içinde bir bağlantı var ise (insider) bugüne kadar edinilen tecrübeler soruşturmanın daha kesin sonuçlara ulaşma olasılığının yüksek olduğunu göstermektedir. Tespit / isnat (attribution) çalışmaları ile ilgili teknik düzeydeki önemli bir soru da tespit edilen ya da edilmesi mümkün olan saldırgan ile ilgili ne yapı-

---

54 **ÖZEL Cevat / AHİ M. Gökhan,** "Bilişim Suçlarında Usul ve Sorumluluk Sistemi Üzerine Öneriler",
http://www.turkhukuksitesi.com/makale_179.htm, E.T.13.10.2019.

55 **KASAPOĞLU Can,** "Hayaletlerin İzlerini Sürmek: Uluslararası Nitelikteki Siber Saldırıların Soruşturulması", EDAM Siber Politikalar ve Dijital Demokrasi Yayınları, 2017/4, s.1.

lacağıdır. Bir yanıltıcı kullanılarak saldırganı tuzak bir hedefe çekmekten (honeypot), saldırgana 'işaretlenmiş' data göndererek kimliğini-aracı sistemler de dahil olmak üzere-iz sürerek bulmak (reverse flow) gibi birçok yöntem bulunmaktadır. Ancak tüm bu yöntemlerin de belirli teknik gereksinimleri vardır. Örneğin bir honeypot, ancak yanıltıcı tuzağa yönelen siber saldırılar ile ilgili tespit yapabilir ve tuzağın bizatihi kendisinin incelenmesi dahi özel uzmanlaşma gerektirmektedir[56].

E. Uluslararası Hukukta Saldırı Suçu Bağlamında Siber Saldırılar

Uluslararası hukuk geniş anlamda incelendiğinde savaş suçlarının başlıca üç tür suç kapsamı şeklinde değerlendirildiği görülmektedir. Bunlar saldırı suçu[57], insanlığa karşı suç[58] ve dar anlamda savaş suçudur[59].

Birleşmiş Milletler (BM) Antlaşması ile ilke olarak kuvvet kullanılmasının yasaklanması sonucu günümüzde başta BM olmak üzere uygulanan uluslararası hukuka aykırı kuvvet kullanılması bir saldırı olarak nitelendirilmektedir. Nitekim 14.12.1974 tarihinde BM Genel Kurulunun 3314 sayılı kararı ile kabul edilen Saldırının Tanımı belgesinin

---

56 **KASAPOĞLU** (2017), s.3 – 4.

57 Uluslararası Ceza Mahkemesi Roma Statüsü, madde 8 "Saldırı Suçu" başlığı altında şu şekilde açıklanmıştır: Madde 8/2. *"Saldırı fiili", bir devlet tarafından, bir başka Devletin egemenliğine, toprak bütünlüğüne veya bağımsızlığına karşı veya BM Şartı'na aykırı başka şekillerde silahlı kuvvet kullanılmasıdır".* Detaylı bilgi için bakınız: **KAYA İbrahim**, Uluslararası Hukukta Temel Belgeler, Seçkin Yayıncılık, Ankara, 2013, s.412.

58 3.5.1993 tarih ve 808 (1993) sayılı BM Güvenlik Konseyi kararı ile kabul edilen Eski Yugoslavya Mahkemesi Statüsü 5.maddesine göre ister uluslararası ister ulusal nitelikte olsun, silahlı çatışmalar sırasında herhangi bir sivil halka karşı işlenen belirtilen fiiller insanlığa karşı suç kabul edilmektedir. Bu fiiller; i) kasten öldürme, ii) toplu yok etme, iii) köle etme, iv) sürgün, v) hapsetme, vi) işkence, viii) ırza geçme, viii) siyasal ırkçı ve dinsel nedenlerle zulmetme, ix) öteki insanlık dışı muameleler. Detaylı bilgi için bakınız: **PAZARCI**, s.656.

59 8.8.1945 tarihli Londra Antlaşmasının eki Statünün 6/b maddesinde ve 19.1.1946 tarihli Tokyo Uluslararası Mahkemesi Statüsünün 5/b maddesinde dar anlamda savaş suçları için kişilerin yargılanması ve cezalandırılması düzenlenmiş bulunmaktadır. Nuremberg Statüsünde "savaş suçları" şu şekilde tanımlanmaktadır; kasten öldürme, kötü muamele ya da sivil halkın ya da işgal atındaki sivil halkın sürgünü, kölelik ya da başka amaçla çalıştırma, savaş tutsaklarına ya da denizdeki kişilere kötü muamele, rehinelerin öldürülmesi, kamu ya da özel mülkiyetin yağmalanması, gereksiz yere kentlerin, kasaba ve köylerin yok edilmesi ya da askeri gereklilik olmadan bunların yakılıp yıkılması ile sınırlı olmak üzere savaş yasalarını ya da yapıla gelişlerini ihlaller. Detaylı bilgi için bakınız: **PAZARCI**, s.656.

1.maddesinde bir devletçe, başka bir devletin egemenliğine, ülke bütünlüğüne ya da siyasal bağımsızlığına karşı ya da BM Antlaşmasına aykırı herhangi bir biçimde silahlı kuvvet kullanılması saldırı olarak değerlendirilmektedir[60].

Uluslararası hukukta *jus ad bellum*, silahlı kuvvet kullanılmasının haklılığı, silahlı kuvvete son çare olarak başvurulması gibi savaşın gerekçelerinin hukuka uygunluğuna ilişkin kuralları ifade etmektedir. *Jus in bello* ise, silahlı bir çatışmada hukuka uygun araç ve yöntemlerin kullanılması gibi savaş başladıktan sonraki kuralları ifade etmektedir[61]. Herhangi iki ülke savaşa başladığında, savaş hukuku kuralları uygulanmakta ve bu kurallara uyulmaması devletlerin sorumluluğuna yol açmaktadır.

Saldırı kavramı ile ilgili BM Genel Kurulu'nun almış olduğu 3314 sayılı karar kavramının açıklayıcılığı açısından önemli unsurlar içermektedir. Söz konusu kararın 1. Maddesi şu şekildedir;

BM 3314 Sayılı Karar "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[62]*".*

Uluslararası hukukta kabul gören genel tanımlara göre saldırı yasağı kapsamının açıklanmasına yönelik saldırı kavramı tanımı 3314 Sayılı Karar'ın 1.maddesinde genel bir tanımla, takip eden maddelerde de açıklayıcı hükümler ile saldırı örnekleri tanımlanmaya çalışılmıştır. Söz konusu kararın 1.maddesinde belirtilen silahlı kuvvet kullanma tanımı, kanaatimizce siber saldırılar açısından önemli bir sorun teşkil etmektedir. Silahlı kuvvet kullanma kavramının ne ifade ettiği 3314 Sayılı Karar'da ayrıca tanımlanmasına rağmen, Karar'da sayılan saldırı eylemi örnekleri, silahlı kuvvet kavramının içeriğini daha da belirginleştirmek açısından önemli ipuçları sunmaktadır. Karar'ın 3.maddesinde ayrı paragraflar halinde saldırı eylemi örnekleri sayılmıştır[63].

