ULUSLARARASI HUKUK BAĞLAMINDA SİBER SAVAŞ VE SAVAŞ HUKUKU KURALLARININ SİBER SAVAŞA UYGULANABİLİRLİĞİ MESELESİ

Arş. Gör. Erdi ŞAFAK
Yakın Doğu Üniversitesi Hukuk Fakültesi – Kamu Hukuku Bölümü - Uluslararası Hukuk ABD. erdi.safak@neu.edu.tr

GİRİŞ

Savaş, uluslararası hukukta kuvvet kullanmanın en yoğun, en kapsamlı ve etkileri en ağır olan biçimi olarak ifade edilmektedir[1]. Günümüzde silahlı çatışmalar hukukunda, 1907 Lahey Sözleşmeleri, III, XII ve XIV sayılı Sözleşmeleri ve 1949 Cenevre Sözleşmeleri bazı ek düzenlemelerle yürürlüktedir. Uluslararası hukukta, devletler tarafından sınırlı olarak kuvvete başvurulması ise savaşa varmayan kuvvet kullanma yolları olarak ifade edilmektedir[2].

Savaş ya da savaşa varmayan kuvvet kullanma eylemleri ve sonuçlarının bir takım kurallara bağlandığı uluslararası hukuk düzeni, bu kurallara uyulmaması durumunda devletlerin sorumluluğu konusunu da gündeme getirmektedir. Savaşın ilan edilmesi, yürütülmesi ve sona erdirilmesi kuralları genel cephe savaşları için düzenlenmiş olup, yeni savaş yöntemleri ile ilgili düzenlemelere uluslararası hukukta ihtiyaç her geçen gün artmaktadır. Özellikle gelişen teknoloji ile birlikte, klasik silahların yerini siber enstrümanların alacağı yönündeki düşünceler, savaş hukukunda önemli bir sorun halini almaktadır.

Bizde bu noktadan hareketle mevcut savaş hukuku kuralları çerçevesinde, olası bir siber savaş senaryosunun yaşanması durumunda kuralların ne şekilde uygulanabileceğini incelemeye çalışacağız. Bugüne kadar herhangi iki ülke arasında bir siber savaş yaşanmamıştır. Ancak gelişen teknoloji siber savaşın

asla yaşanmayacağı yönündeki düşünceleri sorgular hale getirmiştir. Çalışmamız genel olarak iki bölümden oluşacaktır. İlk olarak silahlı çatışmalar hukuku kurallarını ve bu kuralların siber saldırılara etkisini inceleyeceğiz. İkinci bölüm ise siber savaş örneği sayılabilecek bazı saldırıları yine silahlı çatışmalar hukuku çerçevesinde irdeleyeceğiz.

I. Silahlı Çatışmalar Hukuku Açısından Siber Faaliyetlerin Değerlendirilmesi

Silahlı çatışma kavramını anlamak için genelden özele doğru bir daraltma yapmak gerekirse önce savaş kavramından başlamak gerekmektedir. Grotius'a göre "savaş bir toplumun, bir ulusun veya devletler topluluğunun isteklerini diğer bir ulus ve devletler topluluğuna zorla kabul ettirmek amacıyla giriştikleri bir mücadeledir[3]".

Kuvvet kullanmayı ve şiddeti içeren bir çatı kavram olan savaş, devletler tarafından icra edilmektedir. Muharebe veya çarpışma 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[4].

Pazarcı'nın belirttiği üzere silahlı çatışmalar temel olarak dört şekilde sınıflandırılabilir: 1) Devletlerarasındaki silahlı çatışmalar, 2) Taraflardan bi-

3 **ASLAN, M. Yasin**, Savaş Hukukunun Temel Prensipleri, *Türkiye Barolar Birliği Dergisi*, Sayı 79, 2008, s. 247 / **YEŞİL, Feyzullah**, Uluslararası Hukukta Silahlı Çatışmalar ve Devlet Dışı Aktörler, Türkiye Büyük Millet Meclisi Başkanlığı İdari Teşkilatı Dış İlişkiler Ve Protokol Başkanlığı Uzmanlık Tezi, Ankara – 2015, s.6.

4 **VARLIK, Ali Bilgin**, Savaşı Tanımlamak: Terminolojik Bir Yaklaşım, *Avrasya Terim Dergisi*, Cilt: 1, Sayı: 2, 2013, s. 126. / **YEŞİL**, Uluslararası Hukukta Silahlı Çatışmalar ve Devlet Dışı Aktörler, s.6.

risinin uluslararası örgüt olduğu silahlı çatışmalar, 3) Bir devletin hükümet kuvvetleri ile hükümete karşı gelen silahlı gruplar arasındaki silahlı çatışmalar, 4) Bir devlet içerisinde, değişik silahlı gruplar arasındaki silahlı çatışmalar[5]. Bu noktadan hareketle çalışmamız genel olarak devletlerarasındaki silahlı çatışmaların siber enstrümanlar ile gerçekleştirilmesi üzerine olacaktır.

Devletlerarası silahlı çatışmaları, uluslararası hukuka göre ikiye ayırmak olanaklıdır. Bunlar; savaş ve savaşa varmayan silahlı çatışmalardır. Günümüzde uluslararası sistemde devletlerin birçoğunun taraf olduğu 1949 Cenevre Sözleşmeleri[6]'nin 2.maddesine göre Sözleşme hükümlerinin kapsadığı insancıl hukuk kuralları anlan her iki tür devletlerarası silahlı çatışmalarda da uygulanacaktır[7].

Savaşın geniş kapsamı örf ve âdet kuralları içerisinde yer almakla birlikte bunun yazılı hale getirilmesi evrensel nitelikte kabule ilişkin bir adımdır. Bu çerçevede atılan önemli bir adım 1899 ve 1907 tarihli Lahey Sözleşmeleri ve Bildirileridir. Sözleşmeler sırasıyla şunlardır[8]:

- I Nolu Sözleşme (1899)
- Milletlerarası Uyuşmazlıkların Barışçı Yollarla Çözümüne Dair Sözleşme
- II Nolu Sözleşme (1899)
- Kara Savaşındaki Kural ve Örflere Dair Sözleşme
- III Nolu Sözleşme (1899) – 1864 Tarihli Cenevre Sözleşmesi'nin Deniz Savaşı'na Uyarlanmasına Dair Sözleşme

---

5 **PAZARCI, Hüseyin**, Uluslararası Hukuk Dersleri, IV. Kitap, Turhan Kitabevi, Ankara, 2000, s. 137 / **YEŞİL**, Uluslararası Hukukta Silahlı Çatışmalar ve Devlet Dışı Aktörler, s.6.

6 Cenevre sözleşmeleri ya da Cenevre Konvansiyonları, İsviçre'nin Cenevre şehrinde yapılmış dört muahededir. Uluslararası hukukta insan hakları üzerine yapılmış ve 1949 yılında imzalanmış önemli sözleşmelerdendir ve uluslararası olan veya olmayan çatışma durumlarında silahlı güçler ve insani yardım örgütleri tarafından uyulması beklenen standartları belirler. 1859 yılında Solferino Muharebesi'nde yaşanan vahşete şahit olarak etkilenen Jean Henry Dunant'ın çabaları sonucunda oluşmuştur. Silahlı çatışma hukuku veya harp hukuku olarak da bilinen uluslararası insancıl hukukun temel kaynağıdır.
https://tr.wikipedia.org/wiki/Cenevre_S%C3%B6zle%C5%9Fmeleri

7 **PAZARCI,** Hüseyin, Uluslararası Hukuk Dersleri - 4. Kitap, Turhan Kitabevi, Ankara – 2018, s.165 – 166. / **SUR, Melda**, Uluslararası Hukukun Esasları, Dokuz Eylül Üniversitesi Yayınları, İzmir - 2000, s.273 – 274.

8 **TÜTÜNCÜ, Ayşe, Nur**, İnsancıl Hukuka Giriş, Beta Yayınları, İstanbul – 2012, s.5 – 8. / **ASLAN**, Savaş Hukukunun Temel Prensipleri, s.28 -29. / **YEŞİL, Feyzullah**, Uluslararası Hukukta Silahlı Çatışmalar ve Devlet Dışı Aktörler, Türkiye Büyük Millet Meclisi Başkanlığı İdari Teşkilatı Dış İlişkiler Ve Protokol Başkanlığı Uzmanlık Tezi, Ankara – 2015, s.25 – 26.

- I Nolu Sözleşme (1907)

– Milletlerarası Uyuşmazlıkların Barışçı Yollarla Çözümüne Dair Sözleşme

- II Nolu Sözleşme (1907)

– Sözleşme Borçlarının Ödenmesinde Kuvvet Kullanımının Sınırlanmasına Dair Sözleşme

- III Nolu Sözleşme (1907) – Muhasamatın Başlamasına Dair Sözleşme

- IV Nolu Sözleşme (1907)

– Kara Savaşındaki Kural ve Örflere Dair Sözleşme

- V Nolu Sözleşme (1907) – Bir Kara Savaşında Tarafsız Güçlerin ve Kişilerin Hak ve Görevlerine Dair Sözleşme

- VI Nolu Sözleşme (1907)

– Muhasamatın Başlangıcında Düşman Ticaret Gemilerinin Statüsüne Dair Sözleşme

- VII Nolu Sözleşme (1907)

– Ticaret Gemilerinin Savaş Gemilerine Dönüştürülmesine Dair Sözleşme

- VIII Nolu Sözleşme (1907)

– Otomatik Denizaltı Müsademeli (Dokunmayla Kendiliğinden Patlayan Sualtı Mayınları) Mayınların Döşenmesine Dair Sözleşme

- IX Nolu Sözleşme (1907)

– Savaşta Deniz Kuvvetlerinin Bombardımanına Dair Sözleşme - X Nolu Sözleşme (1907)

– Cenevre Sözleşmesi İlkelerinin Deniz Savaşına Uydurulmasına Dair Sözleşme

- XI Nolu Sözleşme (1907)

– Deniz Savaşında Zapt Hakkının Kullanılmasına Dair Bazı Sınırlamalara İlişkin Sözleşme

- XII Nolu Sözleşme (1907)

– Milletlerarası Ganaim Mahkemesi Kurulmasına Dair Sözleşme - XIII Nolu Sözleşme (1907)

– Deniz Savaşı Sırasında Tarafsız Devletlerin Hak ve Yükümlülüklerine Dair Sözleşme

Uluslararası hukukta savaşın tam olarak tanımlanmasında karşılaşılan zorluklar, uluslararası toplumda devletlerarasında kuvvete başvurulması durumlarının tümünü belirli birtakım uluslararası hukuk kurallarına bağlama isteği ile de birleşince, uygulanan uluslararası hukukta 1949 Cenevre Sözleşmeleri ile getirilen silahlı çatışma kavramı aracılığıyla kısmen aşılmış bulunmaktadır[9].

Tallinn Kitapçığı 20.madde[10] "Silahlı Çatışma Hukukunun Uygulanabilirliği" başlığı altında, siber çatışmaların da silahlı çatışmalar hukuku kurallarına göre yürütülmesini düzenlemiştir. İlgili maddenin devamı; *"Silahlı çatışma bağlamında yürütülen siber operasyonlar, silahlı çatışma yasalarına tabidir"* şeklinde düzenlenmiştir.

Sonuç olarak silahlı çatışma hukuku kuralları çerçevesinde yürütülen siber operasyonlar, silahlı çatışma yasalarına tabidir. Siber enstrümanların kullanılmasında gözetilecek kurallar ve yasaklar bundan sonraki bölümde değerlendirilecektir.

i. Silahlı Çatışmaların Başlatılması ve Hukuksal Durumu Açısından Siber Faaliyetlerin Değerlendirilmesi

Silahlı çatışmalar ile ilgili kuralların açıklanmasından önce bazı kavramları belirtmek yerinde olacaktır. Bu kavramlar *jus ad bellum* ve *jus in bello* olarak iki aşama şeklinde açıklanabilir. *Jus ad bellum* genel itibariyle bir devletin savaşı başlatabilmesi için var olan haklardır. *Jus in bello* ise çatışmanın içeriğine dair bir kavramdır. Çatışmanın başlaması ile *jus in bello* uygulanmaya başlanır. Çatışmayı başlatan sebepler, çatışmanın meşruluğu veya tarafların haklılığı ise *jus in bello*'nun konusu değil *jus ad bellum* ile alakalıdır.

Jus in bello kurallarını içeren üç grup sözleşme bulunduğu görülmektedir. Bunlar; - Lahey tipi sözleşmeler, - Cenevre tipi sözleşmeler, - New York tipi sözleşmelerdir[11].

Silahlı çatışmalar hukuku açısından bakıldığında da *jus in bello* iki ana gruba ayrılmaktadır. Birinci grubu, 1899 ve 1907 yıllarında oluşturulan ve savaş esnasında kullanılması yasak olan silah türleri ve savaş tekniklerini

9 **PAZARCI**, Uluslararası Hukuk Dersleri 4. Kitap, s.167.

10 Tallinn Manual on the International Law Applicable to Cyber Warfare, The law of armed conflict generally, Rule 20 – Applicability of the law of armed conflict.

11 **ASLAN, M. Yasin**, Savaş Hukukunun Temel Prensipleri, *Türkiye Barolar Birliği Dergisi*, Sayı 79, 2008, s.49. / **YEŞİL**, Uluslararası Hukukta Silahlı Çatışmalar ve Devlet Dışı Aktörler, s.39.

düzenleyen Lahey Sözleşmeleri oluşturmaktadır. İkinci grubu ise insancıl hukuk olarak da adlandırılan, 1949 yılında yapılan Cenevre Sözleşmeleri ve bu Sözleşmelere Ek 1977 Protokolleri oluşturmaktadır. İkinci grup kurallar, savaş esnasında sivil halk ve yaralanma, hastalık veya esaret gibi nedenlerle savaşamayacak duruma gelmiş askerlerin korunmasına ilişkindir[12]. Her iki grup da silahlı çatışmaların farklı yönlerini ele alarak birbirini tamamlamaktadır.

Silahlı çatışma bağlamında, silahlı çatışmalar sırasında uygulanacak kurallar (*jus in bello*), tıpkı diğer araçlarda olduğu gibi, düşmanlıklarda siber araçların kullanımını düzenlemek için de geçerlidir. Meşru müdafaa hakkı, kuvvet gerekliliği ve orantı sınırı kullanım esasları ve koşullar siber silahlı saldırı unsuru açısından da değerlendirilecektir. Siber silahlı saldırıya verilen müdahalenin, tepki, gereklilik ve orantılılık gerekliliklerini karşıladığı sürece siber eylem şeklinde olması yasal bir gereklilik değildir[13].

Uluslararası silahlı çatışmalar, savaş ve savaşa varmayan silahlı çatışmalar durumuna göre değişiklik göstermektedir. Savaşın başlaması fiilen bir tarafın ötekine silahlı saldırısı ile gerçekleşebileceği gibi taraflardan birinin ötekine savaş ilan etmesi ile de gerçekleşebilmektedir. Böylece taraflar arasındaki ilişkiler barış hukuku durumundan savaş hukuku durumuna geçmiş olmaktadır[14].

