ÇANAKKALE ARAŞTIRMALARI TÜRK YILLIĞI

Yıl / Year **20** Sayı / Issue **32** Bahar / Spring **2022** ss. **21-45**

Geliş Tarihi: 20.01.2022 Kabul Tarihi: 26.02.2022

# Siber Saldırıların BM Şartı'nda Yer Alan Silahlı Saldırı Kavramı Kapsamında Değerlendirilmesi

**Muharrem Uğur BOZKURT***

**Özet**

*Teknolojinin gelişimi, bilgisayarların kullanım alanlarının yaygınlaşması ve bilgisayara olan bağımlılığın artmasıyla birlikte siber uzay da bir savaş alanı haline gelmiştir. Siber uzaydaki askeri faaliyetlere yönelik uluslararası düzenleme olmayışı, buradaki eylemlerin uluslararası hukukun kapsamı dışında olduğu anlamına gelmemektedir. BM Şartı'nda yer alan ilke ve yasakların, nispeten yeni bir kuvvet kullanma şekli olan siber savaş için de geçerli olduğu kabul edilmektedir. Kuvvet kullanma yasağının istisnası olan meşru müdafaa hakkının kullanılabilmesi için bir silahlı saldırının gerçekleşmiş olması ön koşulu aranmaktadır. Gerçekleşen silahlı saldırının hangi silahları içerdiği saldırının varlığını etkilememektedir. Bir silah olarak siber yöntemlerin kullanımı sonucunda ortaya çıkan etkilerin kinetik etkiye sahip silahlarla gerçekleştirilecek saldırılar seviyesine çıkabileceği yaşanmış örneklerle sabittir. Bu nedenle boyut ve etkileri bakımından belirli bir eşiği aşan siber saldırılar meşru müdafaa hakkına esas teşkil edecek silahlı saldırıyı oluşturabilir.*

**Anahtar Kelimeler:** *Siber Savaş, Siber Saldırı, Silahlı Saldırı, Meşru Müdafaa.*

**Assessment of Cyber Attacks within the Concept of Armed Attack in the UN Charter**

**Abstract**

*Cyber space became a new domain of warfare with the development of technology, proliferation of usage areas of computers and increased dependency on computer systems. Absence of an international regulation for military activities in the cyber domain does not mean these activities are beyond the scope of international law. The principles and prohibitions in the UN Charter are regarded to be in force for cyber warfare which is a comparatively new way of use of force. In order to use the right of self defence, which is an exception of the prohibition of use of force, occurrence of an armed attack is required. The weapons, which the actual armed attack comprised of, does not affect the existence of the attack. It is proven with experience that the effects resulting from the use of cyber methods as a weapon can reach the level of attacks with weapons with kinetic effects. Therefore, cyber attacks those surpass a threshold in terms of their scale and effects may constitute an armed attack which will be the basis for self defence.*

**Keywords:** *Cyber Warfare, Cyber Attack, Armed Attack, Self Defence.*

* Orcid: 0000-0002-3343-1857 E-posta: ubozkurt@gmail.com

## Giriş

Teknolojik gelişme giderek artan bir hızla sürerken silahlı kuvvetler de bundan payına düşeni almaktadır. Hatta günlük hayatımızda kullandığımız birçok teknolojinin (mikrodalga, GPS, bilgisayar ve hatta internet) savunma sanayii laboratuvarlarında geliştirildiğini söylemek yanlış olmayacaktır. Daima daha etkin, düşmanı daha uzaktan vuran ve kendine yönelik riskleri en aza indirmeyi amaçlayan silahlara sahip olma arzusu, silah sanayiini önemli bir araştırma geliştirme alanı haline getirmektedir. Özellikle anavatanın uzağında askeri güç kullanımı sonucunda meydana gelen can kayıplarının toplumda yarattığı hassasiyetin giderek artması ve kamuoyunun yönetimler üzerindeki artan baskısı, devletleri savaş alanına ayak basmadan istediğini elde etmeye yönelik yöntemler geliştirmeye itmektedir. Bu yöntemler balistik füzeler, insansız sistemler gibi açık askeri yetenekler olabildiği gibi, bunları destekleyen örtülü, doğrudan kaynağına atfedilmesi güç araçları da içerebilmektedir.