---

60 **PAZARCI**, s.654-655.

61 **ÇİFCİ**, s.110.

62 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.

63 Madde 3- Savaş ilan edilmiş olsun olmasın, aşağıdaki fiillerin herhangi birisi 2'nci madde hükümlerine tabi ve ona uygun şekilde bir saldırı fiili niteliği taşır:

Silahlı kuvvet kullanmanın dinamik yapısı dikkate alındığında, yapısı itibariyle fiziki gücü içermeyen ancak silahlı saldırı ile aynı derecede somut zararlara sebep olabilen siber saldırılar, silahlı bir saldırı gibi değerlendirilip siber saldırı bir silah ile eş değere sahip olabilecektir. Örneğin, kimyasal, biyolojik ve radyolojik silahlar da yapısı itibariyle silahlı saldırılar gibi yıkıcı olmamasına rağmen kuvvet kullanma kapsamında silahlı bir saldırı eylemi olarak değerlendirilmektedir. Siber saldırılar bağlamında 2010 yılında ABD'nin İran'ın nükleer kapasitesine yönelik yapılan STUXNET[64] virüs saldırısı, bunun açık örneğini teşkil etmektedir. Dolayısıyla siber saldırılar açık bir şekilde doğrudan fiziki zararlara yol açabilme eşiğini geçmiş ve ciddi zararlar verebilme kapasitesine erişmiştir. Yine başka bir örnek verecek olursak, siber saldırılar neticesinde doğalgaz hatlarının sabote edilmesi, nükleer merkezlerin imha edilmesi, hava trafiğinin felç edilip binlerce kişinin sabotaja uğraması gibi yüzlerce zarara sebep olan bir saldırıda siber saldırıyı, silah gibi düşünmeyip, saldırı metodunu uluslararası hukuk kurallarından

---

a- Bir Devletin silahlı kuvvetlerinin diğer bir devleti istila etmesi veya ona hücum etmesi veya ne kadar geçici olursa olsun, böyle bir istiladan veya hücumdan ileri gelen herhangi bir askeri işgal veya kuvvet yoluyla başka bir Devletin ülkesinin veya bir bölümünün ilhakı;

b- Bir Devletin silahlı kuvvetlerinin, başka bir Devletin ülkesini bombardıman etmesi veya bir Devletin diğer bir Devletin ülkesine karşı herhangi bir şekilde silah kullanması;

c- Bir Devletin liman veya kıyılarının diğer bir Devletin silahlı kuvvetleri tarafından abluka altına alınması;

d- Bir Devletin silahlı kuvvetleriyle başka bir Devletin kara, deniz veya hava kuvvetlerine veya deniz veya hava filolarına saldırması;

e- Bir Devletin başka bir Devlette sonuncusuyla yapılan bir anlaşmaya göre bulunan silahlı kuvvetlerinin o anlaşmada öngörülen hükümlere aykırı şekilde kullanılması veya bu silahlı kuvvetlerinin varlığının bu ülkede anlaşmanın sona ermesinden sonra da sürdürülmesi;

f- Ülkesini başka bir Devletin emrine veren bir Devletin, ülkesinin o Devlet tarafından üçüncü bir Devlete karşı saldırı amacıyla kullanılmasına izin vermesi;

g- Bir Devlet tarafından veya bir Devlet adına diğer bir Devlete karşı yukarıda listesi verilen fiillere varan veya o ölçekte olan silahlı kuvvet fiillerini icra eden silahlı çetelerin, grupların, gayri nizami askerlerin veya paralı askerlerin gönderilmesi veya bu gibi fiillere önemli ölçüde karışılması.

64 STUXNET, İran'ın nükleer tesislerini hedef alan ABD ve İsrail uzmanları tarafından üretildiğine inanılan, 2010 yılında ortaya çıkarılan ve yıllar önce sisteme bırakılan daha çok İran (%60), fakat aynı santrifüj ve yazılımı kullandıkları için Endonezya, G. Kore, ve Hindistan'da da zarara neden olan bir koddur. **AKYEŞİLMAN**, s.243.

muaf olarak düşünmek imkânsızdır. Dolayısıyla oldukça etkili fiziki zarara, yaralanmaya ya da ölüme yol açan siber saldırılarda, siber ekipmanların devletler tarafından bir silah gibi kullanılması yarattığı etki neticesine bağlı olarak değerlendirilecektir[65].

Daha öncede değindiğimiz üzere Siber saldırı ve siber savaş ile ilgili kavramları açıklamak üzere NATO tarafından 2013 yılında Tallinn El Kitabı hazırlanmıştır. NATO'nun kurduğu Ortak Siber Savunma Mükemmeliyet Merkezi siber güvenliğin hukuki boyutlarını tartışmak adına çalışmalara başlamış ve 2009 yılında uluslararası uzmanlar grubu oluşturulmuştur. Uzmanlar grubunun çalışmalarının ürünü olan El Kitabı'nın birinci ve ikinci versiyonlarında siber faaliyetlere ilişkin hukuk kuralları incelenmiş; siber faaliyetler için uygulanabilecek ilkeler mevcut uluslararası kurallar ışığında kaleme alınmıştır. Nitekim El Kitabı'nın uluslararası barış ve güvenlik ve siber faaliyetlerin ele alındığı kısımda yer alan ilkeler, uluslararası hukukta düzenlenen kuvvet kullanma, meşru müdafaa hakkı ve kolektif güvenlik sistemine ilişkin kuralların rehberliğinde hazırlanmıştır[66].

III. Siber Saldırı Suçu İşleyen Devlet ya da Devlet Görevlilerinin Yargılanması Meselesi

Uluslararası hukuk kuralları çerçevesinde saldırı suçu işlediği iddia edilen devlet ya da devlet görevlilerinin yargı önüne çıkarılmasının zor olacağı uluslararası hukuk nezdinde geçerliliğini hala sürdürmektedir. Özellikle saldırı suçunu işleyen büyük devletlerin ve devlet görevlilerinin yargılanmasının zorluğu ve hala günümüzde birçok ülkenin uluslararası yargı organlarının yargı yetkisini tanımıyor olması, devletlerin ya da devlet görevlilerinin yargılanamayacağı savını güçlendirmektedir. Bu bağlamda siber saldırı suçu ile ilgili olarak, siber saldırı suçunu işleyen devlet ya da devlet görevlilerinin tespit edilmesinin zor olması kadar, yargılanmaları da şu an için pek gerçekçi görünmemektedir. Ancak konu ile ilgili çalışmaların artmaya başlamış olması, siber saldırı suçunu işleyen devlet ya da devlet görevlilerinin de yargılanması

---

65 **GÜREŞÇİ Ramazan**, "Siber Saldırıların Uluslararası Hukuktaki Güç Kullanımı Kapsamında Değerlendirilmesi", *Savunma Bilimleri Dergisi*, Cilt.18, Sayı:1, 2019, s.87.