1907 tarihli Muhasamatın Başlamasına Dair III Nolu Lahey Sözleşmesi madde 1.uyarınca da, şu durumda savaşın başlayacağı belirtilmiştir[15]:

1- Bir savaş ilanı varsa (koşulsuz ve hemen etki doğurur)

2- Savaş koşuluna bağlı bir ültimatom verilmişse (koşullu savaş ilanı)

Söz konusu hüküm uyarınca, savaş ilanı ve düşmanca davranış arasında herhangi bir zaman belirlenmediği için ilan, bir saldırıdan hemen sonra olmalı ve Sözleşme'yi ihlal etmemelidir. Böylelikle sürpriz saldırılar, devletlerin hukuki uygulamasından çıkarılamamıştır. Bu Sözleşme'yi çok sınırlı sayıda devlet onayladığı için uygulama, ancak akit devletlerle sınırlı kalmıştır. Akit

12 **ACER, Yücel - KAYA, İbrahim**, Uluslararası Hukuk Temel Ders Kitabı, USAK Yayınları, Ankara, 2013, s.251 – 252. / **YEŞİL**, Uluslararası Hukukta Silahlı Çatışmalar ve Devlet Dışı Aktörler, s.39 – 40.

13 **KOH, Harold, Hongju,** "International Law in Cyberspace", *Harvard Internatıonal Law Journal,* Feature: Online December 2012, Volume: 54, p.3 – 4.

14 **PAZARCI**, Uluslararası Hukuk Dersleri 4. Kitap, s.187.

15 **TÜTÜNCÜ**, İnsancıl Hukuka Giriş, s.58. / **PAZARCI**, Uluslararası Hukuk Dersleri 4. Kitap, s.187-189.

olmayanların kendi aralarındaki ve akitlerle akit olmayanlar arasındaki herhangi bir savaş ise, ilanı gerektirmez.

Savaş ilanı, sadece egemen devletler tarafından yapılabilmektedir. Madde 1'de belirtilen ültimatom, bir devletten diğer devlete normal olarak bir zaman belirleyerek yönetilen nihai bir taleptir. Madde 1'deki ifade dikkate alındığında, ültimatom, düşmanca davranışın belirlenen süre sona erince ve talepler de karşılanmayınca başladığına dair koşullu ama kesin bir tehdit içermektedir[16].

İki devlet arasında savaş ilan etmeden veya koşullu ültimatom olmadan düşmanca davranışlar ortaya çıkarsa, taraflar bunu savaş durumu olarak tanımadıklarını açık bir şekilde belirtmedikçe, bu davranışlar normal olarak hukuki anlamda savaş sayılır. Bazı mahkemeler, saldıran devletin hükümeti, savaş durumunun varlığını kabul etmedikçe veya tanımadıkça, birinin diğerine veya orada yerleşmiş olanlara sadece silahlı kuvvetleriyle saldırmasının, savaş oluşturmadığını kabul etmiştir.

Savaş, egemen devlet olmanın normal bir işlevi olarak görülmüştür. Egemen devletin hak iddiası, bu hakları kullanırken ortaya çıkan uyuşmazlıkları barışçıl yollarla halledememesi, amaçlarını güce başvurarak gerçekleştirmekte özgür olması sonucunu getirmiştir. Bu koşullar altında uluslararası hukukun işlevi, devletlerin barış zamanındaki ilişkilerinde her bir devletin bağımsızlığına dayanarak tasarlanmıştır[17].

Uluslararası hukuk, uluslararası silahlı çatışmaların yürütülmesine ilişkin olarak birtakım genel kurallara sahiptir. Bunlar hem karadaki, hem denizdeki ve hem de havadaki çatışmalara ortak kurallardır. Bu kurallar askeri harekâta ilişkin temel kurallar niteliğindedir.

Siber savaş, siber alanda yürütülmektedir ve bir ülkenin kritik altyapısının bileşenlerini hedefleyerek fiziksel alanda hasara yol açabilir. Siber savaş yürütmek için kullanılan silahlar, geleneksel savaşta kullanılan silahlardan en az iki şekilde farklıdır: Kinetik kuvvet kullanımını içermezler ve sivil halka açık olma eğilimindedirler[18].

---

16 **TÜTÜNCÜ,** İnsancıl Hukuka Giriş, s.52. / **PAZARCI**, Uluslararası Hukuk Dersleri 4. Kitap, s.187-189

17 **TÜTÜNCÜ**, İnsancıl Hukuka Giriş, s.52.

18 **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.

Devlet destekli siber operasyonlar, sadece doğrudan ölüm, yaralanma veya yıkıma neden olmakla kalmayıp aynı zamanda askeri operasyonları veya askeri kapasitesini doğrudan olumsuz yönde etkileyerek başka bir devlete zarar verecek şekilde tasarlandıklarında uluslararası bir silahlı çatışmaya yol açacaktır ve böylece silahlı çatışmalar başlayacaktır[19]. Bu bağlamda daha öncede değindiğimiz üzere, savaşın başlaması fiilen bir tarafın ötekine siber silahlı saldırı gerçekleştirmesi durumunda olabilecektir. Ayrıca, siber silahlı bir saldırı olmadan, devletlerin birbirlerine savaş ilan etmeleri durumunda savaş hukuku kuralları başlayacak olup, bu kurallar siber enstrümanlar için de geçerli olacaktır. Bu noktadan hareketle bir sonraki bölümde silahlı çatışmalar hukuku kurallarının siber savaş durumunda ne şekilde uygulanacağı konusunu incelemeye çalışacağız.

ii. Savaş Alanı

Uluslararası hukukta silahlı çatışmaların hukuka uygun geçtiği alan savaş alanı kavramı biçiminde ortaya çıkmaktadır. Savaş alanı kavramı ile genel olarak uluslararası silahlı çatışmaların geçtiği mekân kastedilmektedir[20]. Savaş hukukunda, bir savaş durumunda coğrafi sınırlar söz konusudur. Savaş yapma yetkisi, coğrafi sınırlamaya tabidir[21]. Bu coğrafi sınırlar devletin ülkesel alanı olan, kara, hava, deniz ve uzay alanlarını kapsamaktadır.

Savaş alanı uygulamada, ilke olarak karadaki uluslararası silahlı çatışmalarla ilgili savaşan devletlerin tüm kara ülkelerini içermektedir. Ancak savaşan tarafların açık ya da üstü kapalı kabulü ile devletlerin kara ülkesinin bir kısmının savaş alanı dışında bırakıldığı da söylenebilir. Buna karşılık, ilke olarak savaş alanı oluşturulmaması gerekmekle birlikte, uygulamada kimi üçüncü devletler ülkelerinin de çeşitli nedenlerle savaş alanı oluşturduğuna rastlanmaktadır[22].

Kinetik savaş ve siber savaş arasındaki ampirik ayrımlardan biri çatışmanın doğasıdır: Kinetik savaşta, iki taraf arasındaki çatışmalar belirli bir fiziksel yerde meydana gelir; ilgili tarafların kuvvetleri, bir tarafın muzaffer olacağı bir mücadeleye girişmektedir. Mücadele, savaşan devletler tarafından sağlanan silahlar, tanklar, patlayıcılar gibi geleneksel silahlarla gerçekleştirilir. Çatışma-

19 **MELZER, Nils,** "Cyberwarfare and International Law", *Ideas For Peace And Security*, https://unidir.org/files/publications/pdfs/cyberwarfare-and-international-law-382.pdf. s.24.

20 **PAZARCI**, **Hüseyin,** Uluslararası Hukuk, Turhan Kitabevi, Ankara – 2018, s.612.

21 **TÜTÜNCÜ**, İnsancıl Hukuka Giriş, s.74.

22 **PAZARCI**, Uluslararası Hukuk s.612.

lar, çatışmaya karışan devletlerden birinin topraklarında meydana gelebilir ve olabilir, ancak modern savaş yasaları uyarınca, savaşan taraflar savaşçı olmayanları mücadeleden korumak için çaba göstermelidir[23].

Tallinn Kitabı, siber savaşın faaliyet alanı ve uygulanması ile ilgili önemli ayrıntılar içermektedir. Kitapçığın *"Egemenlik, Yetki Alanı ve Kontrol"* başlıklı bölümünde siber faaliyetlerin devletlerin egemenlik alanlarında gerçekleşeceği belirtilmiştir. Kitapçığın 3. Maddesi: *" Bir devletin kendi toprakları üzerinde siber altyapıyı ve siber faaliyetleri kontrol edebilme hakkının kaynağı egemenliktir. Buradan devamla, bir devletin karasal topraklarında, iç sularında, deniz yetki alanında (deniz yatağı* dâhil) *ve ulusal hava sahasında bulunan siber altyapılar o devletin egemenliği altındadır*" demektedir. Bu noktadan hareketle kara, deniz ve hava savaşlarının gerçekleştiği devletlerin ülkesel alanlarına, siber savaşların da dâhil olduğunu söylemek mümkündür. Siber alanı, savaş hukuku kurallarında belirtilen savaş alanı olarak da açıklayabiliriz.

Tallinn Kitapçığı 21.madde ise "Coğrafi Sınırlamalar" başlığı altında siber savaşın kara, deniz, hava ve uzayda gerçekleşebileceğini açıklamaya çalışmıştır. İlgili maddenin 1.fıkrası Silahlı çatışma hukuku kurallarının, uluslararası hukukun diğer alanlarıyla birlikte, coğrafyayı siber işlemlerin gerçekleştirilebileceği ilgili alan olarak tanımlamaktadır. İlgili yasal konular arasında siber işlemlerin başlatıldığı yer, gerekli araçların yeri ve hedef siber sistemlerin yeri olarak belirtilmiştir. Kural olarak, siber operasyonlar, çatışmaya tarafların, kara parçaları, ulusal suları veya hava sahasının tüm bölgelerinde ya da uzayda gerçekleştirilebilir[24].

iii. Savaşçılar ve Savaşçı Olmayanlar

Uluslararası hukuka göre savaşçı, silahlı çatışma eylemlerine doğrudan katılma hakkı olan kişidir. Savaşçı olmayan kişiler ise bu hakka sahip olmayan bütün kişilerden oluşmaktadır. Uluslararası hukukta savaşçının ilk kez tanımı 1977 tarihli I. Protokol 43/2.maddesinde[25] biraz dolaylı bir biçimde verilmek-

---

23 **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.

24 Tallinn Manual on the International Law Applicable to Cyber Warfare, Rule 21 – Geographical limitations.

25 **43. maddede** "savaşçı" kavramı, devlet dışı birimler olarak ulusal kurtuluş ordularını ve gerilla savaşçılarını içerecek şekilde ve biraz dolaylı bir biçimde verilmektedir. Bu tanıma göre sağlık ve din görevlileri dışındaki, bir tarafın silahlı kuvvetler mensupları savaşçı olup,

tedir. Bu tanıma göre sağlık ve din görevlileri dışındaki çatışmalara katılan bir tarafın silahlı kuvvetler mensupları savaşçı olup çatışmalara doğrudan katılma hakkına sahiptir[26].

Bir devletin düzenli silahlı kuvvetleri mensuplarından o devletin uyrukluğunu taşıyanların doğrudan çatışmalara katılması durumunda savaşçı statüsü kapsamına girmesi hiçbir hukuksal soruna yer vermezken, yabancıların çatışan bir devletin silahlı kuvvetler mensubu olması birtakım sorunlar ortaya çıkarmaktadır. Bu sorun çatışmalara katılanların gönüllü ya da zorla olması durumlarına göre değerlendirilecektir. Silahlı çatışmalara zorla katılanların uluslararası hukuka aykırı düşecek ve bunlar silahlı kuvvetler mensubu sayılmayacaktır. Ancak Pazarcı'ya göre, bu kişilerin bir yabancının çatışanların düzenli kuvvetler mensubu olması durumunda da bu kişilerin savaşçı statüsünden yararlanması gerektiği yönündedir[27].

Uluslararası silahlı çatışmalarda savaşçı statüsü tanınan ikinci grup kişiler, birtakım koşulları yerine getirmeleri kaydıyla, bir devletin ordusunda yer alan milis kuvvetleri ve gönüllü birlikleri mensuplarıdır. Anılan kişilere savaş kurallarının uygulanmasını öngörmek suretiyle üstü kapalı bir biçimde savaşçı statüsünün tanındığını ilk kabul eden antlaşma 1907 IV Sayılı La Haye Sözleşmesinin ek Yönetmeliğin 1.maddesidir[28]. 1907 IV sayılı La Haye Sözleşmesi'nin ek Yönetmeliğinin 1.maddesi uyarınca uluslararası silahlı çatışmalarda savaşçı statüsü alabilmeleri bir takım kurallara bağlanmıştır. Bu kurallar; i) başlarında astlarından sorumlu bir kişinin bulunması, ii) sabit ve uzaktan seçi-

---

çatışmalara doğrudan katılma hakkına sahiptir. Söz konusu 43. madde, savaşçıların savaş esiri statüsünden yararlanmaları için, çatışan tarafların silahlı kuvvetlerinin silahlı çatışmalarda uygulanan uluslararası hukuk kurallarına uyarak bir iç disiplin rejimine sahip olmalarını şart koşarken 44. madde, saldırı öncesi ve askeri harekât sırasında "gerilla savaşçısı"nın silahını açıkça taşıması koşullarını getirmişti.

26 **PAZARCI**, Uluslararası Hukuk, s.579. / **TAŞDEMİR, Hakan - MÜDERRİSOĞLU, Ruhsar – TÜLÜCE, Hicran,** "12 Ağustos 1949 Tarihli Cenevre Sözleşmelerine Ek Uluslararası Silahlı Çatışmaların Kurbanlarının Korunmasına İlişkin 1 No'lu Protokol (I. Ek Protokol)", Kamu-İş Dergisi; Cilt: 7, Sayı: 2/2003, s.16. / **BAŞER, Murat**, İnsancıl Hukuk – Yeni Savaşlar, Yapısal Sorunlar ve Korunmayan İnsan Hakları, Gazi Kitabevi, Ankara – 2004, s.28 – 30.

27 **PAZARCI**, Uluslararası Hukuk Dersleri 4. Kitap, s.236. / **SUR,** Uluslararası Hukukun Esasları, s.277 – 278. / **BAŞER, Murat**, İnsancıl Hukuk – Yeni Savaşlar, Yapısal Sorunlar ve Korunmayan İnsan Hakları, Gazi Kitabevi, Ankara – 2004, s.28 – 30.

28 1907 IV sayılı La Haye Sözleşmesi'nin ek Yönetmeliğinin 1.maddesi. / **SUR,** Uluslararası Hukukun Esasları, s.278. / **BAŞER,** İnsancıl Hukuk – Yeni Savaşlar, Yapısal Sorunlar ve Korunmayan İnsan Hakları, s.28 – 30.

len ayırt edici bir işaret taşımaları, iii) silahlarını açıkça taşımaları, iv) harekâtlarda savaş yasa ve kurallarına uymaları gerekmektedir[29].

Savaşçı statüsü tanınan üçüncü grup kişiler, birtakım koşullarla kitlesel ayaklanmaya katılan kişiler olmaktadır. Kitlesel ayaklanma kavramı genel olarak ister Hükümetçe çağrı üzerine, isterse kendiliğinden bir halkın düşmana karşı ayaklanarak silahlı mücadeleye girmesi kastedilmektedir. Bu tür ayaklanmalar işgal öncesi olabileceği gibi bir ülke işgal edildikten sonra da söz konusu olabilmektedir[30].