Elektroniğin silah teknolojisine dahil olmasıyla savaşın boyutları da değişmiştir. Önceleri daha çok elektromanyetik spektrumun kullanımından ibaret olan elektronik harp, zamanla genişleyerek bilgi savaşı halini almıştır. Bilgi savaşı fiziki ortama ek olarak siber ortamda da devam etmektedir. Siber uzay veya siber ortam *"tüm dünyaya ve uzaya yayılmış durumda bulunan bilişim sistemlerinden ve bunları birbirine bağlayan ağlardan oluşan veya bağımsız bilgi sistemlerinden oluşan sayısal ortam"* olarak tanımlanmaktadır[1]. Bu ortamdaki faaliyetler siber takısı ile ifade edilmektedir (siber savaş, siber saldırı, siber güvenlik vb.).

Siber ortamdaki askeri faaliyetler çok geniş bir çerçevede yürütülebilmektedir. Pasif olarak ağa dair bilgi alınmasından, bilgisayarlar tarafından takip ve kontrol edilen fiziki sistemlerin kontrolünün ele geçirilmesi veya bu sistemlerin çalışmalarına müdahale edilmesine kadar yayılan bir yelpazede gerçekleşebilen faaliyetler, ağdaki verinin imha edilmesi, ağda aktif olarak sahte trafik üretilmesi, veri tabanındaki bilgilerin değiştirilmesi ve bir ağda sunulan hizmetlere erişimin engellenmesini de içerebilmektedir.

Aslında siber saldırının geçmişi düşündüğümüzden daha eskiye dayanmaktadır. Bazı kaynaklarda 1982 yılında ABD tarafından Sovyetler Birliği'ndeki bir boru hattının sadece yazılım kullanılarak patlatılması ilk siber saldırı olayı olarak tanımlanmaktadır[2]. Daha sonraki yıllarda bilgisayar sistemleri ile bilgisayar ağlarının yaygınlaşması ve birçok şeyin bilgisayar destekli sistemlerle kontrol edilmesi, siber saldırı olanaklarını ve olaylarını artırmıştır. Geleneksel askeri harekattan[3] ve hatta terör eylemlerinden[4] daha ucuza mal olan ve kaynağının tespiti daha zor olan siber saldırılar devletler tarafından

1 T.C. Ulaştırma Denizcilik ve Haberleşme Bakanlığı, *Ulusal Siber Güvenlik Stratejisi (2016-2019)*, tarih yok.

2 Marco Roscini, *Cyber Operations and the Use of Force in International Law* (New York: Oxford University Press, 2014), 4.

3 Petr Hruza ve Jiri Cerny, "Cyberwarfare", *International Conference: The Knowledge-Based Organization* 23/1 (2017): 155-160

4 Gabriel Weimann, *"Cyberterrorism: How Real is the Threat"* (2004 Ara). (erişim 24.9.2021)

giderek daha fazla kullanılacaktır. Birçok ülkenin bu amaçla silahlı kuvvetler içerisinde birimler kurdukları bilinmektedir[5]. Sayısı ve şiddeti artan saldırılar karşısında bazı devletlerin de kendilerini savunma ihtiyacı ortaya çıkacak, bu askeri kuvvet kullanımına kadar gidebilecektir.

Gerçekleştiğinde silahlı saldırı kabul edilebilecek, daha önce silahlı çatışmalarda örnekleri görülen birçok eylem bugün siber ortam kullanılarak gerçekleştirilebilmektedir. Örneğin, bilgisayar ağları tarafından yönetilen bir elektrik şebekesinin uzaktan erişim ile devre dışı bırakılması, hatta aşırı yüklenmeye neden olunarak fiziki zarar verilmesi mümkündür. Bu, bir ağa bağlı olsun ya da olmasın bilgisayarlar ile kontrol edilen tüm sistemler için geçerlidir. Barajlar, ulaştırma sistemleri, sanayi tesisleri vb. sistemlerin yönetimindeki aksamalar büyük hasarlara ve can kaybına yol açabilir.