66 Tallinn Manual 2.0 On The International Law Applicable To Cyber Operations, General Editor, MICHAEL N. Schmitts, Cambridge University Press 2017, s.301-373 / **ERDEM Merve/ÖZOCAK Gürkan**, "Siber Güvenliğin Sağlanmasında Uluslararası Hukukun ve Türk Hukukunun Rolü, *Ankara Üniversitesi Hukuk Fakültesi Dergisi*, Sayı:68(1), Ankara, 2019, s.136.

meselesini gündeme getirecektir. Biz de bu noktadan hareket ile siber saldırı suçu işleyen devlet ya da devlet görevlilerinin yargılanması meselesini açıklamaya çalışacağız.

Uluslararası yapının ana özelliklerinden biri, devletlerin fiziki sınırlarına ve yargı yetkisine dayanmasıdır. Ancak, ademi merkeziyetçi ve anarşik olmakla birlikte, siber uzayın sınırları yoktur. Bu nedenle, devletlerin açık bir yargı yetkisi (güçlü hukuki yaptırımlar) de yoktur ve sistem düzeyinde ağırlıklı olarak tek bir aktör belirleyici değildir. Bu konuda Tallinn Kitapçığı bazı önemli ayrıntılar içermektedir. Söz konusu Kitapçığın 1.maddesi *"Egemenlik"* başlığı altında, bir devletin kendi toprakları üzerinde siber altyapıyı ve siber faaliyetleri kontrol edebilme hakkının kaynağını egemenlikten aldığını belirtmektedir. Buradan devamla, bir devletin karasal topraklarında, iç sularında, deniz yetki alanında (deniz yatağı dahil) ve ulusal hava sahasında bulunan siber faaliyetler o devletin egemenliği altında olacaktır ve devlet sorumlu tutulabilecektir[67].

Bunun dışında, birçok özel aktör, siber alanı yönetme ve manipüle etmek bakımından birçok devletten daha güçlüdür. Ayrıca, birçok bireysel bilgisayar korsanı devletler veya şirketler gibi yıkıcı saldırılar başlatabilir. Bu nedenle, fiziki dünyadan farklı olarak, siber dünyasında faaliyet yürüten çok daha fazla eşdeğer aktör veya paydaş bulunmaktadır[68].

A. Siber Saldırı Suçu İşleyen Devletlerin Uluslararası Adalet Divanı'nda Yargılanması Meselesi

BM Antlaşmasına göre, Uluslararası Adalet Divanı (UAD), Örgüt'ün başlıca "yargısal" organı olup Devletleri yargılama yetkisine sahiptir. Uluslararası Adalet Divanının oluşumunu ve yetkilerini düzenleyen kurallar BM Antlaşması 92-96.maddelerinde ve Uluslararası Adalet Divanı Statüsü'nde belirtilmiştir. BM'ye üye olan bütün devletler, aynı zamanda *ipso facto*[69], BM Antlaşması'nın eki olan Uluslararası Adalet Divanı Statüsü'ne de taraf olmaktadırlar[70].

---

67 Tallinn Manual on the International Law Applicable to Cyber Werfare, Rule:1.

68 **AKYEŞİLMAN**, s.269.

69 *"ipso facto" uluslararası hukuk terimi olarak* kendiliğinden, otomatik olarak anlamında kullanılmaktadır.

70 **AYBAY Rona/ORAL Elif**, (2016), Kamusal Uluslararası Hukuk, İstanbul Bilgi Üniversitesi Yayınları, s.350. / **GÜNDÜZ Aslan**, (1998), Milletlerarası Hukuk Temel Belgeler Örnek Kararlar, Beta Yayınları, s.133-135.

UAD, ilke olarak tarafların sundukları uyuşmazlıklarla, BM Şartı ve uluslararası antlaşmalarda öngörülen uyuşmazlıklar açısından yargı yetkisine sahiptir. Statünün 36(1) maddesine göre Mahkemenin yargı yetkisi dört şekilde kurulabilir[71].

1. Ad Hoc Yetki: Taraflar aralarındaki bir uyuşmazlığı uyuşmazlık ortaya çıktıktan sonra Mahkemeye sunmak üzere anlaşabilirler.

2. Tek Taraflı Başvuru: Taraflardan birisinin tek taraflı olarak Mahkemeye başvurması ve diğerinin itiraz etmeyerek davaya katılması da mümkündür. Bu son halde, Mahkemenin yetkisi örtülü olarak kabul edilmiş sayılmaktadır.

3. Anlaşma: Taraflar yürürlükteki karşılıklı antlaşmalara veya çok taraflı sözleşmelere yargı yetkisi konusunda hüküm koyarak, UAD'nin yargı yetkisini, daha uyuşmazlık ortaya çıkmadan, önceden kabul etmiş olabilirler.

Konumuz açısından "siber saldırı suçunun" işlenmesi ile devletlerin UAD önünde yargılanması meselesi, eylemin kuvvet kullanma yasağına aykırı bir eylem olması, silahlı bir saldırı teşkil etmesi veya siber saldırı neticesinde herhangi bir hukuk ihlali iddiasına bağlıdır. Ayrıca yine belirtmek gerekir ki, saldırı kavramının kuvvet kullanma tehdidi ya da kuvvet kullanma kavramlarından hem unsurları hem de hukuksal sonuçları açısından önemli farklılıklar gösterdiği görülmektedir.

1974 tarihli BM Genel Kurulu 3314 (XXIX) sayılı kararında, saldırı suçunun bireylere değil, devletlere sorumluluk getirdiği, bu nedenle saldırı niteliği taşıyan fiillerin bireysel cezai sorumluluk doğurması için, daha belirgin düzenlemelere ihtiyaç olduğu ileri sürülmüştür[72]. Sözü geçen kararda saldırı suçu, barışa karşı işlenmiş bir suç olduğu belirtilmesine karşılık, gerek saldırı fiilinin tanımında gerek saldırını niteliği taşıyan fiiller sayılırken hep devletten söz edilmiş, fiiller bireyselleştirilmemiştir.

BM Antlaşması 2/4.maddesinde belirtilen kuvvet kullanma yasağı, "silahlı saldırı" kavramı ile birlikte değerlendirildiğinde farklı sonuçlar içermektedir. Silahlı saldırı kavramı, kapsam itibariyle BM Antlaşması'nın 2/4.maddesinde sözü edilen uluslararası ilişkilerde "kuvvet kulla-

---

71 **ÜNAL Şeref**, (2005), Uluslararası Hukuk, 1. Basım, Yetkin Yayınları, s.340.