Savaşçı statüsünün tanınması ilgili kişilere öncelikle uluslararası silahlı çatışmalara doğrudan katılma hak ve yetkisini vermektedir. Savaşçı statüsünden yararlanan kişiler karşı tarafın eline düştüğü zaman savaş tutsağı muamelesine bağlı tutulmaktadır.

Sivillerin tanımı I Nolu Ek Protokol'de yapılmıştır. Protokol'ün 50. maddesinde sivillerin kim olduğu belirtilirken, tanım, sivil olmayanlar sayılarak yapılmıştır. 50. maddenin birinci fıkrası şu şekilde düzenlenmiştir:

"Sivil, Üçüncü Sözleşme'nin Madde-4 (A) (1), (2), (3) ve (6)'sında ve bu Protokolün Madde 43'ünde sözü edilen kişi kategorilerine girmeyen kişilerdir. Bir kişinin sivil olup olmadığı konusunda kuşkular olması durumunda, söz konusu kişi sivil sayılacaktır."

Cenevre Sözleşmelerinin Ek I Protokolü uyarınca, siviller savaş dışı statülerini "düşmanlıklara doğrudan katıldıkları sürece" kaybederler[31]. Bu hükme ilişkin yorumlayıcı rehberlik, doğrudan katılımın, savaşan devletler arasında "düşmanlıkların yürütülmesinin bir parçası olarak bireyler tarafından gerçekleştirilen spesifik eylemlerden" oluştuğunu söylemektedirler[32].

---

29 1907 IV sayılı La Haye Sözleşmesi Ek Kara Savaşı Kurallarına İlişkin Yönetmelik Madde: 1 ve 3. / **BAŞER,** İnsancıl Hukuk – Yeni Savaşlar, Yapısal Sorunlar ve Korunmayan İnsan Hakları, s.28 – 30.

30 **PAZARCI**, Uluslararası Hukuk Dersleri 4. Kitap, s.237. / **SUR,** Uluslararası Hukukun Esasları, s.278 – 279. / **BAŞER,** İnsancıl Hukuk – Yeni Savaşlar, Yapısal Sorunlar ve Korunmayan İnsan Hakları, s.28 – 30.

31 Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts (Protocol I) Article 50, June 8, 1977, 1125 U.N.T.S. 3.

32 **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.

Maddede belirtilen Protokol'ün 43. maddesi ise savaşçıları tanımlamaktadır:

"Madde 43: 1. Bir çatışma Tarafına ait olan Silahlı Kuvvetler, söz konusu Taraf karşı Tarafça tanınmayan bir hükümet ya da otorite tarafından temsil ediliyor olsa bile, emrindekilerin yaptıklarından dolayı söz konusu Tarafa karşı sorumlu olduğu bir emir altında bulunan tümüyle organize silahlı kuvvetlerden, gruplardan ve birimlerden oluşur. Bu silahlı kuvvetler, silahlı çatışmalarda uygulanan uluslararası hukuk kurallarına uyulmasını sağlayacak bir iç disiplin sistemine tabi olacaktır.

2. Bir çatışma Tarafının silahlı kuvvetlerine mensup olanlar (Üçüncü Sözleşme'nin Madde 33 ünde kapsanan dini personel ve kurum papazları dışında) savaşçılardır, bir başka deyiş ile doğrudan düşmanca eylemlerde yer alma hakkına sahiptirler.

3. Bir çatışma Tarafı, silahlı kuvvetlerinin bünyesinde bir askeri nitelikli ya da silahlı hukuk uygulama bürosu barındırdığında çatışmaya dâhil olan diğer Taraflara bu konuda tebligatta bulunacaktır."

Uluslararası hukuka göre savaşçı statüsünden yararlanan kişi gruplarından birtakım koşullarda bu niteliğin kaybeden bir başka kişi gurubu da paralı askerler olmaktadır. Paralı asker kavramı ile genel olarak kişisel kazanç amacıyla uyruğundan olunmayan ya da ülkesinde oturulmayan çatışan taraflardan birinin silahlı kuvvetlerine katılarak silahlı çatışmalarda yer alan kişiler belirtilmektedir. Uluslararası silahlı çatışmalar hukukunun geleneksel kuralları bu konuyu ele almamış olup öğretideki ağırlıklı anlayışa göre paralı askerler, milis kuvvetleri ya da direniş harekâtı mensupları arasında yer alarak bunların savaşçı sayılması için aranan koşulları yerine getiriyorsa, paralı askerlerin de savaşçı statüsünden yararlanmasına hiçbir hukuksal engel bulunmamaktadır[33].

Savaş durumunda savaşanlar ile genel olarak iki veya daha fazla ülkenin silahlı kuvvetleri anlaşılmaktadır. Ancak bir siber savaş durumunda, siber saldırıları bir kişi, bir grup, bir örgüt veya bir devlet savaşabilir. NATO Müşterek Siber Savunma Mükemmeliyet Merkezi tarafından hazırlanan "Gürcistan'a Siber Saldırılar: Tanımlanan Yasal Dersler" başlıklı dokümanda Silahlı Çatışma Hukuku'nun siber alanda uygulanması konusu ele alınmıştır. Buna göre;

33 **PAZARCI**, Uluslararası Hukuk Dersleri 4. Kitap, s.242 – 243.

"Silahlı Çatışma Hukuku'nun uygulanabilmesi için gereken şartlardan biri silahlı güçlerin çatışmaya müdahil olmasıdır. Hâlihazırda birçok ülke siber ordu kurmamış veya "siber saldırı" güçleri teşkil etmemiştir. Bu durumda Silahlı Çatışma Hukuku'nun siber savaşa uygulanabilmesi bazı şartlara bağlıdır[34].

Siber saldırılar genellikle devletlerin silahlı kuvvetleri unsurlarınca değil, sivil kişiler tarafından gerçekleştirilmektedir. Olası bir siber savaş durumunda da siber saldırı eylemini gerçekleştiren sivil bir vatandaş olabilir. Bu noktada siber saldırılardan devletlerin sorumlu tutulabilmesi için şahısların eylemlerinin o devletin eylemleri olarak nitelendirilip nitelendirilemeyeceği gibi cevaplanması gereken bazı önemli sorunlar vardır[35]. Bu noktada kanaatimiz olası bir siber savaşta siber saldırıları gerçekleştiren eylemlerin silahlı kuvvet unsurlarınca gerçekleştirilmesi durumunda devletler doğrudan sorumlu tutulabileceklerdir. Olası bir siber savaş durumunda siber saldırı eylemlerini gerçekleştiren sivil vatandaşların eylemleri ise, saldırıyı gerçekleştiren devletle olan ilişki ve aidiyetine bağlı olarak değerlendirilecektir.

Siber saldırı eylemlerini gerçekleştiren bireyler uluslararası literatürde şu şekilde tanımlanmaktadır[36];

- Bilgisayar korsanları,
- Siber teröristler,
- Organize suç örgütleri,
- Endüstri casusları,
- İstihbarat mensupları,
- Kurum içindeki casuslar,
- Yabancı ülkeler.

Siber savaşların harekâtı yönünde ve kazanç elde edebilmesinde bireyler gerek yasal, gerekse yasa dışı yollarla farklı amaçlarla uluslararası arenada yer almaktadır. Özellikle siber anlamda harekâtların yürütülmesinde karşı tarafın olanakları ve kabiliyetleri tam olarak bilinemediği ya da tespit edilemediği için

---

34 ÇİFCİ, Hasan, Her Yönüyle Siber Savaş, TUBİTAK Yayınları, 2. Basım, Ankara - 2017, s.115.

35 ÇİFCİ, Her Yönüyle Siber Savaş, s.115.

36 **KELEŞTEMUR, Atalay,** Siber İstihbarat, Level Kitap, İstanbul – 2015, s.267. / **GÜNTAY, Vahit**, "Siber Güvenliğin Uluslararası Politikada Etki Aracına Dönüşmesi ve Uluslararası Aktörler", *Güvenlik Stratejileri Dergisi,* Yıl:14, Sayı:27, 2018 s.92.

ortak harekat edecek bireylerin veya grupların karakteristik özellikleri doğru tahlil edilmelidir. Bu grupları şu şekilde özetlemek mümkündür[37];

- Bilgisayar Korsanları: Yaptıkları saldırılar neticesinde hedef bilgisayardaki verileri okuyabilir, kopyalayabilir ve değiştirebilirler. Farklı topluluklar oluşturabilen bilgisayar korsanları, bireysel ve gruplar halinde çalışabilmektedir. Sürekli olarak iletişim sistemlerinde yazılımlarında ve internet teknolojilerinde açık arayan bilgisayar korsanları açık buldukları anda durumdan faydalanarak saldırılarını gerçekleştirebilmektedir.

o Siyah Şapkalı Bilgisayar Korsanları: Kötü amaçlı olarak sistemlere sızan, genelde kişisel bilgileri ele geçirmek, tamamen yok etmek gibi saldırgan faaliyetler yürütenlerdir.

o Gri Şapkalı Bilgisayar Korsanları: Sistemlere sadece merak amaçlı sızmakta, herhangi bir kötü amaç taşımamaktadır; fakat yine de yapılan suç teşkil edebilmektedir.

o Beyaz Şapkalı Bilgisayar Korsanları: Siyah şapkalı bilgisayar korsanlarının yapacakları potansiyel tehditleri savuşturmakla yükümlüdür.

· Siber Casuslar: Siber casuslar aslında birer bilgisayar korsanı türevidir. Klasik istihbarat yöntemleri ve anlayışıyla hareket edip siber uzayda etkili olmaya çalışmaktadır. Siber casuslar sızdıkları sisteme zarar vermemekte ve bağlı oldukları yere hizmet etmektedir.

· Toplum Mühendisleri: Toplum mühendisleri ya da sosyal mühendisler olarak da bilinen kişiler, ileri seviyelerde psikoloji ve sosyoloji bilgisine sahiptir. Genellikle istihbarat servisleri tarafından tespit edilmiş kişilere yönelmektedirler. Toplum mühendisleri yazılımsal alandan daha çok insanlar üzerindeki açıklara yönelmektedir.

· Kripto Analizciler: Kriptografik sistemleri ve algoritmaları analiz etmekle görevlidir.

· Ağ ve Sistem Uzmanları: Bir kurum içinde tesis edilmiş olan ağ ve sistemlerin etkin ve sorunsuz çalışmasından sorumlu olan kişilerdir. Bu kişiler aynı zamanda herhangi bir problem olması durumunda problemin kaynağını tespit etme ve kısa sürede çözüm bulma özelliklerine sahiptir.

---

37 **KELEŞTEMUR**, Siber İstihbarat, s.209. / **GÜNTAY**, "Siber Güvenliğin Uluslararası Politikada Etki Aracına Dönüştürülmesi ve Uluslararası Aktörler", s.92.

Harp Zamanında Sivillerin Korunmasına İlişkin IV Nolu Cenevre Sözleşmesi sivillerle ilgili bir sözleşmedir. Bu Sözleşme'de de doğrudan sivilleri tanımlayan bir hüküm bulunmamaktadır. Buna rağmen Sözleşme'de bulunan birçok kuraldan savaşmayan herkesin kapsandığı çıkarımı yapılabilir. Siviller denilince saldırıya uğrayan ya da işgal altında olan devletin vatandaşları akla gelmektedir. Devletin vatandaşları yanı sıra yabancı uyruklu kimseler de bulunabilmektedir. Bu tür yabancı sivillerin belirli koşullarda ülkeyi terk etmelerine izin verilmelidir. Fakat işgalci 18 devlet kendi vatandaşlarını işgal edilen ülkeye yerleştiremez. Savaşanlar ve siviller dışında yer alan özel bir kategori de sağlık ve din görevlileri ile sivil savunma ekipleridir. Bu gruplarda yer alan kişiler özel bir koruma statüsüne sahiptirler[38].

Siber savaşta, sivillerin organize bir silahlı grubun askeri kanadına ait olmayan devlet dışı bilgisayar korsanlarının çoğunu içermesi muhtemeldir. Operasyonları doğrudan düşmanlıklara katılım anlamına geliyorsa, siviller korumalarını kaybederler ve sanki savaşçıymış gibi doğrudan saldırıya uğrayabilirler. Bununla birlikte, savaşçıların aksine, yasal savaş eylemleri için kovuşturmadan muafiyetten yararlanmazlar ve bu nedenle, ulusal yasaların herhangi bir ihlali nedeniyle esirler olarak yargılanabilirler[39].

Siber işlemler genellikle son derece uzmanlaşmış personel tarafından gerçekleştirilir. Savaşan bir devletin silahlı kuvvetlerine üye oldukları ölçüde, statüleri, hakları ve yükümlülükleri geleneksel savaşçılarınkinden farklı değildir.

Siber eylemi gerçekleştiren bireyler farklı grup ve kategorilere göre düzenlenebilmektedir. Siber saldırı eylemi gerçekleştiren bireyler, bilgisayar ve network sistemleri üzerinden ya da bu sistemlere yönelik illegal eylem gerçekleştiren kişilerdir. Bu kişiler genellikle çatışan devletlerin silahlı çatışmalarına doğrudan katılan düzenli silahlı kuvvetleri olamamaktadırlar. Ayrıca bu kişilerin başlarında astlarından sorumlu bir kişinin bulunmamakta, sabit ve uzaktan seçilen ayırt edici bir işaret taşımamaktalar, silahlarını açıkça taşımamaktalar ve harekâtlarda savaş yasa ve kurallarına uymaları tartışmalı bir hal almakta-

---

38 **ACER, Yücel - KAYA, İbrahim,** Uluslararası Hukuk Temel Ders Kitabı, Seçkin Yayıncılık, Ankara – 2014, s.16 – 17.

39 In international armed conflict, civilians deprived of their liberty are protected by the GC IV, AP I and customary law, whereas in non-international armed conflict these protections are reflected in art. 3 common to the Geneva Conventions, AP II and customary law. Depending on the context, human rights law may additionally be relevant. / **MELZER, Nils,** "Cyberwarfare and International Law", *Ideas For Peace And Security*, https://unidir.org/files/publications/pdfs/cyberwarfare-and-international-law-382.pdf. s.35.

dır. Bu bağlamda kanaatimiz ilk olarak siber savaş durumunda, eylemi gerçekleştiren bireyin silahlı kuvvetler mensubu olup olmadığı tespit edilmelidir. İkinci olarak eylemi gerçekleştiren birey sivil bir vatandaş ise eylemi devlet adına gerçekleştirip gerçekleştirilmediğinin tespit edilmesi gerekmektedir.

Tallinn Kitapçığında siber savaşçıların durumu ile ilgili 26.madde[40] "Silahlı Kuvvetlerin Üyeleri" başlığı altında önemli düzenlemeler içermektedir. İlgili madde yukarıda açıkladığımız üzere silahlı kuvvetlerin üyesi olan siber savaşçıların statüsünün ilgili şartlarının silahlı çatışmalar hukukuna tabi olduğudur.