Diğer yandan tüm silah ve sensörlerin ağlar üzerinden komuta ve kontrol edildiği günümüz ağ merkezli savaş ortamında başkalarına ait savaş araçları ve silahların kontrolünün ele geçirilmesi, bunların imha edilmesi veya istenen hedeflere yönlendirilmesi de mümkündür. Özellikle insansız sistemler buna açıktır. Bilim kurgu gibi de görülebilecek bu eylemlerin hemen hepsi son dönemde yaşanmıştır. 2010 yılında Stuxnet adlı bilgisayar virüsü ile İran'ın Natanz nükleer tesisindeki santrifüjler zarar görmüş, nükleer program iki yıl geri gitmiştir[6]. 2013 yılında New York yakınlarındaki küçük bir barajın kontrolü siber saldırı ile ele geçirilmiş, baraj onarım nedeniyle boş olduğundan önemli bir olay yaşanmamıştır[7]. 2014 yılında Almanya'daki bir çelik fabrikasına yönelik siber saldırıda emniyet sistemleri devre dışı bırakılmış, çelik kazanları patlamış, şans eseri yaralanan olmamıştır[8]. 2015 yılında siber saldırı sonucu Ukrayna'daki enerji santrallerinin yaklaşık dörtte biri devre dışı kalmıştır[9]. Ayrıca 2011 yılında ABD ordusuna ait bir insansız hava aracı siber saldırı ile ele geçirilerek yere indirilmiş, Kırım üzerindeki bir ABD hava aracı siber saldırı ile önlenmiştir[10].

Bütün bu gelişmeler göstermektedir ki siber saldırı askeri bir araç olarak kuvvet kullanımında yerini almıştır. Dolayısıyla siber saldırılar ile kuvvet kullanma yasağına aykırı eylemlerin gerçekleşmesi mümkündür[11]. Bunun sonucunda da elbette meşru

5 Michael N. Schmitt, "Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework", *Columbia Journal of Transnational Law* 37 (1999): 898.

6 Yaakov Katz, *"Stuxnet virus set back Iran's nuclear program by 2 years"*, erişim 19 Nisan 2017, http://www.jpost.com/Iranian-Threat/News/Stuxnet-virus-set-back-Irans-nuclear-program-by-2-years.

7 Joseph Berger, *"A Dam, Small and Unsung, Is Caught Up in an Iranian Hacking Case"*, erişim: 11 Nisan 2017 https://www.nytimes.com/2016/03/26/nyregion/rye-brook-dam-caught-in-computer-hacking-case.html?_r=0.

8 BBC, *"Hack attack causes 'massive damage' at steel works"*, erişim: 19 Nisan 2017, http://www.bbc.com/news/technology-30575104.

9 Agy.

10 Isaac R. Porche, *"Cyberwarfare Goes Wireless"*, erişim: 20 Nisan 2017, https://www.usnews.com/opinion/blogs/world-report/2014/04/04/russia-hacks-a-us-drone-in-crimea-as-cyberwarfare-has-gone-wireless.

11 Sara Pangrazzi, *"Self-Defence Against Cyberattacks?: Digital and Kinetic Defence in Light of Article 51 UN-Charter"*, (2021), 12. Erişim: 25.02.2022. https://ict4peace.org/activities/new-

müdafaa hakkının kullanımı gündeme gelecek, getirilecektir. Bu çalışmada bir siber saldırın BM Şartı'nda meşru müdafaa için ön koşul olan "silahlı saldırı"yı oluşturup oluşturmayacağı incelenecektir.

Çalışma sadece silahlı saldırı ile siber saldırının karşılaştırılması ile sınırlandırılmıştır. Siber saldırıya karşı alınacak önlemlerin meşru müdafaa hakkının orantılılık, gereklilik, aciliyet gibi diğer unsurlarına uygunluğu irdelenmeyecektir. Keza devlet dışı aktörlere karşı meşru müdafaanın uygulanabilirliği ile siber saldırıların kaynağının belirlenmesi gibi sorunlar tartışılmayacaktır.