72 **DEMİRAĞ Fahrettin**, "Uluslararası Ceza Divanı, Savaş Suçları – Saldırı Suçu, Mevzuatımıza Göre Savaş Hali", Uluslararası Ceza Divanı, Yayına Hazırlayan: Feridun Yenisey, Arıkan Basım Yayım Dağıtım, Ankara, 2007, s.109.

nımına ya da kuvvet kullanma tehdidine" kıyasla daha dar bir anlama sahiptir. Her türlü silahlı saldırı bir kuvvet kullanımını gerektirdiği halde, her türlü kuvvet kullanma yasağının ihlali, bir silahlı saldırının vukuu şeklinde değerlendirilemez. Silahlı bir saldırıdan söz edebilmek için, çok ciddi düzeyde bir kuvvet kullanımının ve bunun yol açtığı hasarın söz konusu olması gerekmektedir[73].

UAD'ye göre, silahlı saldırı yalnızca bir devletin silahlı düzenli birliklerinin bir uluslararası sınırı aşan eylemleri olarak sınırlandırılamaz. Bir devlet adına ya da bir devlet tarafından silahlı birliklerin, silahlı grupların, düzensiz güçlerin ya da paralı askerlerin bir başka devlete karşı gönderilmesi de silahlı saldırı niteliğine sahip olabilmektedir. Yeter ki bu grupların diğer devlete karşı gerçekleştirdikleri silahlı kuvvet eylemleri, bir devletin düzenli birliklerinin eylemlerinin ağırlığına ulaşmış olsun[74]. Bu nokta da "siber saldırıların" da bir devletin düzenli birliklerinin eylemine ulaşacak nitelikte büyük bir saldırı teşkil etmesi durumunda, "silahlı saldırı suçu" söz konusu olacaktır ve eylemi gerçekleştiren devletin sorumluluğu gündeme gelecektir.

Siber silahın tanımı konusunda yapılan farklı tanımları, siber silahların neden olabilecekleri zarara göre sınıflandırmak yerinde ve işlevsel bir yöntemdir. Bu yaklaşıma göre, siber silahlar bir etki spektrumu üzerinde düşük ve yüksek potansiyele sahip yazılım ve programlar olarak değerlendirilirler. Düşük potansiyele sahip siber silahlar, bir sistemi dışarıdan etkileyebilen ancak bu sitemin içine girmeyi ve onu içerden yönetmeyi başaramayan zararlı yazılımlardır. Yüksek potansiyele sahip siber silahlar ise, bu sistemlerin içine girerek "akıllı unsur" şeklinde çalışan ve otonom şekilde hareket ederek sistemin normal faaliyet sürecine zarar veren zararlı yazılımlardır[75].

Tallinn Klavuzu'nun 13.maddesine göre ise, "silahlı saldırı" seviyesine varan bir siber harekata maruz kalan bir devlet "meşru müdafaa"

---

73 **ARAL BERDAL**, Uluslararası Hukukta Meşru Müdafaa Hakkı, Siyasal Kitabevi, Ankara, 1999, s.17.

74 **ACER Yücel**, Uluslararası Hukukta Saldırı Suçu, Roma Yayınları, Ankara, 2004, s.76.

75 **RİD Thomas/MCBURNEY Peter**, "Cyber-Weapons", *Rusi Journal*, February, Marc p.8 Çeviren; **ÇELİK 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, İzmir, 2013, s.142.

hakkına başvurabilecektir. Söz konusu siber eylemin "silahlı saldırı" olup olmadığına eylemin "ölçü ve etkisi" göz önünde bulundurularak karar verilecek ve bu çerçevede meşru müdafaa hakkı doğacaktır[76].

UAD'nin siber saldırılar ile ilgili yargı meselesi ile ilgili Nikaragua Davası Kararı[77] önemli ipuçları taşımaktadır. Silahlı saldırı kavramının doğduğu asıl kaynağın, tek başına ya da birlikte meşru müdafaa hakkının kullanılmasını düzenleyen BM Statüsü'nün 51.maddesi olduğu söylenebilir. Ancak kavramın 51.maddede tanımlanmadığını yukarı ki bölümlerde açıklamaya çalışmıştık.

1986 tarihli Nikaragua Davası'nda Uluslararası Adalet Divanı, kuvvet kullanma eylemleri arasında açıkça bir ayrıma gitmiş ve "kuvvet kullanmanın en ağır şekli" ve "diğer daha hafif şekilleri" arasında bir ayrım yapılması gerektiğini belirtmiştir. Kuvvet kullanmanın en ağır şeklinin ise "silahlı saldırı" olduğunu ifade etmiştir. Mahkeme'nin silah-

---

76 "Tallinn Manual on The International Law Applıcable to Cyber Warfare", Prepared by The International Group of Experts at The Invitation of The NATO Cooperative Cyber Defence Centre of Excellence, General Editor: SCHMITT, Michael N, Cambridge University Press, 2013, s.53. **GÜMÜŞBAŞ, Ahmet,** "Siber Savaş Hukukunda Meşru Müdafaa Hakkı ve İsnat Edilebilirlik: Stuxnet ve Aramco Saldırıları", *Türk-Arap İlişkileri: Çok Boyutlu Güvenlik İnşası "Karşılıklı Bağımlılık İçin Sektörel ve Finansal Derinleşme" TASAM Yayınları Uluslararası İlişkiler Serisi*, İlk Basım, İstanbul 2016, s.186.

77 1979 yılının Orta Amerika'sında, Nikaragua'da solcu Sandinista devrimcileri sağcı Samoza Hükümetini devirmiş ve yönetimi ele geçirmişti. İdeolojisinin bir parçası olarak, yeni kurulan Sandinista Hükümeti Sovyet Rusya'sı ve Küba ile ilişkiler kurma yoluna gitmiş ve ülkesinde de askeri gücünü iyice arttırmıştı. Lakin devrik devlet başkanı Samoza'nın ulusal muhafızlarından oluşan paramiliter gruplar ülkede boş durmamış, Sandinista Hükümeti aleyhine faaliyetlerde bulunmuştu. İşte tüm sorun da burada düğümlenmekteydi. Bir tarafta ABD, Sandinista Hükümetinin kendi ideolojisini çevre ülkelere yaymaya çalıştığını ve El Salvador'daki hükümet karşıtı gerillalara yardım ettiğini ileri sürmüş; diğer yandan Nikaragua, ABD'nin paramiliter gruplara – ki Sandinista Hükümeti bunlara "kontra" diyordu – askeri, lojistik, eğitim, istihbarat ve tatiksel plan anlamında yardım ettiği söylüyordu. Nikaragua, ABD'nin desteklediği kontralarla mücadelede başarısız olunca, Uluslararası Adalet Divanı'na ABD aleyhine, askeri veya yarı askeri faaliyetleri üzerinden tazminat talebiyle başvurmuştur. Nikaragua Davası hakkında detaylı bilgi için bakınız: "Case Concerning Military And Paramilitary Activities in And Against Nicaragua", Judgment of 27 June 1986, https://www.icj-cij.org/files/case-related/70/070-19860627-JUD-01-00-EN.pdf.