İlgili maddenin 8.fıkrası[41] ise silahlı bir çatışma sırasında siber operasyonlarda bulunan bir kişi, çatışmaya taraf olmayan organize silahlı bir grubun üyesiyse, grubun ve üyelerinin savaşçı kriterlerine uyup uymadıklarına bakılmayacaktır. Bu kişi savaşçı statüsüne sahip olmayacak ve bu nedenle savaşçı dokunulmazlığı olmayıp, savaş esiri olarak da muamele görmeyecektir. Ayrıca Kitapçığın 28.maddesi ise siber operasyonlarda yer alan paralı askerlerin savaşçı dokunulmazlığı ya da savaş esiri statüsüne sahip olmayacaklarını belirtmiştir[42].

Yine ilgili Kitapçığın 32.maddesi[43], "Sivillere Saldırma Yasağı" başlığı altında sivil nüfusun yanı sıra bireysel siviller de siber saldırının konusunun olmayacağını belirtmiştir. 33.madde[44] ise bir kişinin sivil olup olmadığından kuşku duyulması halinde, bu kişinin sivil olarak kabul edilmesi gerektiğini belirtmektedir.

Kitapçığın 34.maddesi[45] "Yasal Saldırı Hedefi Olan Kişiler" başlığı altında siber savaşta hedef alınabilecek bireyleri şu şekilde tanımlamıştır; (a) silahlı kuvvetlerin üyeleri; (b) organize silahlı grupların üyeleri; (c) düşmanlıklarda doğrudan yer alan siviller ve (d) uluslararası bir silahlı çatışmaya katılanlar.

---

40 Tallinn Manual on the International Law Applicable to Cyber Warfare, Rule 26 – Members of the armed forces.

41 Tallinn Manual on the International Law Applicable to Cyber Warfare, Rule 26/8.

42 Tallinn Manual on the International Law Applicable to Cyber Warfare, Rule 28 – Mercenaries.

43 Tallinn Manual on the International Law Applicable to Cyber Warfare, Rule 32 – Prohibition on attacking civilians.

44 Tallinn Manual on the International Law Applicable to Cyber Warfare, Rule 33 – Doubt as to status of persons.

45 Tallinn Manual on the International Law Applicable to Cyber Warfare, Rule 34 – Persons as lawful objects of attack.

iv. Çatışma Araçları ve Yöntemleri

1899 ve 1907 Lahey Sözleşmeleri kapsamında düzenlenen savaş hukuku, savaşta kullanılacak yöntem ve araçları düzenlemektedir. İnsancıl hukuk ise muharebe dışında kalan asker kişileri ve muharebeye hiç katılmayan kişileri korumaktadır. Savaş hukukunun düzenlediği yöntem ve araçlar, insancıl hukukun korumaya çalıştığı değerlere zarar verebileceği için bu iki dal birbirini tamamlayan noktalar içermektedir[46].

1899 ve 1907 Lahey Sözleşmelerinden IV No.lu Sözleşme, devletlerin silahlı çatışmalarda silah ve yöntem olarak "sınırsız seçme hakkına sahip olmadıklarını" öngörmektedir. Bu sözleşmelerden doğan bir başka temel prensip ise, "askeri gereklilikler" ile "insani mülahazalar" arasında bir denge olması gereğidir. Bu konvansiyonların hangi tür silah ve yöntemleri yasakladığına ilişkin ilk temel prensip ise "gereksiz acı ve ölüme yol açan" türden silahların yasaklandığıdır. Bu prensip, yansımaları oldukça geniş olabilecek temel bir prensiptir. Sadece bu prensip gereği, silahlı çatışma taraflarının askeri gerekçelerle açıklanamayacak nitelikte gereksiz acı veren ya da gereksiz ölümlere yol açan, yakıcı, parçalayıcı ve benzeri silahları kullanmaları yasakladığı söylenebilir[47].

Uluslararası hukukta uluslararası silahlı çatışmalar sırasında kullanılacak silahlar ve izlenecek çatışma yöntemleri bakımından uzun süre herhangi bir sınırlamaya rastlanmamakla birlikte, 20.yüzyılda hareket edilen temel anlayış askeri gereklilik ile insancıl düşüncelerin bağdaştırılması olmaktadır. Bu konuda kabul edilen ana ilke, 1907 La Haye Kara Savaşları Kuralları Sözleşmesine ek Yönetmeliğin 22.maddesinde belirtildiği gibi, "Çatışanlar düşmana zarar verme araçlarının seçiminde sınırsız bir hakka sahip değildir" ilkesidir. Aynı ana ilke 1977 I. Protokolünün 35/1.maddesinde, araç seçimine yöntem seçimi öğesi de eklenerek, şöyle açıklanmaktadır: "Herhangi bir silahlı çatışmada tarafların savaş yöntemlerini ve araçlarını seçme hakkı sınırsız değildir[48]."

---

46 ÖKTEM, Emre, Terörizm, İnsancıl Hukuk ve İnsan Hakları, Derin Yayınları, İstanbul – 2011, s.61. / **YEŞİL**, Uluslararası Hukukta Silahlı Çatışmalar ve Devlet Dışı Aktörler, s.39 – 40.

47 **ACER – KAYA**, Uluslararası Hukuk, s.357.

48 **PAZARCI**, Uluslararası Hukuk, s.585. / **TAŞDEMİR, Hakan - MÜDERRİSOĞLU, Ruhsar – TÜLÜCE, Hicran,** "12 Ağustos 1949 Tarihli Cenevre Sözleşmelerine Ek Uluslararası Silahlı Çatışmaların Kurbanlarının Korunmasına İlişkin 1 No'lu Protokol (I. Ek Protokol)", s.19.

Bu ana ilkenin uluslararası hukukta, silahlı çatışma araçları ve yöntemleri bakımından özellikle üç ilke aracılığıyla uygulanması gerçekleştirilmeye çalışılmaktadır. Bunlar, çatışmalarda gereksiz acıların ve ölümlerin yasaklanması, çatışmalar sırasında kimi güven suiistimal nitelikli davranışların yasaklanması ve çatışmalarda savaş dışı kişiler ile sivil yerlerin hedef alınmasının yasaklanması ilkeleridir.

Teknolojik gelişmelerin savaşlara da etki etmesi kaçınılmazdır. Savaşta kullanılan silahların insani sınırlar içinde kontrol edilmesi gereği günden güne artmaktadır. Örneğin yüzyıllar öncesinin savaş aleti olarak kullanılan kılıç ve oklarla ilgili zehirli kılıç ve okların kullanılması yasaklanabilirdi. Oysa günümüzde silahların çeşitlenmesi o kadar ileri düzeydedir ki neredeyse önde gelen her ülkenin kendi silah teknolojisi bulunmaktadır. Bu çeşitliliğin bir sonucu savaşların boyutunun büyümesi ve buna bağlı olarak sivillerin de savaştan doğrudan etkilenir hale gelmesidir. Gelişen savaş teknolojisine göre yapılan bir düzenleme olan 1925 tarihli Savaşta Boğucu, Zehirleyici ve Benzer Gazların ve Bakteriyolojik Savaş Yöntemlerinin Kullanımının Yasaklanmasına Dair Protokol[49] bu çabanın bir sonucu olarak ortaya çıkmıştır[50].

Siber savaşta uygulanan siber enstrümanlar ile ilgili çeşitli görüşler bulunmaktadır. Silahlı kuvvet kullanmanın dinamik yapısı dikkate alındığında, yapısı itibariyle fiziki gücü içermeyen ancak silahlı saldırı ile aynı derecede somut zararlara sebep olabilen siber saldırılar da silahlı bir saldırı gibi değerlendirilebilir[51]. Siber saldırıların dolaylı kinetik etkilerinin, örneğin genel elektrik kesintilerinin, can kaybına neden olabileceği ve bir ülkede hayatın akışına ve asayişe vahim zarar verebileceği için bir silahlı saldırı gibi değerlendirilebileceğini düşünülmektedir[52].

---

49 **Protokol için bkz**. (Protocol for the Prohibition of the Use of Asphyxiating, Poisonous or Other Gases, and of Bacteriological Methods of Warfare. Geneva, 17 June 1925.) https://www.icrc.org/applic/ihl/ihl.nsf/Article.xsp?action=openDocument&documentId=58A096110540867AC12563CD005187B9, Erişim: 11.02.2015 /

50 **YEŞİL**, Uluslararası Hukukta Silahlı Çatışmalar ve Devlet Dışı Aktörler, s.39 – 40.

51 **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.

52 **FİNKELSTEİN, Claire O. / GOVERN, Kevin H.:** "Introduction: Cyber and the Changing Face of War" *Public Law and Legal Theory Research Paper Series Research Paper*, No. 15-20, s.1566. Aktaran: **KASAPOĞLU, Can**, "Siber Savaş: Geleceğin Askeri Gerçekliği ve Günümüzün Bilimkurgusu Arasında, *EDAM Siber Politikalar Kağıtları Serisi*, 2017/2, s.7.

Silahlı çatışmalar hukuku kapsamında savaş yöntemlerine dair sınırlamalar da zaman zaman güncellenerek teknolojik ilerlemeler yakalanmaya çalışılmıştır. Bu konuda uluslararası bazı düzenlemeler yapılmıştır. Bunlar[53];

- 1980 tarihli Fark Gözetmeyen Etkileri Olan ve Aşırı Istıraba Yol Açan Silahların Kullanılmasına Dair Sınırlar veya Yasaklara İlişkin Sözleşme[54],
- 1993 tarihli Kimyevi Silahların Geliştirilmesi, Üretilmesi ve Depolanmasının Yasaklanması ve İmhasına Dair Sözleşme[55],
- 1997 tarihli Anti Personel Mayınların Kullanımının, Depolanmasının, Üretiminin ve Devredilmesinin Yasaklanması ve Bunların İmhası ile İlgili Ottawa Sözleşme[56],
- 2008 tarihli Parça Tesirli Mühimmata Dair Sözleşme[57].

Tallinn Kitapçığı 41.madde[58] "Savaş Araçlarının ve Yöntemlerinin Tanımları" başlığı altında siber savaşta kullanılacak yöntemleri ve araçları tespit etmeye çalışmıştır. İlgili maddeye göre; *"Bu Kılavuzun amaçları doğrultusunda: (a) "siber savaşın araçları" siber silahlar ve bunlarla ilişkili siber sistemlerdir ve (b) 'siber savaş yöntemleri' düşmanlıkların yürütüldüğü siber taktikler, teknikler ve prosedürlerdir."*

Kitapçığın 42.maddesine[59] göre ise siber savaş ya da siber saldırı esna-

---

53 **YEŞİL**, Uluslararası Hukukta Silahlı Çatışmalar ve Devlet Dışı Aktörler, s.38 – 39.

54 Sözleşme için bkz. Convention on Prohibitions or Restrictions on the Use of Certain Conventional Weapons Which May be Deemed to be Excessively Injurious or to Have Indiscriminate Effects. Geneva, 10 October 1980. (https://www.icrc.org/applic/ihl/ihl.nsf/Treaty.xsp?action=openDocument&documentId=7A690F9945FF9ABFC12563CD002D6D8E, Erişim: 11.02.2019).

55 Sözleşme için bkz. http://www.tbmm.gov.tr/tutanaklar/KANUNLAR_KARARLAR/kanuntbmmc080/kanuntbmmc080/kan untbmmc08004238.pdf, Erişim: 11.02.2015 http://www.msb.gov.tr/asad/AskeriMevzuat/Uluslararasi_Antlasmalar/Silahli_Catisma_Hukuku/SC H18.html, Erişim: 11.02.2019.

56 Sözleşme için bkz. http://www.msb.gov.tr/asad/AskeriMevzuat/Uluslararasi_Antlasmalar/Silahli_Catisma_Hukuku/SC H18.html, Erişim: 11.02.2019.

57 Sözleşmeye bugüne kadar 115 ülke katılmıştır. Bkz. Convention on Cluster Munitions, May 2008, http://www.clusterconvention.org/files/2011/01/Convention-ENG.pdf, Erişim: 11.02.2019.

58 Tallinn Manual on the International Law Applicable to Cyber Warfare, Rule 41 – Definitions of means and methods of warfare.

59 Tallinn Manual on the International Law Applicable to Cyber Warfare, Rule 42 – Superfluous

sında, Gereksiz yaralanmaya veya gereksiz acılara neden olacak nitelikte siber savaş araçlarını veya yöntemlerini kullanmak yasaktır.

Tallinn Kitapçığının 43.maddesi[60] ise "Ayrımcı Olmayan Araçlar Veya Yöntemler" başlığı altında, doğası gereği ayrım gözetmeyen siber savaş araçlarını veya yöntemlerini kullanmak yasaktır. Ayrıca 44.madde[61] gereğince ise silahlı çatışma yasasında belirtilen bazı nesnelerle ilişkili siber bubi tuzaklarının kullanılması da yasaktır. 45.madde[62] ise siber savaşın bir yöntemi olarak sivillerin açlığı yasaklanmıştır.

Tallinn Kitapçığının 48.maddesi ise "Silahların Gözden Geçirilmesi" başlığı altında iki önemli tanıma yer vermektedir. Bunlar, Devletlerin, elde ettikleri veya kullandıkları siber savaş araçlarının, Devleti bağlayan silahlı çatışma yasasının kurallarına uymasını sağlaması ve yine Devletler, teknolojik çalışmalarını, bu Protokol tarafından belirlenen kurallar çerçevesinde yeni bir siber savaş yöntemi olarak yasaklanıp yasaklanmadığına dikkat etmelidir.

Bu noktadan hareketle uluslararası silahlı çatışmalar sırasında kullanılacak silahlar ve izlenecek çatışma yöntemleri siber enstrümanlar için de geçerli olacaktır diyebiliriz. Gereksiz acılara ve ölümlere yol açabilecek siber saldırı faaliyetleri, savaş hukuku kuralları çerçevesinde düşünüldüğünde yasaklanan silahlar gibi değerlendirilebilir. Zira yine silahlı çatışmaların yürütülmesi kuralları çerçevesinde kimi silahlar yasaklanmıştır. Yasaklanan silahların birinci gurubu, aşırı derecede yaralayan ve ayrım gözetmeyen etkileri bulunan kimi konvansiyonel silahlara ilişkindir. Ayrıca kimyasal silahlarda yasaklanan silahlar arasında ikinci grubu oluşturmaktadır. Yasaklanan silahların üçüncü grubunu biyolojik ve bakteriyolojik silahlar oluşturmaktadır[63]. Sonuç olarak yasaklanan silahlar kategorisinde gerçekleşecek saldırı faaliyetleri, siber saldırılar çerçevesinde de gerçekleşebilecektir. Örneğin daha öncede değindiğimiz üzere, 2010 yılında ABD'nin İran'ın nükleer kapasitesine yönelik yapılan STUXNET[64] virüs saldırısı sonucunda nükleer tesis önemli bir zarar görmüş-

injury or unnecessary suffering.

60 Tallinn Manual on the International Law Applicable to Cyber Warfare, Rule 43 – Indiscriminate means or methods.

61 Tallinn Manual on the International Law Applicable to Cyber Warfare, Rule 44 – Cyber booby traps.

62 Tallinn Manual on the International Law Applicable to Cyber Warfare, Rule 45 – Starvation.

63 **PAZARCI**, Uluslararası Hukuk, s.587.