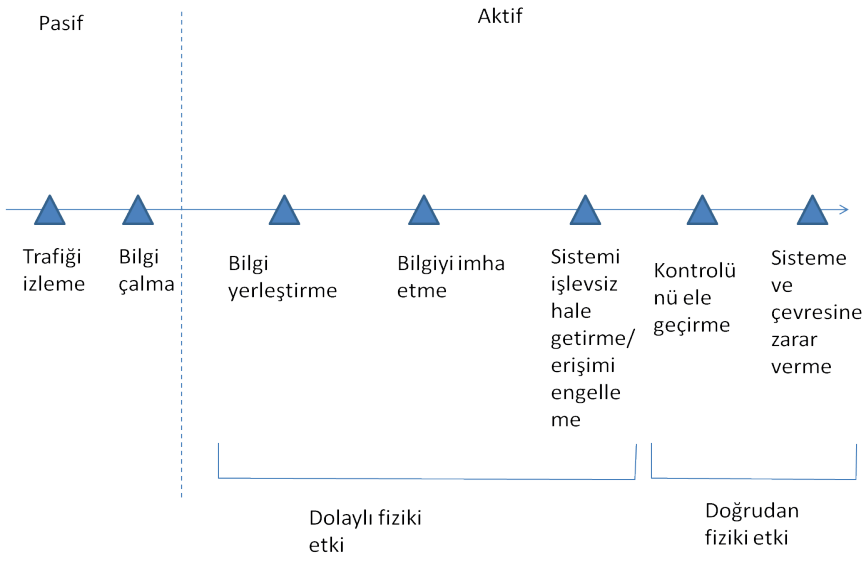
## 1. Siber Savaş: Ortam, Silahlar ve Yöntemler

Elektroniğin gelişimi ile birlikte doğal olarak askeri alanda kullanımı da artmıştır. Başlangıçta sadece düşmanın tespit edilmesi için kullanılan elektromanyetik dalgalar zamanla karşı tarafa zarar vermek için de kullanılır hale gelmiştir. Elektronik savaş olarak adlandırılan bu yöntemle, elektromanyetik dalgaların yönlendirilmesiyle düşman sistemlerin yanıltılması, kör edilmesi ve fiziksel zarar verilmesi mümkün hale gelmiştir. Hatta zaman içerisinde sadece elektronik cihazlar değil insanlar üzerinde de etkili olan cihazlar geliştirilmiştir.

Birçok sistemin bilgisayarlar yoluyla uzaktan kontrol edilmesi, bunları başkalarının da kontrolüne açık hale getirmiştir. Bunun sonucunda elektronik savaş, bilgi savaşı haline dönüşerek siber uzaya genişlemiştir. Bu genişleme sadece mekânsal olarak değil, yetenek bakımından da gerçekleşmiştir. Tamamen izole bir sistem kurulmadığı takdirde (ki bunun çok mümkün olmadığı Stuxnet saldırısında görülmüştür) sizin tarafınızdan erişilebilen her türlü sisteme düşmanın da erişimi mümkündür. Bunun içindir ki aralarında Türkiye'nin de bulunduğu birçok ülke silahlı kuvvetlerine bağlı siber güvenlik birimleri kurmuştur. Bunların bazıları sadece korunma amaçlıyken, bazılarının saldırı yeteneği de geliştirdiği bilinmektedir.

Siber silahları, bilinen silahlarla benzetim yoluyla açıklamak mümkündür. Havada uçarak hedefine ulaşan bir balistik füze, kabaca bir taşıyıcı ve harp yükünü içeren başlıktan oluşur. Asıl kinetik etkiyi yaratan başlıktır. Hiçbir özelliği olmayan bir başlığın yaratacağı etki mancınıkla atacağınız bir kayanın çarpmasından çok farklı değildir. Bir siber silah ise hedefine ulaşmak için siber uzayı kullanır. Bu ortamda menzil sonsuzdur. Taşıyıcı, dosyalar veya veri paketleri; faydalı yük ise istenen etkiyi yaratmak üzere hazırlanmış bir yazılımdır. Siber silahlarla yapılabilecekler ise veri trafiğinin izlenmesinden kasten zarar vermeye kadar geniş bir yelpazeye yayılmaktadır. Siber savaşın ve siber saldırının anlaşılabilmesi için öncelikle siber ortam ve silahların tanınması gerektiğinden bu kısımda kısaca siber ortam, zararlı yazılımlar ve bunların saldırı yöntemleri hakkında bilgi verilecektir.