YILMAZ Eren Alper/IRK Orhan, "Nikaragua Divan Kararları Işığında Kuvvet Kullanma ve Meşru Müdafaa Sorunu", *CBÜ Sosyal Bilimler Dergisi*, Cilt:13, Sayı:2, 2015.

lı saldırı kavramını savaş kavramının eş anlamlısı olarak mı kullandığı net bir şekilde belirtilmemiştir. Mahkeme'ye göre bir eylemin silahlı saldırı sayılabilmesi için, mutlaka bir devletin düzenli silahlı kuvvetlerinin sınırı aşma eylemini gerçekleştirmiş olması gerekmektedir. Bir devlet tarafından ya da bir devlet adına, silahlı birliklerin, silahlı grupların, düzensiz kuvvetlerin ya da paralı askerlerin bir başka devlete gönderilmesi de silahlı saldırı niteliğine sahip olabilmektedir. Ancak belirtilen bu silahlı grupların gerçekleştirdikleri silahlı kuvvet eylemlerinin düzenli birliklerin gerçekleştirdikleri kadar ağır bir niteliğe ulaşması gerekmektedir. Mahkeme bu tanımı 3314 Sayılı Karar'ın 3.maddesinin g bendinden aynen alınmıştır ve 3.maddenin g bendindeki tanımı, yapıla geliş değeri kazanmış bir terim olarak nitelendirmiştir[78].

A. Siber Saldırı Suçu İşleyen Devlet Görevlilerinin Uluslararası Ceza Mahkemesi'nde Yargılanması Meselesi

Uluslararası Ceza Mahkemesi (UCM) Roma Statüsü'nün "Bireysel Ceza Sorumluluğu" başlıklı 25.maddesinin 1.fıkrasında, Mahkeme'nin yalnızca gerçek kişiler bakımından yargı yetkisi olduğu açıkça belirtilmiştir.

UCM Roma statüsünün 5.maddesinin 2.paragrafı ise Mahkeme'nin saldırı suçu üzerinde yargı yetkisini kullanabilmesi için, saldırı suçunu tanımlayan ve saldırı suçuna ilişkin yargılamaların yapılacağı şartları belirleyen bir düzenlemenin kabul edilmesi gerektiğini öngörmüştü. UCM Üye Devletler Asamblesi'nin 14 Aralık 2017 tarihinde oybirliğiyle kabul ettiği Karar uyarınca, UCM'nin saldırı suçu bakımından yargı yetkisi, 17 Temmuz 2018 itibariyle aktif hale gelmiştir[79]. Statünün 121.maddesinde belirtilen şartlar çerçevesinde statüye eklenecek bu düzenleme ile saldırı suçu üzerinde yargı yetkisi kullanılmaya başlanacaktır. 121.maddenin 1.paragrafı, bu nitelikte bir eklemenin ya da değişikliğin statü yürürlüğe girdikten 7 yıl sonra yapılabileceğini belirtmekteydi[80]. İlerleyen yıllarda UCM kurulması çalışmalarının başarı ile sonuçlandırıldığı Roma Konferansı'nda, Mahkeme'nin statüsü ile birlikte çeşitli kararlar da kabul edilmiştir. Bu kararlardan birisi de Konferans So-

---

78 **ACER**, s.168.

79 Resolution ICC-ASP/16/Res.5 Adopted at the 13th plenary meeting, on 14 December 2017, by consensus, https://insanhaklarimerkezi.bilgi.edu.tr/media/uploads/2017/12/25/ICC-ASP-16-Res5-ENG.pdf.

80 **ACER**, s.6.

nuç Belgesi'ni imzalayan ve Konferans'a davet edilen ülkelerin temsilcilerinden oluşan 'Uluslararası Ceza Mahkemesi için Hazırlık Komisyonu' kurulması ve UCM'nin kurulmasına ve işleyişine ilişkin pratik kararların oluşturulması üzerine olmuştur[81].

Roma Statüsü'nün 12.maddesine[82] göre, Uluslararası Ceza Mahkemesi'nin yargı yetkisini kullanabilmesi için,

1- Suçun işlendiği ülke Statüye taraf olmalı (mülkilik ilkesi) veya

2- Sanık, Statüye taraf olan bir devletin vatandaşı olmalı (faile göre şahsilik) ya da

3- Statüye taraf olmayan bir Devlet Mahkeme'nin yargı yetkisini geçici olarak kabul etmiş olmalıdır[83].

Uluslararası Ceza Mahkemesi statüsünün 13.maddesinde[84] mahkemenin yargılama mekanizmasının kimler tarafından harekete geçiri-

---

81 **ACER Yücel**, "Uluslararası Hukukta Saldırı Suçunun Temel Unsurları: Tanım Çalışmaları ve Yansımalar", *Uluslararası Hukuk ve Politika Dergisi*, Cilt:1, No:3, 2005, s.17.

82 **Uluslararası Ceza Mahkemesi Statüsü- Madde 12 Yargı Yetkisinin Kullanılmasına İlişkin Ön Koşullar**: 1- Bir Devlet, bu Statüye taraf olmakla, 5.maddede bahsi geçen suçlarla ilgili olarak Mahkeme'nin yargı yetkisini kabul etmiş olur. 2- Aşağıdaki devletlerden bir veya daha fazlası Statüye taraf ise ya da 3.paragrafa uygun olarak yargı yetkisini tanımış ise Mahkeme 13.maddenin (a) veya (c) bentleri ile ilgili olarak yargı yetkisini kullanabilir: (a) Toprakları üzerinde sorun teşkil eden olayın meydana geldiği devlet ya da suç, bir uçak veya gemide işlenmiş ise gemi veya uçağın kayıtlı bulunduğu devlet; (b) Suçlanan kişinin vatandaşı olduğu devlet, 3- Bu Statüye taraf olmayan devletin 2.paragrafa göre kabulü aranıyorsa, o devlet Mahkeme Yazı İşleri Dairesi'ne sunacağı bir bildirge ile suç konusu olayla ilgili olarak Mahkemenin yargı yetkisini kabul edebilir. Kabul eden devlet 9.Bölüm'e uygun olarak erteleme ya da istisna olmaksızın Mahkeme ile işbirliği yapacaktır.

83 Konferans sırasında Güney Kore tarafından sunulan, suçun işlendiği ülkenin veya sanığı elinde bulunduran veya sanığın veya mağdurun vatandaşı olduğu devletin Statüyü onaylamış olması halinde Mahkemenin yargı yetkisini kabul eden öneri ise kabul edilmemiştir. Uluslararası Ceza Mahkemesi'nin yargı yetkisi hakkında detaylı bilgi için bakınız; **TURHAN Faruk,** "Uluslararası Cezam Mahkemesi'nin Yargı Yetkisi" Uluslararası Ceza Divanı, Yayına Hazırlayan: YENİSEY, Feridun, Arıkan Yayınları, İstanbul, 2007, s.127.