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

tür. Saldırı sonucunda nükleer tesiste herhangi bir patlama, yaralanma ya da ölme durumu olmamıştır ancak saldırının etkisi düşünüldüğünde, kimyasal bir silahlı saldırının etkilerine varabileceği tahmin edilmektedir.

Sonuç olarak siber saldırıların sadece kuvvet kullanmanın ötesinde silahlı bir saldırı olarak nitelendirilebilmesi için, en azından bir nevi hasara neden olması gerekmektedir. Bu noktada yine örnek vermek gerekirse, bir siber savaş durumunda herhangi bir barajın kapaklarının siber saldırılarla açılıp bir şehrin sel altında kalmasına ve insanların ölmesine neden olması, silahlı bir saldırı gibi kabul edilebilir[65].

v. Çatışmalarda Kişilerin, Malların ve Çevrenin Korunması

Uluslararası hukukun uluslararası çatışmalar sırasında özel olarak korunmasını düzenlediği kişiler öncelikle bu çatışmaların mağdurları olmaktadır. Bunların başlıcaları hastalar, yaralılar, deniz kazazedeleri, savaş tutsakları ve siviller olmaktadır. Anılan kişi gruplarından başka uluslararası hukuk ayrıca bu kişilerin korunması konusunda hizmet veren başta sağlık ve din görevlileri olmak üzere görevlilere ilişkin olarak da birtakım koruma kuralları içermektedir[66].

Uluslararası silahlı çatışmaların yürütülmesinde bir başka önemli ilke, silahlı çatışmaların yürütülmesi esnasında düşman malların ilke olarak zarara uğratılmamasıdır. Bu ilke, genel bir biçimde 1907 La Haye Yönetmeliği'nin 23/g maddesinde, savaş gereksinimlerinin kaçınılmaz kıldığı durumlar hariç, düşman mallarını yok etmeyi ya da bunlara el konulmasını yasaklamaktadır. Anılan hükümde zarar verilmemesi gereken düşman mallarının niteliği bildirilmediği için, askeri gereklilik dışında kalan, kamuya ya da özel kişilere ait tüm taşınır ve taşınmaz malların bu kapsama sokulduğunu var saymak doğru olacaktır[67].

Uluslararası hukuk kuralları çerçevesinde silahlı çatışmaların sürdürülmesi esnasında çevrenin korunmasına da önem verilmiştir. 1977 tarihli I. Pro-

---

çok İran (%60), fakat aynı santrifüj ve yazılımı kullandıkları için Endonezya, G. Kore, ve Hindistan'da da zarara neden olan bir koddur **AKYEŞİLMAN, Nezir,** Disiplinlerarası Bir Yaklaşımla Siber Politika & Güvenlik, ORION Yayınları, 1. Bası, Ankara - 2018, s.243.

65 ÇİFCİ, Her Yönüyle Siber Savaş, s.113.

66 **PAZARCI**, Uluslararası Hukuk, s.599. / **PAZARCI**, Uluslararası Hukuk Dersleri 4. Kitap, s.272 – 292.

67 **PAZARCI**, Uluslararası Hukuk, s.607. / **SUR,** Uluslararası Hukukun Esasları, s.280./ **PAZARCI**, Uluslararası Hukuk Dersleri 4. Kitap, s.272 – 292.

tokol'ün 35/3.maddesi konu ile ilgili şu düzenlemeye yer vermektedir: *"Doğal çevrede yaygın, uzun süreli ve ağır zararlara neden olan ya da neden olması beklenen savaş yöntemlerinin ya da ara*çlarının kullanılması yasaktır.

Uluslararası çatışmalar sırasında, kültür varlıkları da koruma kapsamına alınmıştır. Eski çağlardan bu yana, savaşlarda insanlığın kültürel mirası tahrip edilmiş, kültürel değeri olan mekânları tahrip etmek, düşmana zarar verme yollarından biri olarak algılanmıştır. 18. yüzyıl ile birlikte kültür mirasının korunması yönünde çabalar başlamıştır. 20. yüzyılın başlaması ile birlikte, yapılan sözleşmelere kültür varlıklarının korunması ile ilgili hükümler konmaya başlanmıştır[68]. 1977 tarihli I. Ek Protokol'de de kültür varlıklarının korunmasına ilişkin hüküm yer almaktadır. Protokol'ün 53. maddesinde, kültür varlıkları koruma kapsamına alınmıştır. Anılan maddede, bu korumanın, Silahlı Çatışmalar Halinde Kültürel Varlıkların Korunması Hakkındaki 1954 tarihli La Haye Sözleşmesinden bağımsız olduğu belirtilmektedir[69].

Belirtilen kurallar çerçevesinde kişilerin, malların ve çevrenin korunması ilkesi, siber faaliyetler açısından da geçerli olacaktır. Zira olası bir siber savaş esnasında özellikle sivillerin zarar görmemesi önemli bir hukuk kuralı olacaktır.

Yeni tür savaş şekli olan siber savaşın sivillere karşı uygulanması, hem Cenevre Sözleşmeleri'nin "sivillerin korunması" kapsamına hem de daha sonra BM'nin onayladığı "gelişigüzel – hedef ayırt etmeyen – etkisi olan silahlar" konulu protokollerin kapsamına girebilir[70].

Tallinn Kitapçığının 47.maddesi[71] "Ek Protokol I Uyarınca Misillemeler" başlığı altında, Devletlerin sivil nüfusu, sivil nesneleri, kültürel nesneleri ve ibadet yerlerini, sivil nüfusun hayatta kalması için vazgeçilmez nesneleri, doğal ortamı ve barajları ve nükleer elektrik üretim istasyonlarına zarar verilmesini yasaklamaktadır.

---

68 **PAZARCI**, Uluslararası Hukuk, s.258 – 259. / **SUR,** Uluslararası Hukukun Esasları, s.280. / **PAZARCI**, Uluslararası Hukuk Dersleri 4. Kitap, s.300.

69 **TAŞDEMİR - MÜDERRİSOĞLU – TÜLÜCE,** "12 Ağustos 1949 Tarihli Cenevre Sözleşmelerine Ek Uluslararası Silahlı Çatışmaların Kurbanlarının Korunmasına İlişkin 1 No'lu Protokol (I. Ek Protokol)", s.14. / **SUR,** Uluslararası Hukukun Esasları, s.280. / **PAZARCI**, Uluslararası Hukuk Dersleri 4. Kitap, s.300.

70 ÇİFCİ, Her Yönüyle Siber Savaş, s.140.

71 Tallinn Manual on the International Law Applicable to Cyber Warfare, Rule 47 – Reprisals under Additional Protocol I.

Kitapçığın 82.maddesi[72] "Kültür Varlıklarına Saygı ve Koruma" başlığı altında şu şekilde düzenlenmiştir; "*Silahlı bir çatışmanın tarafları, siber operasyonlardan etkilenebilecek veya siber alanda yer alan kültürel mülkiyete saygı göstermeli ve korumalıdır. Özellikle dijital kültür varlıklarını askeri amaçlarla kullanmaları yasaktır."* 83.madde[73] ise "Doğal Çevrenin Korunması" başlığı altında şu şekilde düzenlenmiştir; "*(a) Doğal çevre sivil bir nesnedir ve bu nedenle siber saldırılara ve etkilerine karşı genel korumaya sahiptir (b) Ek Protokol I Taraf Devletlerin, doğal çevrede yaygın, uzun vadeli ve ciddi hasara neden olması amaçlanan veya beklenebilecek siber yöntemleri veya savaş araçlarını kullanmaları yasaktır.*

vi. Kara, Deniz ve Havada Uluslararası Silahlı Çatışmaların Yürütülmesine İlişkin Kurallar ve Siber Faaliyetlerin Bu Alanda Yürütülmesi

Karada meydana gelen silahlı çatışmalar belirli bir mekân üzerinde gerçekleşmektedir. Uluslararası hukuk, uluslararası silahlı çatışmaların hukuksal açıdan gerçekleştirilmesi uygun olan alanları belirlemek suretiyle bu alanların dışındaki silahlı çatışmalara hukuksal etkiler atfetmeme ya da kimi yaptırımlar uygulama yoluna gitmektedir[74].

Karadaki silahlı çatışmalarda en çok dikkat edilmesi gereken noktalardan biri yalnızca savaşçılara ve askeri hedeflere saldırılması sınırlaması olmaktadır. Böylece sivil halka, sivil bina ve mallara saldırılması yasaktır.

Karadaki silahlı çatışmalarda en çok dikkat edilmesi gereken noktalardan biri yalnızca savaşçılara ve askeri hedeflere saldırılması yönündedir. Böylece sivil halka, sivil bina ve mallara saldırılması yasaktır. Ancak çatışmalar sırasında kimi savaşçıların sivil halkın arasına saklanarak eylemde bulunması ya da sivil yerlere silah ya da cephane depolamak ya da gizlemek suretiyle buraların askeri amaçla kullanılması ve hatta sivil yerden silahlı eylemlerin gerçekleştirilmesi gibi durumlarda sivil ile askeri hedeflerin ayırt edilmesi zorlaşmaktadır[75].

---

72 Tallinn Manual on the International Law Applicable to Cyber Warfare, Rule 82 – Respect and protection of cultural property.

73 Tallinn Manual on the International Law Applicable to Cyber Warfare, Rule 83 – Protection of the natural environment.

74 **PAZARCI**, Uluslararası Hukuk Dersleri 4. Kitap, s.305. / **PAZARCI**, Uluslararası Hukuk, s.611 – 613.

75 **PAZARCI**, Uluslararası Hukuk Dersleri 4. Kitap, s.308. / **PAZARCI**, Uluslararası Hukuk, s.611 – 613.

Sivil halka, bina ve mallara saldırılması, bir kural dışılık olarak üç durumda olanaklıdır; i) sivil kişilerin yabancı kuvvetlere ya da askeri hedeflere karşı silah kullanması ya da kuvvet kullanması gibi doğrudan çatışmalarda yer alması durumunda yalnızca bu çatışmalar sırasında, ii) sivillerin askeri hedeflerin çok yakınında aynı hedefi oluşturacak bir durumda bulunması, iii) sivillerin saldıranın elde edeceği askeri avantaja oranla aşırı zararlara uğramayacağı durumlarda[76].

Denizdeki silahlı çatışmalarda kullanılan silahlar ve başvurulan yöntemler de bu konuda geçerli olan yukarıda özetlediğimiz genel kurallara uymak zorundadır. Ancak bu genel kurallar yanında yalnızca denizdeki silahlı çatışmalar için söz konusu olan birtakım silah kısıtlaması ya da yöntem yasaklaması kuralları ile de karşılaşılmaktadır. Bu bağlamda denizde silah kısıtlanmasına ilişkin en önemli düzenleme 11.2.1971 tarihli Deniz ve Okyanus Yatağına Nükleer Silahların ve Öteki Kitle Yokedici Silahların Yerleştirilmesinin Yasaklanması Antlaşmasıdır. Hem barış hem de savaş zamanında geçerli olan bu Antlaşmaya göre taraf devletler kıyılarda esas çizgiden 12 mil uzaklıktan itibaren deniz yatağına ve toprak altına nükleer silah ve kitle yokedici silah koymama dolayısıyla da kullanmama yükümünü kabul etmektedirler[77].

Denizdeki uluslararası silahlı çatışmalarda savaşan devletlerin üç tür gemisi söz konusu olmaktadır. Bunlar: savaş gemileri, silahlandırılmış ticaret gemileri ve hastane gemileridir. Uluslararası hukuka göre bir savaş gemisi, ister su üstü gemisi ister su altı gemisi olsun, düşman savaş gemisini önceden uyarmadan saldırma ve batırma yetkisine sahiptir. Yine, bir savaş gemisi düşman savaş gemisini ele geçirdiği zaman bu gemi otomatik olarak ele geçirilen devletin malı olmaktadır[78].

Denizde silah kısıtlamasına ilişkin en önemli düzenleme 11.2.1971 tarihli Deniz ve Okyanus Yatağına Nükleer Silahların ve Öteki Kitle Yokedici Silahların Yerleştirilmesinin Yasaklanması Antlaşmasıdır. Hem barış hem de savaş zamanında geçerli olan bu antlaşmaya göre taraf devletler kıyılarda esas çizgiden 12 mil uzaklıktan itibaren deniz yatağına ve toprak altına nükleer silah ve kitle yokedici silah koymama ve dolayısıyla da kullanmama yükümünü kabul

76 **PAZARCI**, Uluslararası Hukuk Dersleri 4. Kitap, s.309. / **PAZARCI**, Uluslararası Hukuk, s.616 – 622.

77 **PAZARCI**, Uluslararası Hukuk Dersleri 4. Kitap, s.316. / **PAZARCI**, Uluslararası Hukuk, s.622.

78 **PAZARCI**, Uluslararası Hukuk Dersleri 4. Kitap, s.316. / **PAZARCI**, Uluslararası Hukuk, s.622.

etmektedir. Ancak anılan Antlaşmada yalnızca nükleer silahlar açıkça belirtilmiş olup öteki kitle yokedici silahların neler olduğu belirtilmediği için, öteki silahların neleri kapsadığı açıklıkla ortaya çıkmış değildir. Öğreti genellikle öteki silahların biyolojik ve bakteriyolojik silahlarla kimyasal silahlar olduğunu belirtmektedir[79].

Uluslararası hukukta, kara ve deniz savaşları için olanın aksine, havada uluslararası silahlı çatışmalara ilişkin olarak herhangi bir evrensel nitelikli antlaşma bulunmaması nedeniyle hava savaş alanı kavramını açıkça belirleyen herhangi bir bağlayıcı uluslararası belge yoktur. Havada silahlı çatışmalarda kullanılabilecek silahlarla ilgili olarak her türlü fırlatılan patlayıcı ve yakıcı maddenin kullanılması izinli görülmektedir. Bu konuda 1923 La Haye Kuralları anılan silahların açıkça serbest olduğunu öngörmektedir[80].

Havada silahlı çatışmalarda kullanılabilecek silahlarla ilgili olarak her türlü fırlatılan patlayıcı ve yakıcı maddenin kullanılması izinli görülmektedir. Bu konuda 1923 La Haye Kuralları anılan silahların açıkça serbest olduğunu öngörmektedir (madde 18). Devletlerin uygulaması da bu yöndedir. Belirtilen temel ilkeye açıkça getirilen tek sınırlama 1980 tarihli Kimi Konvansiyonel Silahların Kullanılmasının Yasaklanması ve Kısıtlanması Sözleşmesi'nin hava saldırılarında sivillerin yoğun bulunduğu bölgelerde yakıcı silahların kullanımını yasaklaması olmaktadır. Öte yandan, bir takım biyolojik ve kimyasal silahların nerede kullanılırsa kullanılsınlar etkileri aynı olacağı için bu tür silahların havada da kullanılması yasaktır. Bu kısıtlamaya nükleer silahları da eklemek mümkündür[81].