publication-self-defence-against-cyberattacks-digital-and-kinetic-defence-in-light-of-article-51-un-charter/




**Şekil 1. Siber Saldırı Hedefleri**

### 1.1. Siber Ortam

Siber ortam her ne kadar mantıksal bir uzay olarak bilinse de fiziki ve mantıksal beş katman içeren bir yapıdır[12]. En alttaki coğrafi katman ağdaki unsurların fiziksel konumlarıdır. Siber uzayın kendisi fiziksel olmasa da onu oluşturan donanım bir yerlerde konuşlanmıştır. Bunun üzerindeki fiziksel ağ katmanı, ağı oluşturan donanım ve altyapıdır. Kablolar, bilgisayarlar, yönlendiriciler, sunucular bu katmanı oluşturur. Bu iki fiziksel katman üzerinde mantıksal ağ katmanı yer alır. Bu, bilginin taşındığı sanal uzayıdır. Mantıksal ağ katmanı kullanıcılara siber kişi katmanı yoluyla bağlanır. Bu katmanda kişiler e-posta adresleri, IP adresi, cep telefonu numarası gibi ayrıntılarla tanımlanır. En üstte ise insan katmanı bulunur. Bu katman ağı kullanan gerçek insanlardan oluşur.

Siber ortamın mantıksal katmanlarında sınırlar ve sabit yollar yoktur. Veri parçalara ayrılarak mümkün olan yollardan hedefe ulaşır ve burada tekrar birleştirilir. Gönderici ve hedef noktalar arasındaki denetimsizlik; verinin izlenmesi, çalınması ve değiştirilmesini mümkün kılar. Bu nedenle uzaktan erişilebilen sistemler her zaman için yetkisiz müdahale olasılığı ile karşı karşıyadır.

### 1.2. Silahlar

Siber ortamda silahlar daha önce belirtildiği gibi istenen komutları yerine getiren yazılımlardan ibarettir. Bu yazılımlar çalışma ve çoğalma yollarına göre farklı adlarla

12 Paul Rosenzweig, *Cyber Warfare* (Praeger, 2013), 19.

adlandırılabilir. Farklı türlerin çalışma ve yayılma yöntemleri ayrı ayrı kullanılabildiği gibi kombine bir şekilde de kullanılabilirler.

Bilgisayar virüsleri, kullanıcının izin veya bilgisi dışında bilgisayar veya sistemin çalışma şeklini değiştiren, kendisini başka bir program içerisine gizleyen küçük programlardır[13]. Virüsler kendilerini bir başka dosya içerisine kopyalayarak onun bir parçası olurlar. Bu dosya çalıştırıldığında bilgisayara zarar verebilir ve kendini başka dosyalara kopyalayabilir. Virüslerin iki özelliği vardır: kendiliğinden çalışırlar ve kendilerini kopyalarlar. Veriye zarar vermekten sistemi çökertmeye kadar farklı amaçlar için kullanılabilirler.

Solucanlar, sistemden sisteme, (virüslerin aksine) kendilerini taşıyacak bir program kullanmaksızın kopyalayan programlardır[14]. Yayılmak için işletim sisteminin zafiyetlerinden yararlanırlar. Çoğalması için ilave eyleme ihtiyaç duymaması ağ boyunca süratle yayılmasına olanak tanır ve bant genişliğinin tüketimiyle yıkıcı etkiye yol açar.

Truva atları, kullanılmak istenen programlar gibi görünen ama aslında zararlı olan yazılımlardır. Virüslerden farkı kendilerini kopyalamamasıdır. Truva atları çalıştırıldığında verinin kaybına veya çalınmasına ya da uzaktan yetkisiz erişime olanak veren kapılar açılmasına yol açabilir[15]. Bir truva atının bulaşması için kullanıcının bu programı kendisinin kopyalaması ve çalıştırması gerekir (örneğin bir e-posta ekini açarak).

Botlar sistemin diğer unsurları ile otomatik olarak etkileşme giren zararlı yazılımdır. Normalde bir insan tarafından gerçekleştirilecek işlemleri otomatik yaparlar. Aktif olduğunda merkez ile iletişime geçer. Botlar tarafından oluşturulan ağlar özellikle uzaktan kontrollü DDoS[16] saldırıları için kullanılırlar.