84 **Uluslararası Ceza Mahkemesi Statüsü- Madde 13 Yargı Yetkisinin Kullanılması:** Bu tüzük hükümleri gereğince, 5. maddede bahis konusu bir suç ile ilgili olarak Mahkeme, aşağıdaki koşullarda yargı yetkisini kullanabilir: (a) 14. madde gereğince bir taraf devlet tarafından Mahkeme savcısına başvurulan bir veya birden fazla suçun işlenmiş göründüğü durum; (b) Birleşmiş Milletler Sözleşmesi'nin VII. bölümüne uygun olarak hareket eden BM Güvenlik Konseyi tarafından Mahkeme savcısına başvurulan bir veya birden fazla suçun işlenmiş göründüğü durum; (c) 15.

lebileceği belirtilmiştir. Maddenin (a) bendinde belirtilen taraf devletlerin savcılığa başvurusuyla soruşturmanın başlatılması 14.maddede düzenlenmiştir. Madde uyarınca taraf devletlerden birisi, bir veya birden fazla suçun işlenmiş gözüktüğünü belirterek yargılama yapılıp yapılmayacağının belirlenmesi amacıyla durumun soruşturulmasını savcılıktan talep edecektir. Başvuruda bulunan devlet mümkün olduğu kadar maddî vakıaları ortaya koyacak ve başvuruyu elindeki belgelerle destekleyecektir[85].

Mahkeme BM Güvenlik Konseyi'nce BM Antlaşması'nın VII. Bölümü bağlamında, Mahkemenin savcısına havale edilmiş konularda (madde 13/b) da yargılama yapmakla görevlidir. BM Güvenlik Konseyi'nce havale edilmiş konularda, ilgili devletin Roma Sözleşmesi'ne taraf olup olmadığının bir önemi yoktur.

Roma Statüsü Madde 15bis/5 ise Mahkeme'nin yargı yetkisini tanımayan devletlerin saldırı suçunu işlemeleri durumunda ne gibi bir prosedürün işleneceğini düzenlemektedir. Söz konusu madde hükmü: "*Bu Statüye taraf olmayan bir Devlet bakımından, saldırı suçu söz konusu Devletin vatandaşları tarafından veya o Devletin toprakları üzerinde işlendiğinde, Divan saldırı suçu üzerinde yargılama yetkisini kullanamaz"* demektedir.

UCM nezdinde Devlet başvurusu veya savcının kendiliğinden soruşturma açması kapsamında saldırı suçu üzerinde yargı yetkisinin kullanılması madde 15 *bis*[86] 'te düzenlenmiştir. 15 *bis* (1) maddesine göre

---

maddeye uygun olarak bir suçun işlendiğine dair savcı tarafından soruşturma başlatılması.

85 **KILIÇ Ali Şahin**,"Uluslararası Ceza Mahkemesi ve Devletlerin Egemenliği Üzerine Ulusal Egemenlik Odaklı Bir İnceleme", *Ankara Üniversitesi Hukuk Fakültesi Dergisi*, Ankara, 2009, s.628.

86 **Uluslararası Ceza Mahkemesi Statüsü – Madde 15 *bis*** Saldırı Suçu Üzerine Yargı Yetkisinin Kullanılması (Devlet Başvurusu, Re'sen) : 1. Mahkeme, saldırı suçu üzerindeki yargı yetkisini, bu madde hükümlerine bağlı olarak madde 13 paragraf (a) ve (c)'ye uygun olarak kullanabilir. 2. Mahkeme, yargılama yetkisini ancak değişikliklerin otuz Taraf Devlet tarafından onaylanması ya da kabul edilmesinden bir yıl sonra işlenecek saldırı suçları üzerinde kullanabilir. 3. Mahkeme, Statüde bir değişikliğin kabul edilmesi için gerekli olan oy çoğunluğu ile aynı çoğunlukta Taraf Devletin, 1 Ocak 2017 tarihinden sonra alacağı karara bağlı olarak, saldırı suçu üzerinde yargılama yetkisini bu madde kapsamında kullanmaya başlar. 4. Bir taraf Devlet, daha önceden bir saldırı fiilinden kaynaklanan saldırı suçu üzerinde Divanın yargılama yetkisini kabul etmediğinde yönelik Yazı İşleri Bürosu Başkanı'na bir bildirimde bulunmamışsa, Mahkeme, madde 12 uyarınca, söz konusu Taraf Devlet

UCM, saldırı suçu üzerindeki yargı yetkisini, 15 *bis* maddesinin hükümlerine bağlı olarak 13'üncü maddenin (a) ve (c) paragraflarına uygun olarak kullanabilecektir[87].

BM Güvenlik Konseyi tarafından yapılan başvuru üzerine Saldırı Suçu üzerinde yargı yetkisinin kullanılması madde 15 *ter*[88]'de düzenlenmiştir. BM Şartı'nın VII'inci Bölümü kapsamında hareket eden BM Güvenlik Konseyi tarafından UCM Savcısı'na gönderilen bir veya birden fazla suçun işlendiği izlenimini veren bir durumda, UCM Savcısı soruşturmaya 53 (1)'inci maddede de belirtildiği şekilde başlayacaktır. 53(1)(a)-(c) bentleri çerçevesinde durumu değerlendirip soruşturma açılıp açılmamasına karar verecektir. Soruşturma açılmaması yönünde karar vermesi durumunda Güvenlik Konseyi madde 53(3)(a) hükmü uyarınca, savcının takipsizlik kararının gözden geçirilmesi için talepte bulunabilir. Ön Yargılama Dairesi, savcının madde 53(1) ve 53(2) kapsamında vermiş olduğu takipsizlik kararını gözden geçirebilecek ve savcıdan bu kararını tekrar değerlendirmesini isteyebilecektir. Bu aşamadan sonra Güvenlik Konseyi'nin sonradan aynı olayla ilgili olarak yaptığı tespitler 15 ter (4) maddesi gereği UCM'yi ve dolayısıyla savcılığı bağlamayacaktır. Bu hükümle UCM'nin bağımsızlığı sağlanmıştır.

Saldırı suçunun tanımına ilişkin uluslararası yargı kararları ve ilişkin tartışmalar temelinde, silahlı saldırı kavramının özellikle "sonuçları" açısından saldırı suçunun oluşması için beklenen seviyeye ulaşma-

---

tarafından işlenen saldırı suçu üzerinde yargılama yetkisini kullanabilir. Böyle bir bildirimin geri alınması her zaman mümkün olup, Taraf Devlet tarafından bu husus üç yıl içinde değerlendirilir.

87 **TEZCAN Durmuş / ERDEM Mustafa Ruhan / ÖNOK Murat,** Uluslararası Ceza Hukuku, Seçkin Yayınları, Ankara, 2017, s. 559.