Karada, denizde ya da havada çatışmaların yürütülmesi durumunda belirtilen kurallar siber faaliyetler içinde geçerli olacaktır diyebiliriz. Zira karada belirtilen kuralların temel çerçevesi sivillerin, sivil binaların ve malların zarar görmemesini belirtmektedir. Bu noktada siber enstrümanlar ile sivillere, sivil binalara ya da mallara zarar verilmesi devletlerin sorumluluğunu gündeme getirecektir. Ancak bu durumda özellikle belirtilmesi gereken konu söz konusu siber saldırıların devlete isnat edilmesi meselesidir. Siber saldırıların bir devlet tarafından koordine edilip edilmediğinin anlaşılması oldukça zordur[82]. Siber

79 **PAZARCI**, Uluslararası Hukuk Dersleri 4. Kitap, s.323. / **PAZARCI**, Uluslararası Hukuk, s.622.

80 1923 Tarihli La Haye Antlaşması Madde 18.

81 **PAZARCI**, Uluslararası Hukuk Dersleri 4. Kitap, s.332. / **PAZARCI**, Uluslararası Hukuk, s.626 – 627.

82 **GÜMÜŞBAŞ**, **Ahmet,** "Siber Savaş Hukukunda Meşru Müdafaa Hakkı ve İsnat Edilebilirlik: Stuxnet ve Aramco Saldırıları", *Türk-Arap İlişkileri: Çok Boyutlu Güvenlik İnşası "Karşılıklı*

ortamda eylemin gerçekleştirilmesi ve eylemi gerçekleştiren bireyin ya da bireylerin belirlenmesi ile ilgili özellikleri, siber saldırıların bir devlete isnat edilebilirliğini oldukça güç kılmaktadır. Siber harekâtların anonim olarak farklı ülkelerden, farklı bilgisayarlar kullanılarak gerçekleşmesi eylemlerin arkasındaki esas gücün tespitini oldukça zorlaştırmaktadır. Saldırının kaynağının yani kullanılan bilgisayarın hatta onu kullanan kişinin tespit edilmesi, saldırıyı bir devlete isnat etmek için yeterli değildir.

Karada, denizde ya da havada silahlı çatışmaların gerçekleştirilmesi devletin silahlı unsurlarınca gerçekleştirilmektedir. Siber alanda çalışmamızın bazı bölümlerinde de değindiğimiz üzere bu tür çatışmalar siber ordular vasıtasıyla gerçekleştirilmektedir. "Siber ordu" ülkeyi ya da kurumu siber dünyadan gelebilecek tehdit ve saldırılara karşı koruyacak ve gerektiğinde karşı siber saldırılar gerçekleştirebilecek yetenekteki bilgi güvenliği uzmanlarından oluşturulmaktadır. Siber ordunun mensupları, hem saldırı, hem de koruma yöntemlerini çok iyi bilmek zorundadır. Bu konuda önde gelen ülkelerde genelde iki tür siber ordu bulunmaktadır[83]:

· Devlet eliyle yetiştirilen ve resmi olarak kullanılan birimler ve

· Devlet tarafından desteklenen, gönüllülerden oluşup resmi olmayan birimler.

Siber çatışmalar bilgi ve iletişim ağlarının yaygınlaşmasıyla ve dijitalleşme sürecinde ortaya çıkan, siber teknolojinin kara, hava ya da deniz savaşlarında bir araç olarak kullanılması sosyal, ekonomik ve siyasal nedenlerin hedef alınmasıyla ortaya çıkmıştır. Siber hem teknolojik yapısı hem de sosyal boyutuyla oldukça kapsamlı ve komplike bir ekosistemdir. Hızlı gelişmesi ve yaygınlaşması toplum ve bilim tarafından anlaşılması ve analiz edilmesinde zorluklar ortaya çıkarmaktadır. Siber çatışmaların küresel çatışma trendlerine etkisi, ulusal ve küresel güvenliğe kattığı boyut ve ürettiği tehdit ve caydırıcılık onu analiz etmeyi ve anlamayı zorunlu hale getirmektedir. Siber çatışmalar bugün ve gelecekte küresel, stratejik, askeri ve diplomatik mücadelede bir araç ve yöntem olarak ortaya çıkmakta ve ülkelerin teknolojik gelişmişlik ve dijitalleşmesi kendi aleyhine kullanılabilmektedir[84].

Bağımlılık İçin Sektörel ve Finansal Derinleşme" TASAM Yayınları Uluslararası İlişkiler Serisi, İlk Basım, İstanbul 2016, s188.

83 ÇİFCİ, Her Yönüyle Siber Savaş, s.23.

84 **AKYEŞİLMAN,** Disiplinlerarası Bir Yaklaşımla Siber Politika & Güvenlik, s.208.

vii. Savaş Durumunda Casusluk ve Siber Casusluk Durumu

Uluslararası hukukta yukarıda belirtilen savaşçı statüsünden yararlanan kişilerin birtakım koşullarda bu niteliklerini kaybettikleri kabul edilmektedir. Böylece savaşçı tanımı kapsamına kural dışılık oluşturan bu kişi gruplarından biri casuslardır. Casuslar uluslararası silahlı çatışmalar hukuku çerçevesinde çatışan taraflardan birinin harekât alanı içinde karşı tarafa iletmek üzere gizli bir biçimde bilgi toplamasını belirlemekte olup bu tür eylemlerde bulunan kişiler casus olarak nitelendirilmektedir[85]. Casusluk eyleminden söz edebilmek için eylemin gizli ya da yalancı bir gerekçe altında ve karşı tarafın harekât alanı içerisinde yapılmış olması zorunludur. Böylece 1907 La Haye Yönetmeliğine göre bir asker kişinin üniforması ile karşı tarafın harekât alanında bilgi toplaması ya da sivil kişinin açıkça bu eylemi yapması casusluk kabul edilmektedir[86].

1907 La Haye Yönetmeliğinin 31.maddesine göre casusluk eyleminde bulunan silahlı kuvvetler mensubu kişinin eylemini gerçekleştirip birliğine döndükten sonra yakalanması durumunda savaş tutsağı olarak muamele göreceği öngörüldüğü için, asker kişinin yalancı bir kimlik altında eylem sırasında yakalanması durumunda savaşçı statüsünden yararlanamayacağı belirtilmektedir. Öte yandan 1907 La Haye I. Protokolünün 46.maddesi casusluk eylemi sırasında yakalanan karşı çatışan taraf silahlı kuvvetleri mensubu bir kişinin casusluk muamelesi göreceğini, savaş tutsağı statüsünden yararlanamayacağı ön görmektedir[87].

Siber casusluk, siber alanda kişilerin veya kurumların dijital ayak izlerini takip etmek, terör örgütlerinin olası tehditlerini tespit etmek, siber saldırıların oluşmasını önlemek ve hedefteki kişi veya kurumlara düzenlenecek olan siber saldırıların öncesinde istihbarat toplanması gibi geniş bir alan üzerinde sorumluluk üstlenmiştir. Ayrıca siber saldırılar neticesinde elde edilen bilgiler siber istihbarata dâhil olmaktadır.

Tallinn Kitapçığı 66.madde[88] "Siber casusluk" başlığı altında bazı düzenlemeler içermektedir. İlgili maddeye göre; (a) Silahlı bir çatışma sırasında bir

85 1907 IV Sayılı La Haye Kara Savaşı Kuralları Sözleşmesine Ek Yönetmelik, Mad.29/1. / **PAZARCI**, Uluslararası Hukuk Dersleri 4. Kitap, s.242.

86 **PAZARCI**, Uluslararası Hukuk Dersleri 4. Kitap, s.242.

87 **PAZARCI**, Uluslararası Hukuk Dersleri 4. Kitap, s.242.

88 Tallinn Manual on the International Law Applicable to Cyber Warfare, Rule 66 – Cyber espionage.

düşmana yönelik siber casusluk ve diğer bilgi toplama biçimleri, silahlı çatışma yasasını ihlal etmemektedir; (b) Düşmanların kontrolündeki topraklarda siber casusluk yapan silahlı kuvvetlerin bir üyesi savaş esiri olma hakkını kaybeder ve ait olduğu silahlı kuvvetlere katılmadan önce yakalanırsa casus olarak muamele görebilir.

viii. Silahlı Çatışmaların Durdurulması, Sona Ermesi ve Hukuksal Durum

Uluslararası silahlı çatışmaların durdurulması silahlı çatışmaların kesin bir biçimde sona erdirilmesi anlamına gelmemektedir. Burada söz konusu olan yalnızca silahlı çatışmaların geçici bir süre durdurulması olup, durdurma işleminin kapsamına göre, bu durumda üç değişik kavram çerçevesinde gerçekleşebilmektedir. Böylece uluslararası silahlı çatışmaların durdurulması, uygulanan uluslararası hukukta açıkça tanımlamaları verilmemekle birlikte, ateş-kes, silah bırakma ve teslim şeklindedir[89].

Ateş-kes, belirli bir alandaki silahlı çatışmaya geçici bir süre için ara verilmesini belirtmektedir. Ateş – kes sayesinde çatışan tarafların çatışma alanındaki yaralılarını toplaması ve ölülerini toplayarak gömmesi sağlanmaktadır[90]. Silah bırakışımı, 1907 La Haye IV Sayılı Kara Savaşı Sözleşmesine ek Yönetmeliğin 36.maddesinde, çatışan taraflar arasında karşılıklı anlaşma ile savaş eylemlerinin askıya alınması olarak tanımlanmaktadır[91]. Teslim ise, düşman kuvvetlerin gücüne ve durumuna bağlı olarak bir çatışan tarafın askeri eylemlerine son vermesi ve düşman tarafın iradesini kabullenmesidir[92].

Uluslararası silahlı çatışmaların ise uygulamada değişik yollarla sona erdiği söylenebilir. Bunlar barış antlaşması yapılması da dâhil silahlı çatışmaların tarafların iradesi ile sona ermesi ve çatışan devletlerden birinin ortadan kalkması ile silahlı çatışmaların sona ermesi durumlarıdır[93].

---

89 **PAZARCI**, Uluslararası Hukuk, s.638. / **PAZARCI**, Uluslararası Hukuk Dersleri 4. Kitap, s.348 – 359.

90 **PAZARCI**, Uluslararası Hukuk, s.638. / **PAZARCI**, Uluslararası Hukuk Dersleri 4. Kitap, s.348 – 359.

91 **PAZARCI**, Uluslararası Hukuk, s.639. / **PAZARCI**, Uluslararası Hukuk Dersleri 4. Kitap, s.348 – 359.

92 **PAZARCI**, Uluslararası Hukuk, s.640. / **PAZARCI**, Uluslararası Hukuk Dersleri 4. Kitap, s.348 – 359.

93 **PAZARCI**, Uluslararası Hukuk, s.640. / **PAZARCI**, Uluslararası Hukuk Dersleri 4. Kitap, s.348 – 359.

Silahlı çatışmaların sona ermesi ya da durdurulması ile ilgili kurallar siber savaş içinde geçerli olacaktır. Siber savaş ile ilgili net bir olay henüz gerçekleşmemiş olsa da, olası bir siber savaşın başlaması ve sona ermesi, uluslararası silahlı çatışmalar hukuku kuralları çerçevesinde gerçekleştirilecektir.

II. Siber Savaş Örnekleri Bağlamında Meydana Gelen Olaylar Ve Çatışma Hukuku Kurallarının Uygulanabilirliği Meselesi

i. Estonya Saldırı

Estonya'ya yönelik olarak 2007 yılında Rusya Federasyonu kaynaklı olarak gerçekleştirildiği iddia edilen siber saldırılar, siber güvenlik literatürünün yanı sıra uluslararası hukuk açısından da önemli ayrıntılar içermektedir. Söz konusu siber saldırı, Estonya Parlamentosu'nun Tallinn Meydanı'ndaki Bronz Asker Anıtı'nı kaldırma kararı almasıyla başlamış olmakla birlikte, saldırının arka planında Estonya, Rusya ilişkilerindeki yıllardan beri süregelen gerginliğin yanı sıra, Rusya'nın başta ABD olmak üzere, diğer NATO üyeleriyle yaşadığı küresel mücadelenin de etkisi bulunmaktadır[94].

Estonya Hükümeti'nin İkinci Dünya Savaşı sırasında hayatını Estonya'da kaybeden Rus askerleri anısına dikilen heykelin yerinin değiştirilmesi için aldığı karar sonrası ülkenin internet alt yapısını felç eden Hizmet Dışı Bırakma (DDoS), saldırıları başlamıştır. Saldırılarla Rus Hükümeti arasında doğrudan bir bağlantının varlığına ilişkin bir kanıt olmasa da, saldırıların Rus Hükümeti'nin emriyle gerçekleştirildiğine dair yorumlar yapılmıştır. Yoğun saldırı ile ülkede bankacılık işlemleri, devlete ait internet siteleri haber portalları gibi başlıca internet hizmetleri kullanılamaz hale gelmiştir. Yoğun DDoS bankaları sıkıntıya sokmuş olmasının üstüne bir de kendi sistemlerini kapatmıştır. Saldırıların çoğunun Rusya'dan geldiğinin tespit edilmesi üzerine Estonya yurt dışından gelen internete hatlarını kapatmış ama buna rağmen saldırılar birkaç hafta daha devam etmiştir[95].

---

94 **BIÇAKÇI, Salih**, "Yeni Savaş ve Siber Güvenlik Arasında NATO'nun Yeniden Doğuşu", *Uluslararası İlişkiler*, Cilt 9, Sayı 34 (Yaz 2012), s.214 – 215. **DARILICI**, Siber Uzay ve Siber Güvenlik, s.205. / **Kollektif Yazarlar**, Siber Mücadeleye Giriş, s.191 – 193.

95 «İlk Siber Savaş», https://www.haberturk.com/dunya/haber/23642-ilk-siber-savas, 18.05.2007. / "Estonya'yla Siber Savaş", http://www.gazetevatan.com/estonya-yla-siber-savas-119963-dunya/ 18.05.2007 / **BAŞARAN Alper**, (2016), Siber Savaş Cephesinden Notlar, Arion Yayınevi, s.38. /**AKYEŞİLMAN**, Disiplinlerarası Bir Yaklaşımla Siber Politika, s.239.

Estonya'ya saldırı düzenleyen köle bilgisayarların kontrol merkezinin Rusya'da olduğu ve programın da kiril alfabesi[96] ile yazıldığı tespit edilmiştir. Estonya, NATO'ya konuyu taşıyarak yardım istemiş Rus hükümeti ise saldırıların arkasında olmadığını iddia etmiştir. Dünya kamuoyu bu saldırıların, arkasında Rus Hükümeti veya istihbarat servislerinin olup olmadığını şu ana kadar kesin olarak öğrenememiştir[97].

Estonya'ya yönelik yapılan siber saldırılar üç aşamalı olarak 27 Nisan 2007 yılında başlamış, 2 Mayıs 2007 yılında zirve noktasına ulaşmış ve 8 – 9 Mayıs Rusya'nın zafer günü kutlamalarında da devam etmiştir. Aynı gün dönemin Rusya Devlet Başkanı Vladamir Putin Estonya'yı kınayan mesajlar yayınlamıştır[98].

Siber alanın anonim uzay yapısından kaynaklanan isnat – ispat ilişkisi kurulması noktasındaki zorluk dikkate alınarak, bu saldırıların Rusya kaynaklı olduğunu kesin olarak ispatlamak oldukça zordur. Estonya söz konusu siber saldırıları gerçekleştiren bazı IP'lerin Rusya kaynaklı olduğunu, saldırganların çoğunlukla Rusça dilini kullanarak blog ve forum sayfalarında organize olduklarını, büyük ölçüde bilgisayar korsanlığı tecrübesi olan kişilerden oluştuklarını iddia ederek, saldırı ile ilgili olarak Rusya'yı doğrudan suçlamıştır[99].