Zararlı yazılım kategorisinde bunların haricinde de fidye yazılımları, reklam yazılımları, casus yazılımlar, rootkit'ler gibi yazılım türleri olmakla birlikte çalışmanın amacı dışında olduğundan bunlara ilişkin açıklamaya gerek görülmemiştir.

### 1.3. Saldırı Yöntemleri

Siber saldırılar, bir bilgisayar ağının ya da ağdaki verinin bütünlüğüne, gizliliğine ya da erişilebilirliğine yöneltilmektedir. Saldırının amacına, kullandığı yöntem ve araçlara göre farlı sınıflandırmalar mevcuttur. Burada temel yöntemleri göstermesi bakımında Larson ve Cockcroft'un dörtlü sınıflandırması[17] tercih edilmiştir. Bu saldırı yöntemleri

13 Symantec Corporation, *"What is the difference between viruses, worms, and Trojans?"*, erişim: 3 Haziran 2017. https://support.symantec.com/en_US/article.TECH98539.html.

14 Norton, *"What is a computer worm, and how does it work?"*, erişim: 25 Eylül 2021, https://us.norton.com/internetsecurity-malware-what-is-a-computer-worm.html.

15 Eset, *"Truva Atı"*, erişim: 25 Eylül 2021, https://www.eset.com/tr/trojan-horse/.

16 *Distributed Denial of Service:* Bir ağ hizmetine farklı yerlerden çok sayıda istek göndererek, sistemin gerçek kullanıcılara hizmet vermesini engellemeyi amaçlayan saldırı türü.

17 Robert E. Larson ve Lance Cockcroft, *CCSP: Cisco Certified Security Professional Certification* (McGRaw-Hill, 2003).

ayrı ayrı, sırayla veya kombine bir şekilde kullanılabilir.

Keşif saldırıları yetkisiz bir kullanıcının ağ ile ilgili bilgi almak için yaptığı saldırılardır. Bu saldırılarda elde edilen bilgi sonraki daha ciddi saldırılar için kullanılabilir.

Erişim saldırıları ağın kaynaklarına erişimi ifade eden genel bir terimdir. Ağa erişim sağlandıktan sonra gizli bilgiler çalınabilir ya da veriye zarar verilebilir.

Erişimin engellenmesi (Denial of Service-DoS) saldırılarında amaç normal kullanıcıların bir bilgisayar veya ağ tarafından sağlanan hizmetlere erişiminin engellenmesidir. Bunu sağlamak için ağ faydasız trafik ile meşgul edilerek sistem doyuma ulaştırılır ve normal taleplere cevap veremez hale gelir. Erişimin engellenmesi saldırıları, başka (masum) bilgisayarlara yerleştirilecek ajanlar (bot) vasıtasıyla kurulan bir sanal ağ tarafından (botnet) yürütülebilir.

Veri işleme saldırılarında, gönderen ve alan sistemler arasına giren bir kişi tarafından üretilen sahte veri, gönderen sistemden geliyormuş gibi alıcıya gönderilir. Bu yöntemle bilgisayar ile bu bilgisayar tarafından kontrol edilen sistem arasına girilerek sistemin istenen şekilde kontrol edilmesi veya sistemin bilgisayarın kontrolünden çıkması sağlanabilir.

## 2. BM Sistemi'nde Meşru Müdafaa, Silahlı Saldırı ve Siber Saldırı

### 2.1. Kuvvet Kullanma Yasağı ve Meşru Müdafaa

II. Dünya Savaşı'nın neden olduğu yıkım ve büyük acılar sonucunda dünya genelinde barış ve güvenliği korumak, barışın bozulmasına karşı ortak önlemler almak ve uyuşmazlıkların barışçı yollarla çözülmesi amacıyla kurulan Birleşmiş Milletler örgütüyle birlikte uluslararası ilişkilerde yeni bir sistem oluşturulmuştur. Bu yeni sistemde devletlerin birbirleriyle olan ilişkilerinde kuvvete başvurmaları yasaklanmıştır. Birleşmiş Milletler öncesinde de kuvvet kullanımını sınırlama ve yasaklama girişimleri olmakla birlikte, bu girişimlerden istenen sonuç alınamamış, II Dünya Savaşı engellenememiştir.