88 **Uluslararası Ceza Mahkemesi Statüsü – Madde 15 *ter* Saldırı Suçu Üzerine Yargı Yetkisinin Kullanılması (Güvenlik Konseyi Başvurusu):** 1. Mahkeme, saldırı suçu üzerindeki yargılama yetkisini bu madde hükümlerine bağlı olarak, madde 13 paragraf (b)'ye uygun olarak kullanabilir. 2. Mahkeme, yargılama yetkisini ancak değişikliklerin otuz Taraf Devlet tarafından onaylanması ya da kabul edilmesinden bir yıl sonra işlenecek saldırı suçları üzerinde kullanabilir. 3. Mahkeme, Statüde bir değişikliğin kabul edilmesi için gerekli olan oy çoğunluğu ile aynı çoğunlukta Taraf Devletin, 1 Ocak 2017 tarihinden sonra alacağı karara bağlı olarak, saldırı suçu üzerinde yargılama yetkisini bu madde kapsamında kullanmaya başlar. 4. Mahkeme dışındaki bir organ tarafından saldırı fiiline yönelik yapılacak bir tespit, bu Statü kapsamında Mahkemenin kendi tespitlerine helal getirmez. 5. Bu madde, madde 5'de değinilen diğer suçların yargılama şartlarına herhangi bir biçimde helal getirmez.

yabileceği genel olarak ifade edilebilir. Saldırı suçu açısından, bir silahlı saldırının sonuçlarının ağır sonuçlar olması gerektiği hem II. Dünya Savaşı'na ilişkin yargılamalarda hem de UCM hazırlık çalışmaları kapsamında ifade edilmiştir. Saldırı suçunun oluşumu açısından silahlı kuvvetlerin kullanılması, ya önemli can ve mal kaybına yol açmalı ya da kısmen ya da tamamen kalıcı veya kısa süreli işgal ya da ilhaka yol açmalıdır[89].

Siber saldırılara ilişkin olarak, saldırı eylemini gerçekleştiren bireyin ya da bireylerin UCM'de yarılanması meselesi, yukarıdaki paragrafta da açıkladığımız üzere, saldırının ağır sonuçlar yaratması neticesi ile ilgilidir. Normal bir silahın etkisini yaratan siber saldırı eylemi, neticesi itibariyle ağır can kayıpları, yaralanmalar veya etkisini uzun süre sürdürecek bir saldırı gerçekleştirmiş ise, saldırıyı gerçekleştiren devlet görevlilerinin yargılanması meselesi söz konusu olabilecektir. Sonuç olarak saldırı suçu açısından, savaş kavramının açıklığa kavuşturulması gereken kısmı, siber saldırıların silahlı kuvvet kullanma eyleminin kapsam ve sonuçları açısından ne şekilde birbirine benzetilebileceği ile ilgilidir. Kanaatimiz II. Dünya Savaşı'na ilişkin yargılamalarda ve UCM hazırlık çalışmalarında sunulan teklifler ve oluşturulan ortak metinlerde, bir silahlı kuvvet kullanma eylemine savaş niteliği kazandıran unsurun, savaşın kapsam ve sonuçları açısından sahip olduğu niteliklerin[90] siber saldırılar açısından da geçerli olacağı şeklindedir.

SONUÇ

Günümüz savaşları, cephelerden siber ortama taşınmış olup, kara, hava, deniz ve uzay alanından sonra siber alan beşinci savaş alanı olarak ifade edilmeye başlamıştır. Teknolojinin gelişmesiyle birlikte devlet kurumlarının bilgi alt yapılarının ve vatandaşların kişisel bilgilerinin gizliliğinin korunması meselesi önemli bir sorun haline gelmiştir.

Siber saldırı ve siber savaş kavramlarının farklı açıklamaları ve konunun uluslararası hukuk nezdinde henüz geçerli bir kabul görmemesi, bu konu ile ilgili yapılacak çalışmalara olan ihtiyacı arttırır niteliktedir. Normal bir savaş stratejisinden çok daha az maliyete ve daha yıkıcı etkilere sahip olabilecek potansiyeli taşıyan siber saldırılar ile ilgili BM nezdinde yeni kuralların belirlenmesi ihtiyacı her geçen gün artmaktadır. Siber saldırı suçunun "kuvvet kullanma" ya da "saldırı suçu" bağ-

89 **ACER**, s.169.

90 **ACER**, s.169.

lamında ne şekilde değerlendirileceği belirtilmeli ve bunlara ne gibi yaptırımlar uygulanacağı da açıklığa kavuşturulması gereken konulardandır.

Çalışmamızda da açıklamaya çalıştığımız üzere bir siber saldırı, silahlı bir saldırının etkilerini oluşturduğu oranda silah gibi değerlendirilecek ve saldırı suçunu meydana gelebilecektir. Bu noktadan hareketle, siber saldırı suçunu işleyen devletlerin ya da devlet görevlilerinin, Uluslararası Adalet Divanı ya da Uluslararası Ceza Mahkemesi'nde yargılanması meselesi gündeme gelebilecektir.

KAYNAKLAR

ACER, Yücel, Uluslararası Hukukta Saldırı Suçu, 2004, Roma Yayınları, Ankara.

ACER, Yücel (2005), "Uluslararası Hukukta Saldırı Suçunun Temel Unsurları: Tanım Çalışmaları ve Yansımalar", *Uluslararası Hukuk ve Politika Dergisi*, Cilt:1, No:3, s.17.

AKYEŞİLMAN, Nezir, Disiplinlerarası Bir Yaklaşımla Siber Politika & Güvenlik, 2018, ORION Kitabevi, Ankara.

ARENDS, J. Frederik, "Homeros'dan Hobbes ve Ötekine:Avrupa Geleneğinde 'Güvenlik' Kavramı", *Uluslararası İlişkilerde Çatışmadan Güvenliğe*, Derleyenler:

AYDIN, Mustafa, BRAUCH, Hans, Günter, ÇELİKPALA, Mitat vd., 2012, İstanbul Bilgi Üniversitesi Yayınları, İstanbul.

AYBAY, Rona/ORAL, Elif, Kamusal Uluslararası Hukuk, 2016, İstanbul Bilgi Üniversitesi Yayınları, 1. Basım, İstanbul.

BAŞARAN, Alper, Siber Savaş Cephesinden Notlar, 2016, Arion Yayınevi, İstanbul.

BAYRAKTAR, Gökhan, Siber Savaş ve Ulusal Güvenlik Stratejisi, 2015, İstanbul.

BRAUCH, Hans, Günter, "Güvenliğin Yeniden Kavramsallaştırılması: Barış, Güvenlik, Kalkınma ve Çevre Kavramsal Dörtlüsü, *Uluslararası İlişkilerde Çatışmadan Güvenliğe*, Derleyenler: AYDIN, Mustafa, BRAUCH, Hans, Günter, ÇELİKPALA, Mitat vd., 2012, İstanbul Bilgi Üniversitesi Yayınları, İstanbul.

BRENNER Susan W. / CLARKE Leo L., "Conscription and Cyber Conflict: Legal Issues", *CCD COE Publications,* 2011,

https://ccdcoe.org/uploads/2018/10/ConscriptionAndCyberConflictLeaglIssues-Brenner-Clarke.pdf.

CANLI, Mustafa: "Siber Güvenlik", *Ankara Siyasal ve Ekonomik Araştırmalar Merkezi Raporu*, 2013, Ankara.

CLAUSEWITZ, Carl, Von, Savaş Üzerine, (Çeviren: Şiar Yalçın), 1977 Spartaküs Yayınları, İstanbul.