Rusya'nın, Estonya'ya yönelik gerçekleştirdiği iddia edilen siber saldırı başta ABD olmak üzere, NATO tarafından siber alanın ortaya koyduğu yeni imkânların Batılı ülkeler için yeni bir tehdit algılaması olarak okumasına

---

96 Kiril alfabesi yaygın olarak Slav dillerinin yazımında kullanılan alfabedir. En eski Slav kitaplarının yazıldığı iki alfabeden biri (diğeri Glagol alfabesi) olan Kiril yazısı, Aziz Kiril ve kardeşi Metodius tarafından 9. yüzyılın ilk çeyreğinde oluşturulmuştur. Yapılan araştırmaların gösterdiklerine göre Kiril ve Metodius'un öğrencileri, 9. yüzyılın ortasında günümüzde Kiril alfabesi olarak bilinen ve halen Rusya, Ukrayna, Bulgaristan, Bosna, Sırbistan ve diğer ülkelerde kullanılan bu alfabeyi Orta Çağ Yunan (Bizans) alfabesinin temelinde geliştirerek Yunancada bulunmayan birtakım Slav seslerini de buraya eklemişlerdi. https://tr.wikipedia.org/wiki/Kiril_alfabesi.

97 ÇİFCİ, Her Yönüyle Siber Savaş, s.184. / **AKYEŞİLMAN**, Disiplinlerarası Bir Yaklaşımla Siber Politika, s.240. / **LEGRİS, Emilie – WALAS**, Dimitri, "Regulation of Cyberspace by International Law: Reflection on Need and Methods", *ESIL Reflections*, Volume:7, Issue:1, http://www.esil-sedi.eu/sites/default/files/ESIL%20Reflection%20Legris%20Walas.pdf.

98 ÇAKMAK, Haydar – SOYOĞLU, İbrahim, Kemal, "Doğu Avrupa ve Asya'dan Siber Saldırı Örnekleri", Suç, Terör ve Savaş Üçgeninde Siber Dünya, **Editörler: ÇAKMAK, Haydar – ALTUNOK**, Taner, Barış Platin Kitabevi, Ankara – 2009, s.121.

99 **YENER, Yavuz**, "8. Yılında Estonya Saldırılarına Çok Boyutlu Bir Bakış", https://siberbulten.com/siber-saldirilar-2/8-yilinda-estonya-saldirilarina-cok-boyutlu-bir-bakis/. 26.03.2015.

neden olmuştur. Bu tarih sonrasında, ABD'nin önderliğinde NATO ortak bir siber güvenlik stratejisi geliştirilmesi noktasında ciddi adımlar atmaya başlamıştır. Bununla birlikte, NATO üyesi ülkelerin her biri de kendi ulusal siber güvenlik stratejileri planlama noktasında yeni girişimlerde bulunmuşlardır[100].

Sonuç olarak Estonya'ya gerçekleştirilen siber saldırılar, BM Antlaşması Madde 2/4 ile bağlantılı "kuvvet kullanma" olarak değerlendirilebilecek ve eylemi gerçekleştiren devletin uluslararası sorumluluğu gündeme gelecektir. Siber saldırı neticesinde herhangi bir ölme ya da yaralanma yaşanmamış olsa da, ülkede bankacılık işlemleri, devlete ait internet siteleri haber portalları gibi başlıca internet hizmetleri kullanılamaz hale gelmesi, doğrudan iç işlerine müdahale ve vatandaşların onurunu zedeleyici bir harekettir.

ii. Gürcistan Saldırısı

Genel ve soyut olarak tarihsel arka plana bakarsak bilindiği üzere, Abhazya ve Güney Osetya, SSCB'nin dağılması sonrasında de facto bağımsız bölgeler olarak varlıklarını sürdürmüşlerdir. 2008 yaz ayları boyunca süregelen bir dizi milliyetçi provokasyon neticesinde, 7 Ağustos 2008 tarihinde Gürcistan Askeri Kuvvetleri'nin ülkenin toprak bütünlüğünü tesis etmek amacıyla Güney Osetya'ya yönelik operasyona başlamasına cevaben, Rus güçleri de 8 Ağustos 2008 tarihinde Osetya'ya girmiş ve sonrasında da Gürcistan'ı işgal operasyonunu faaliyete geçirmiştir[101].

Gürcistan'ın Rusya ile yaşadığı gerginliğin arka planında, bu ülkenin NATO'ya tam üyelik hedefi ve Batı Blok'u ile yakınlaşmasının bulunduğu pek çok kaynakta ileri sürülmektedir. Gürcistan'a yönelik siber saldırılar 7 Ağustos 2008 gecesinden itibaren Estonya saldırılarına benzer şekilde ülkenin kritik alt yapılarını hedef alan hizmet dışı bırakma saldırıları şeklinde başlamıştır. Bu saldırılar da kullanılan siteler incelendiğinde, sitelerin ABD'den çalınan kredi kartlarıyla Rusya ve Türkiye'de açıldığı belirlenmiş, ayrıca saldırı için gönderilen spam e-postaların hazırlandığı da tespit edilmiştir[102].

Gürcistan'a yönelik siber saldırılar da Estonya saldırısına benzer şekil-

---

100 **DARICILI, Ali Burak,** Siber Uzay ve Siber Güvenlik – ABD VE Rusya Federasyonu'nun Siber Güvenlik Stratejilerinin Karşılaştırılmalı Analizi, Dora Yayıncılık, Bursa - 2017, s.207.

101 **BIÇAKÇI,** "Yeni Savaş ve Siber Güvenlik Arasında NATO'nun Yeniden Doğuşu", s.191. / **DARICILI**, Siber Uzay ve Siber Güvenlik, s.211.

102 **BIÇAKÇI,** "Yeni Savaş ve Siber Güvenlik Arasında NATO'nun Yeniden Doğuşu", s.191. / **DARICILI**, Siber Uzay ve Siber Güvenlik, s.211. / ÇAKMAK – DEMİR, "Siber Dünyadaki Tehditler ve Kavramlar", s.47.

de, ülkenin hükümet, medya ve finans sektörlerini felç etmeyi amaçlamıştır. Ancak, Gürcü nüfusunun sadece %10'nun o dönemde internet erişimine sahip olduğu yani Estonya'nın tersine Gürcistan'ın ağlanma oranı ve e-devlet kapasitesi sınırlı olduğu için bu saldırılar Estonya örneğinin aksine kısmen etkili olmuştur. Ayrıca saldırılar esnasında Gürcistan'ın NATO üyeliği henüz gerçekleşmediği için İttifakın güvenlik şemsiyesinden doğrudan yararlanmış fakat NATO uzmanlarından saldırılara karşı koyma noktasında doğrudan destek almıştır[103].

Gürcistan'a gerçekleştirilen siber saldırılar neticesinde Gürcü bankaları sistemlerini kapatmak zorunda kalmıştır. Rus siber savaşçılar daha da ilerleyerek Gürcistan üzerinden dünya bankalarına saldırılar düzenlemiş ve bu bankalar da Gürcistan ile aralarındaki bağlantıları koparmışlardır[104].

Gürcistan'a yönelik olarak düzenlenen siber saldırılardan çıkartılabilecek en önemli sonuç bunun gerçek bir hibrit savaş[105] niteliği taşımasıdır. Geleneksel savaş yöntemlerini kullanan Rusya, eş zamanlı olarak siber saldırıları da başlatmıştır. Rusya'nın uyguladığı bu savaş düzenine hibrit savaş olarak tanımlamak mümkündür. Olayın bu şekilde gerçekleşmesi NATO'nun hibrit savaşa olan inancını destekledi. Ancak siber savaş konusunda NATO'nun kavramsal tercihi "siber güvenlik" kavramını kullanmak olmuştur. Saldırıyla cevap verilmesinin gerekeceği durumlar için de müttefik güçlerinin siber saldırı yeteneklerini kullanmayı planlamaktadır. Geleneksel savaş konusunda hazırlıklı olan NATO siber savunma konusundaki eksikliklerini de Bükreş zirvesi sonrasında hızlıca gidermeye çalıştı. Özellikle NATO Siber Savunma Yönetimi Otoritesi'nin kuruluşunu takip eden ilk 10 ay içinde Siber Harekât'a yönelik kavramları tartışmak üzere beş kez toplanmıştı. Bu toplantılarda NATO'ya

---

103 **DARICILI**, Siber Uzay ve Siber Güvenlik, s.211 – 212. / "Rusya Gürcistan'ı Sanal Alemde de Vurdu", https://www.dw.com/tr/rusya-g%C3%BCrcistan%C4%B1-sanal-alemde-devurdu/a-3575502, 18.08.2008.

104 **Kollektif Yazarlar,** Siber Mücadeleye Giriş, s.195. / ÇİFCİ, Her Yönüyle Siber Savaş, s.185 – 186.

105 Hibrit savaşın "Konvansiyonel, konvansiyonel olmayan ve politik ve ideolojik manipülasyonu da içeren asimetrik araçlardan oluşan bir kombinasyon" olduğunu söylemiş bu savaş türünün "özel harekatlar ve konvansiyonel askeri güçleri; istihbarat ajanlarını; siyasi provokatörleri; medya temsilcilerini; ekonomik açıdan göz dağı vermeyi; siber saldırıları; vekalet savaşı yürüten unsurları, yarı askeri unsurları, terörist ve suç örgütlerini" içerdiği ifade edilmektedir. Detaylı bilgi için bakınız: DUMLUPINAR, Nihat, "Hibrit Savaş: İran Silahlı Kuvvetleri", ANKASAM | *Uluslararası Kriz ve Siyaset Araştırmaları Dergisi*, https://dergipark.org.tr/en/download/article-file/391794, 2017.

ait kavramlar oluşturulmuştu[106].

Gürcistan'a yönelik gerçekleştirilen siber saldırıları, Estonya'ya yönelik saldırılar gibi değerlendirmek mümkündür. Saldırılar sonucu herhangi bir ölme ya da yaralanma olmadığı için, sorumluluk yine iç işlerine karışma ve vatandaşların onurunu kırıp, devletin kamu hizmetlerini yerine getirememesi şeklinde değerlendirmek mümkündür. Bu noktada da yine eylemi gerçekleştiren devletin uluslararası sorumluluğu ihlal ettiği kanısına varmak mümkündür.

iii. İran Saldırısı

Siber savaş örnekleri bağlamında son değerlendireceğimiz örnek vaka 2010 yılında İran'ın nükleer tesislerine yönelik ABD tarafından gerçekleştirildiği iddia edilen "Stuxnet" saldırısıdır. Stuxnet isimli gelişmiş virüs tarafından İran'ın nükleer tesisleri fiziksel hasara uğratılarak, İran'ın nükleer programını sürdürme süreci geciktirilmiştir.

Görüldüğü üzere, "Stuxnet", 2010 Haziran ayında fark edilen ve İran'ın Natanz nükleer geliştirme tesisine saldırmak için geliştirilmiş olan bir siber yazılımdır. Bu saldırı, resmi olarak hiçbir devlet tarafından üstlenilmemiş olsa da saldırı çok büyük ihtimalle ABD – İsrail ortak yapımı bir subversif gizli faaliyet olarak değerlendirilmektedir. Zaten bu iddia ile ilgili olarak bugüne kadar her iki ülkeden de herhangi bir yalanlama gelmemiştir[107].

Stuxnet virüsü, Natanz nükleer tesisindeki çalışmaların uzaktan takibine olanak sağlamakla birlikte santralde bulunan santrifüjlerden[108] yaklaşık 1000

106 **BIÇAKÇI**, "Yeni Savaş ve Siber Güvenlik Arasında NATO'nun Yeniden Doğuşu", s.219. / **DARICILI**, Siber Uzay ve Siber Güvenlik, s.212. / **AKYEŞİLMAN**, Disiplinlerarası Bir Yaklaşımla Siber Politika ve Siber Güvenlik, s.244. / ÇELİK, "Stuxnet Saldırısı ve ABD'nin Siber Savaş Stratejisi: Uluslararası Hukukta Kuvvet Kullanmaktan Kaçınma İlkesi Çerçevesinde Bir Değerlendirme", s.162-163.

107 «İran›a Siber Saldırı Düzenlendiği İddiası», https://www.dw.com/tr/irana-siber-sald%C4%B1r%C4%B1-d%C3%BCzenledi%C4%9Fi-iddias%C4%B1/a-6050644 27.09.2020. **BIÇAKÇI**, **Salih**, "NATO'nun Gelişen Tehdit Algısı: 21. Yüzyılda Siber Güvenlik", *Uluslararası İlişkiler Dergisi*, Cilt 10, Sayı 40 (Kış 2014), s.108. / **DARICILI**, Siber Uzay ve Siber Güvenlik, s.104.

108 **Santrifüj**, genellikle elektrikli bir motor yardımıyla sabit eksenli, dairesel dönme hareketi gerçekleştiren bir laboratuvar aletidir. Santrifüj aletinin yüksek devir sayısı, içerisine yerleştirilen karışımların çökelme prensibine göre ayrılmasını sağlar. Ağır parçalar merkezkaç kuvveti yardımıyla tüpün alt kısmında toplanır (dairesel harekette dışarı doğru gider). Aynı mantıkla daha hafif parçalar tüpün üst kısmına doğru hareket eder (dairesel hareketin merkezine doğru yol alır). Süspansiyonlar veya emülsiyonlar bu şekilde kolaylıkla ayrılabilir. Örneğin kan, en üst kısmında serum, orta kısımda yağ, alt kısımda ise pıhtı kalacak şekilde

tanesini uğrattığı zarar neticesinde durdurmuştur. Uranyum zenginleştirme faaliyetlerinin parçası olan bu nükleer tesisin yaklaşık beşte biri işlemez hale gelmiştir. Santrifüjleri kontrol eden SCADA, sisteminin işleyişi bozarak verim kaybına neden olmuştur. Tamiri aylar sürecek bir hasara sebep olan bu operasyonun geçici surette de olsa fiziki bir zarara sebebiyet verdiği açıktır ve siber kuvvet kullanımı olarak değerlendirilebilecektir[109].

Türünün ilk örneği olan fiziksel tahribata neden olduğu için Stuxnet'i ilk siber silah saldırı olarak değerlendirenler bulunmaktadır. Yine Stuxnet'in dış politika hedeflerine ulaşmak için ülkelerin kullandığı ilk saldırgan siber araç olduğu da ileri sürülmektedir. Konvansiyonel silahların başaramayacağını başaran, kendi kendisini yok ettiğinden ve kaynağı belli olmadığından kurbanı çaresi bırakan Stuxnet, siber uzay, hem siber silah hem de uluslararası savaş konseptini derinden etkileyen çok önemli bir dönüm noktasıdır[110].

Stuxnet saldırısının uluslararası hukukta saldırı suçu teşkil etmesi ve saldırıya karşı meşru müdafaa hakkını doğuracak düzeyde olup olmadığını anlamak için öncelikle eylemlerin 'siber saldırı' eşiğini aşıp aşmadığını tespit etmek gerekmektedir. Bunun değerlendirilmesi, saldırı eyleminin ölçü ve etkileri göz önünde bulundurularak yapılması gerekmektedir[111].

İlk olarak gerçekleşecek siber eylemin ölüm veya yaralanmaya sebebiyet verip vermediği ya da böyle bir durumun oluşacağına dair yakın bir tehdidin olup olmadığının sorgulanması gerekmektedir. Bilişim ve güvenlik şirketlerinin yaptıkları incelemelere göre, Stuxnet saldırısında herhangi bir ölüm veya

---

ayrıştırabilir. https://tr.wikipedia.org/wiki/Santrif%C3%BCj.

109 «İran Santraline Siber Saldırı», https://www.ntv.com.tr/turkiye/iran-santraline-siber-saldiri,AXHxFm9_QkuTRIRoalq78Q, 27.09.2020./
GÜMÜŞBAŞ, "Siber Savaş Hukukunda Meşru Müdafaa Hakkı ve İsnat Edilebilirlik: Stuxnet ve Aramco Saldırıları", s.185. / ÇELİK, "Stuxnet Saldırısı ve ABD'nin Siber Savaş Stratejisi: Uluslararası Hukukta Kuvvet Kullanmaktan Kaçınma İlkesi Çerçevesinde Bir Değerlendirme", s.162-163.

110 **AKYEŞİLMAN**, Disiplinlerarası Bir Yaklaşımla Siber Politika ve Siber Güvenlik, s.244. / **GÜREŞÇİ,** "Siber Saldırıların Uluslararası Hukuktaki Güç Kullanımı Kapsamında Değerlendirilmesi", s.83. / ÇELİK, "Stuxnet Saldırısı ve ABD'nin Siber Savaş Stratejisi: Uluslararası Hukukta Kuvvet Kullanmaktan Kaçınma İlkesi Çerçevesinde Bir Değerlendirme", s.162-163.

111 **GÜMÜŞBAŞ,** "Siber Savaş Hukukunda Meşru Müdafaa Hakkı ve İsnat Edilebilirlik: Stuxnet ve Aramco Saldırıları", s188. / **AKYEŞİLMAN**, Disiplinlerarası Bir Yaklaşımla Siber Politika ve Siber Güvenlik, s.244. / ÇELİK, "Stuxnet Saldırısı ve ABD'nin Siber Savaş Stratejisi: Uluslararası Hukukta Kuvvet Kullanmaktan Kaçınma İlkesi Çerçevesinde Bir Değerlendirme", s.162-163.

yaralanma olmuş, ne de böyle bir yakın tehdit öngörülmüştür. Stıxnet saldırısı, nükleer santrifüjlerde erime ve yanmaya sebebiyet verse de bunlar can kaybı ya da yaralanmaya sebebiyet düzeyde etkilere sahip bir eylem olarak görülmemiştir[112].

Stuxnet saldırısı, esas itibariyle İran'ın nükleer kapasite geliştirme faaliyetlerinin takip edilmesi ve santrallerin işleyişlerini bozarak nükleer programın ertelenmesi amaçlanmakta idi. Ülkenin enerji altyapısı için kritik önemi haiz bir nükleer tesisi hedef alan bu eylem, ancak ciddi düzeyde yıkıcı bir etki olması veya enerji arzını sarsacak şekilde ciddi bir aksaklığa sebebiyet vermesi durumunda 'siber saldırı' olarak nitelenebilecektir. Bu yüzden de 'siber saldırı' eşiğini aşmayan bu operasyonun, İran'ın meşru müdafaa hakkını doğurmadığı söylenebilecektir[113].

Stuxnet'in iddia edildiği üzere Amerika ve İsrail'e isnat edilebilmesi için ciddi delillerin bulunması gerekmektedir. ABD, söz konusu saldırıda bir rolü olduğuna dair herhangi bir resmi beyanda bulunmamıştır. Ancak İran Sivil Savunma Kurumu, yaptığı açıklamada Stuxnet virüsünün nükleer santrallere ilişkin edindiği bilgileri nereye rapor ettiğinin izinin sürüldüğünü ve buranın ABD'nin Texsas eyaletinde olduğunu tespit ettiklerini iddia etmişlerdir. Bunun yanında birçok bilişim uzmanı saldırının arkasında ABD ve İsrail'in olduğunu iddia etmiştir. Ancak tüm bunlara rağmen isnat edilebilirlik standartlarını sağlayacak güçlü deliller ortaya konulamamıştır.

Stuxnet saldırısı meşru müdafaa hakkını doğuracak düzeyde siber saldırılar olsaydı bile, isnat edilebilirlik standartları sağlanamadığı için iddialara konu olan ABD ve İsrail eylemlerden sorumlu tutulamayacaklardır[114].

---

112 **GÜMÜŞBAŞ,** "Siber Savaş Hukukunda Meşru Müdafaa Hakkı ve İsnat Edilebilirlik: Stuxnet ve Aramco Saldırıları", s188. / **AKYEŞİLMAN**, Disiplinlerarası Bir Yaklaşımla Siber Politika ve Siber Güvenlik, s.244. / ÇELİK, "Stuxnet Saldırısı ve ABD'nin Siber Savaş Stratejisi: Uluslararası Hukukta Kuvvet Kullanmaktan Kaçınma İlkesi Çerçevesinde Bir Değerlendirme", s.162-163.

113 **GÜREŞÇİ, Ramazan**, Siber Saldırıların Uluslararası Hukuktaki Güç Kullanımı Kapsamında Değerlendirilmesi, *Savunma Bilimleri Dergisi,* Mayıs 2019, Cilt:18, Sayı:1, s.83. / **AKYEŞİLMAN**, Disiplinlerarası Bir Yaklaşımla Siber Politika ve Siber Güvenlik, s.244. / ÇELİK, "Stuxnet Saldırısı ve ABD'nin Siber Savaş Stratejisi: Uluslararası Hukukta Kuvvet Kullanmaktan Kaçınma İlkesi Çerçevesinde Bir Değerlendirme", s.162-163.

114 ÇELİK, "Stuxnet Saldırısı ve ABD'nin Siber Savaş Stratejisi: Uluslararası Hukukta Kuvvet Kullanmaktan Kaçınma İlkesi Çerçevesinde Bir Değerlendirme", s.162-163.

SONUÇ

Uluslararası hukukta silahlı çatışmalarda hukuka uygun araç ve yöntemlerin kullanılması ve savaş başladıktan sonra bazı kurallara uyulması uluslararası antlaşmalar ile belirlenmeye çalışılmıştır. Bu kurallara uyulmaması durumunda ise devletlerin sorumluluğu gündeme gelecektir ve kurallara uymayan devlete karşı bazı yaptırım metotları uygulanabilecektir.

Uluslararası silahlı çatışmalar ile ilgili hukuki düzenlemeler, kara, deniz ve hava savaşları ile ilgili düzenlemelere yer vermektedir. Ancak bu düzenlemeler gelişen teknoloji ile birlikte bazı yeni kuralların oluşması ihtiyacı hissedilmektedir. Bizde bu kapsamda çalışmamızda olası bir siber savaş durumunda mevcut kuralların, siber savaş için geçerli olup olmayacağı meselesini değerlendirmeye çalıştık. Mevcut kurallardan ilki savaş alanı ve savaşın ilan edilmesi ile ilgilidir. Bu iki kural çerçevesinde siber savaş esnasında devletlerin ülkesel alanı da savaş alanı olarak kabul edilebilecektir. Savaş ilan edilmesi meselesi ise uluslararası hukukta zorunlu olmadığı için, siber savaş durumunda da herhangi bir ilanda bulunma zorunluluğu yoktur. Siber savaş ile ilgili en önemli meselelerden birisi, silahlı çatışmalar hukukunda belirtilen savaşçı tanımının, siber savaşçılar için uygulanmasının zorluğudur. Siber savaşçılar genellikle silahlı kuvvetler mensubu olmayı, sivil vatandaşlar olmaktadır. Ancak yine de bu durum silahlı çatışmalar hukuku kuralları bu kişiler için de geçerli olup, devletlerin bu kişiler üzerinde de denetim ve kontrol yetkisi bulunmaktadır. Son olarak kara, deniz ve hava da silahlı çatışmaların yürütülmesi de yine siber savaş için de geçerli olacaktır. Burada dikkat edilmesi gereken esas nokta, siber saldırılardan kullanılan siber enstrümanların silahlı bir saldırının etkisini doğuracak sonuç yaratması beklenmektedir.

Günümüzde NATO ve BM gibi uluslararası kuruluşlar siber savaş ile ilgili bazı kuralların oluşması yönünde çalışmalar gerçekleştirmektedir. Bu zamana kadar herhangi bir siber savaş gerçekleşmemiştir. Ancak daha önce de değindiğimiz üzere teknolojinin her geçen hızlı bir şekilde gelişmesi, ilerleyen yıllarda savaş konseptini de değiştirebilecektir diyebiliriz.

KAYNAKÇA

ACER, Yücel - KAYA, İbrahim, Uluslararası Hukuk Temel Ders Kitabı, Seçkin Yayıncılık, Ankara – 2014.

ASLAN, M. Yasin, Savaş Hukukunun Temel Prensipleri, Türkiye Barolar Birliği Dergisi, Sayı 79, 2008.

BAŞER, Murat, İnsancıl Hukuk – Yeni Savaşlar, Yapısal Sorunlar ve Korunmayan İnsan Hakları, Gazi Kitabevi, Ankara – 2004.

BIÇAKÇI, Salih, "Yeni Savaş ve Siber Güvenlik Arasında NATO'nun Yeniden Doğuşu", Uluslararası İlişkiler, Cilt 9, Sayı 34 (Yaz 2012).

BIÇAKÇI, Salih, "NATO'nun Gelişen Tehdit Algısı: 21. Yüzyılda Siber Güvenlik", Uluslararası İlişkiler Dergisi, Cilt 10, Sayı 40 (Kış 2014).

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.

ÇAKMAK, Haydar – SOYOĞLU, İbrahim, Kemal, "Doğu Avrupa ve Asya'dan Siber Saldırı Örnekleri", Suç, Terör ve Savaş Üçgeninde Siber Dünya, Editörler: ÇAKMAK, Haydar – ALTUNOK, Taner, Barış Platin Kitabevi, Ankara – 2009.

DARICILI, Ali Burak, Siber Uzay ve Siber Güvenlik – ABD VE Rusya Federasyonu'nun Siber Güvenlik Stratejilerinin Karşılaştırılmalı Analizi, Dora Yayıncılık, Bursa – 2017.

FİNKELSTEİN, Claire O. / GOVERN, Kevin H.: "Introduction: Cyber and the Changing Face of War" Public Law and Legal Theory Research Paper Series Research Paper, No. 15-20, s.1566. Aktaran: KASAPOĞLU, Can, "Siber Savaş: Geleceğin Askeri Gerçekliği ve Günümüzün Bilimkurgusu Arasında, EDAM Siber Politikalar Kağıtları Serisi, 2017/2.

GÜNTAY, Vahit, "Siber Güvenliğin Uluslararası Politikada Etki Aracına Dönüşmesi ve Uluslararası Aktörler", Güvenlik Stratejileri Dergisi, Yıl:14, Sayı:27, 2018.

GÜMÜŞBAŞ, Ahmet, "Siber Savaş Hukukunda Meşru Müdafaa Hakkı ve İsnat Edilebilirlik: Stuxnet ve Aramco Saldırıları", Türk-Arap İlişkile-

ri: Çok Boyutlu Güvenlik İnşası "Karşılıklı Bağımlılık İçin Sektörel ve Finansal Derinleşme" TASAM Yayınları Uluslararası İlişkiler Serisi, İlk Basım, İstanbul 2016.

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

KELEŞTEMUR, Atalay, Siber İstihbarat, Level Kitap, İstanbul – 2015.

KESKİN, Funda, Uluslararası Hukukta Kuvvet Kullanma: Savaş, Karışma ve Birleşmiş Milletler, Mülkiye Birliği Vakfı Yayınları Tezler Dizisi:4, Ankara 1998.

KOH, Harold, Hongju, "International Law in Cyberspace", Harvard Internatıonal Law Journal, Feature: Online December 2012, Volume: 54.

LEGRİS, Emilie – WALAS, Dimitri, "Regulation of Cyberspace by International Law: Reflection on Need and Methods", ESIL Reflections, Volume:7, Issue:1,

http://www.esil-sedi.eu/sites/def ault/files/ESIL%20Reflection%20Legris%20Walas.pdf.

MELZER, Nils, "Cyberwarfare and International Law", Ideas For Peace And Securıty,

https://unidir.org/files/publications/pdfs/cyberwarfare-and-international-law-382.pdf.

ÖKTEM, Emre, Terörizm, İnsancıl Hukuk ve İnsan Hakları, Derin Yayınları, İstanbul – 2011.

PAZARCI, Hüseyin, Uluslararası Hukuk Dersleri, IV. Kitap, Turhan Kitabevi, Ankara, 2000.

PAZARCI, Hüseyin, Uluslararası Hukuk Dersleri - 4. Kitap, Turhan Kitabevi, Ankara – 2018.

SUR, Melda, Uluslararası Hukukun Esasları, Dokuz Eylül Üniversitesi Yayınları, İzmir – 2000.

TAŞDEMİR, Hakan - MÜDERRİSOĞLU, Ruhsar – TÜLÜCE, Hicran, "12 Ağustos 1949 Tarihli Cenevre Sözleşmelerine Ek Uluslararası Silahlı Çatışmaların Kurbanlarının Korunmasına İlişkin 1 No'lu Protokol (I. Ek

Protokol)", Kamu-İş Dergisi; Cilt: 7, Sayı: 2/2003, s.16.

TÜTÜNCÜ, Ayşe, Nur, İnsancıl Hukuka Giriş, Beta Yayınları, İstanbul – 2012.

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

YENER, Yavuz, "8. Yılında Estonya Saldırılarına Çok Boyutlu Bir Bakış",

https://siberbulten.com/siber-saldirilar-2/8-yilinda-estonya-saldirilarina-cok-boyutlu-bir-bakis/. 26.03.2015.

YEŞİL, Feyzullah, Uluslararası Hukukta Silahlı Çatışmalar ve Devlet Dışı Aktörler, Türkiye Büyük Millet Meclisi Başkanlığı İdari Teşkilatı Dış İlişkiler Ve Protokol Başkanlığı Uzmanlık Tezi, Ankara – 2015.

İnternet Haber Kaynakları

"İran'a Siber Saldırı Düzenlendiği İddiası",

https://www.dw.com/tr/irana-siber-sald%C4%B1r%C4%B1-d%C3%BCzenledi%C4%9Fi-iddias%C4%B1/a-6050644 27.09.2020.

"İran Santraline Siber Saldırı",

https://www.ntv.com.tr/turkiye/iran-santraline-siber-saldiri,AXHxFm9_QkuTRIRoalq78Q, 27.09.2020.

"Rusya Gürcistan'ı Sanal Alemde de Vurdu",

https://www.dw.com/tr/rusya-g%C3%BCrcistan%C4%B1-sanal-alemde-de-vurdu/a-3575502, 18.08.2008.