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

DEDEOĞLU, Beril, "Yeniden Güvenlik Topluluğu: Benzerliklerin Karşılıklı Bağımlılığından Farklılıkların Birlikteliğine", *Uluslararası*

İlişkilerde Çatışmadan Güvenliğe, Derleyenler: AYDIN, Mustafa, BRAUCH, Hans, Günter, ÇELİKPALA, Mitat vd., 2012, İstanbul Bilgi Üniversitesi Yayınları, İstanbul.

DEMİRAĞ Fahrettin, (2007), "Uluslararası Ceza Divanı, Savaş Suçları – Saldırı Suçu, Mevzuatımıza Göre Savaş Hali", Uluslararası Ceza Divanı, Yayına Hazırlayan: Feridun Yenisey, Arıkan Basım Yayım Dağıtım.

ERDEM, Merve/ÖZOCAK, Gürkan, (2019), "Siber Güvenliğin Sağlanmasında Uluslararası Hukukun ve Türk Hukukunun Rolü, *Ankara Üniversitesi Hukuk Fakültesi Dergisi*, Sayı:68(1).

FLOWERS, Angelyn, "Cyberwar: The What, When, Why and How", *IEEE Technology And Socıety Magazıne,* Fall 2014, s.14,

file:///C:/Users/NewTech/Downloads/Cyberwar_The_What_When_Why_and_How_Commentary%20(1).pdf

GRAY, Chris, Hables, Postmodern Savaş – Yeni Çatışma Politikası, Çev: Derya Kömürcü, 2000, Alfa Yayınları, İstanbul.

GÜMÜŞBAŞ, Ahmet, (2016), "Siber Savaş Hukukunda Meşru Müdafaa Hakkı ve İsnat Edilebilirlik: Stuxnet ve Aramco Saldırıları", Türk-Arap İlişkileri: Çok Boyutlu Güvenlik İnşası "Karşılıklı Bağımlılık İçin Sektörel ve Finansal Derinleşme" TASAM Yayınları Uluslararası İlişkiler Serisi.

GÜNDÜZ Aslan, (1998), Milletlerarası Hukuk Temel Belgeler Örnek Kararlar, Beta Yayınları,

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

KASAPOĞLU, Can, "Hayaletlerin İzlerini Sürmek: Uluslararası Nitelikteki Siber Saldırıların Soruşturulması", EDAM Siber Politikalar ve Dijital Demokrasi Yayınları, 2017/4.

KAYA, İbrahim, Terörle Mücadele ve Uluslararası Hukuk, 2005, USAK Yayınları, Ankara.

KAYA, İbrahim, Uluslararası Hukukta Temel Belgeler, 2013, Seçkin Yayıncılık.

KILIÇ, Ali Şahin, (2009), "Uluslararası Ceza Mahkemesi ve Devletlerin Egemenliği Üzerine Ulusal Egemenlik Odaklı Bir İnceleme", *Ankara Üniversitesi Hukuk Fakültesi Dergisi.*

Kolektif Yazarlar, *Siber Güvenliğe Giriş*, 2017, Kutlu Yayınevi, 1.Bası, İstanbul.

KURT, Selim, "Yeni Terörizmin Geleceğin Güvenlik Ortamına Etkileri: DAEŞ Örneği," *Geleceğin Güvenliği*, Editör: Ahmet Yıldız, 2019, TASAM Yayınları, İstanbul.

KÜÇÜKCAN, Talip, "Terörün Sosyolojisi: Toplumsal Kökenleri Anlama İmkanı", *Uluslararası İlişkilerde Çatışmadan Güvenliğe*, Derleyenler: AYDIN, Mustafa, BRAUCH, Hans, Günter, ÇELİKPALA, Mitat vd., 2012, İstanbul Bilgi Üniversitesi Yayınları, İstanbul.

MERAY, Seha L., Lozan Barış Konferansı – Tutanaklar – Belgeler, Takım 1, Cilt:3, Ankara Üniversitesi Siyasal Bilgiler Fakültesi Yayınları, No:320.

ÖZEL, Cevat/AHİ M. Gökhan, "Bilişim Suçlarında Usul ve Sorumluluk Sistemi Üzerine Öneriler",

http://www.turkhukuksitesi.com/makale_179.htm,

PAZARCI, Hüseyin, *Uluslararası Hukuk*, 2016, Turhan Kitabevi, 15. Basım, Ankara.

SANDIKLI, Atilla/ YİVCİVER, Gökhan: Siber Terörizm Stratejik Rapor, 2014, TASAM Yayınları, Aralık.

SCHIMITT, M/VIHUL, L. (Ed), *Tallinn Manual 2.0 On The International Law Applicable to Cyber Operations*, Cambridge University Press, UK, 2017.

SINGER, Peter, Warren/ FRIEDMAN, Allan: *Siber Güvenlik ve Siber Savaş*, 2015, Buzdağı Yayınevi, Ankara.

ÜNAL Şeref, Uluslararası Hukuk, 1. Basım, Yetkin Yayınları, 2005.

Tallinn Manual On The International Law Applicable To Cyber Warfare, General editor, Michael N. Schmitt, Cambridge University Press 2013.

Tallinn Manual 2.0 On The International Law Applicable To Cyber Operations, General Editor, MICHAEL N. Schmitts, Cambridge University Press 2017.

TEZCAN Durmuş / ERDEM Mustafa Ruhan / ÖNOK Murat, (2017), Uluslararası Ceza Hukuku, Seçkin Yayınları.

TOPAL, Ahmet Hamdi, Uluslararası Terörizm ve Terörist Eylemlere Karşı Kuvvet Kullanımı, 2005, Beta Yayınları.

UZUN, Elif, (2017), Milletlerarası Hukuka Aykırı Eylemlerinden Dolayı Devletin Sorumluluğu, 1. Basım, Seçkin Yayınları

VARLIK Ali Bilgin, Savaşı Tanımlamak: Terminolojik Bir Yaklaşım, Avrasya Terim Dergisi, Cilt: 1, Sayı: 2, 2013.

YILMAZ, Abdullah, Batuhan, (2018), "Siber Ağ Güvenlik kavramının Gelişimi", *CyberMag Dergisi*, Sayı:32.

YILMAZ, Muzaffer, Ercan, "Westphalia'dan Günümüze Savaş", *Uluslararası İlişkilerde Çatışmadan Güvenliğe*, Derleyenler: AYDIN, Mustafa, BRAUCH, Hans, Günter, ÇELİKPALA, Mitat vd., 2012, İstanbul Bilgi Üniversitesi Yayınları, İstanbul.

YILMAZ, Eren, Alper/IRK Orhan, "Nikaragua Divan Kararları Işığında Kuvvet Kullanma ve Meşru Müdafaa Sorunu", *CBÜ Sosyal Bilimler Dergisi*, Cilt:13, Sayı:2, Haziran 2015.

ZABUNOĞLU, H. Gökçe, "Günümüzde Ulus Devlet", *Erciyes Üniversitesi Hukuk Fakültesi Dergisi*, Cilt. XIII, S. 1, (2018).