BM Şartı'nın 2. maddesinde yer alan kuvvet kullanma yasağının artık andlaşma hükmünün ötesinde bir örf adet hukuku kuralı haline geldiği ve tüm devletler için bağlayıcı olduğu kabul edilmektedir[18]. Buna göre: "*Tüm üyeler, uluslararası ilişkilerinde gerek herhangi bir başka devletin toprak bütünlüğüne ya da siyasal bağımsızlığına karşı, gerek Birleşmiş Milletler'in Amaçları ile bağdaşmayacak herhangi bir biçimde kuvvet kullanma tehdidine ya da kuvvet kullanılmasına başvurmaktan kaçınırlar.*"[19]. Şartın bu hükmü ile yasaklanan askeri kuvvet kullanımıdır. Ekonomik ve siyasi içerikli zorlama önlemlerinin de bu yasak kapsamında dâhil edilmesine yönelik öneriler açıkça reddedilmiştir[20].

18 Malcolm N. Shaw, *International Law* (Cambridge: Cambridge University Press, 2008), 1123.

19 Birleşmiş Milletler Andlaşması (1945), erişim: 1 Ocak 2017, https://www.tbmm.gov.tr/komisyon/insanhaklari/pdf01/3-30.pdf.

20 Birleşmiş Milletler, Summary Report of the Eleventh Meeting of the Committee I/1, *Documents of the United Nations Conference on the International Organisation*.(San Fransisco, 5 Haziran

Kuvvet kullanma ve kullanma tehdidi yasağına rağmen barış ve güvenliğin bozulması halinde birlikte hareket edilmesini hedefleyen kolektif güvenlik sisteminde, kuvvet kullanma yetkisi (barışın bozulması halinde) Birleşmiş Milletlerin yürütme organı statüsündeki Güvenlik Konseyine verilmiştir. Güvenlik Konseyine tanınan bu yetki dışında, BM Şartı'nda kuvvet kullanma yasağının tek bir istisnası vardır: meşru müdafaa. Meşru müdafaa hakkı, Şart'ın 51. maddesinde düzenlenmiştir. Buna göre:

> *"Bu Andlaşma'nın hiçbir hükmü, Birleşmiş Milletler üyelerinden birinin silahlı bir saldırıya hedef olması halinde, Güvenlik Konseyi uluslararası barış ve güvenliğin korunması için gerekli önlemleri alıncaya dek, bu üyenin doğal olan bireysel ya da ortak meşru savunma hakkına halel getirmez. Üyelerin bu meşru savunma hakkını kullanırken aldıkları önlemler hemen Güvenlik Konseyi'ne bildirilir ve Konsey'in işbu Andlaşma gereğince uluslararası barış ve güvenliğin korunması ya da yeniden kurulması için gerekli göreceği biçimde her an hareket etme yetki ve görevini hiçbir biçimde etkilemez."*

Birleşmiş Milletler Şartı'nda meşru müdafaa kısıtlı olarak ele alınmış, gereklilik, orantılılık gibi diğer unsurlara yer verilmemiştir. Bunun sonucu olarak da "51. maddede yer alan hakkın metinde belirtildiği şekilde tüketici olduğu" ve "örf adet hukukunda ayrıca bir meşru müdafaa hakkının yer aldığı" şeklinde iki ayrı görüş ortaya çıkmıştır[21]. Uluslararası Adalet Divanı (UAD) bu konu ile ilgili yorumunda 51. maddenin ancak meşru müdafaa hakkının örf adet hukukundaki varlığı ile anlamlı olacağını, bununla birlikte 51. madde hükmünün örf adet hukukunu kapsadığını söylemenin mümkün görülmediğini, dolayısıyla meşru müdafaa hakkının örf adet hukuku ve andlaşmalarda eş zamanlı olarak yürürlükte olan bir kural olduğunu belirtmiştir[22].

### 2.2. Silahlı Saldırı

51. madde kapsamında meşru müdafaa hakkı, kuvvet kullanma yasağının oldukça sınırlı bir istisnasını oluşturmaktadır. Buna göre öncelikle üye devletin bir silahlı saldırıya (*armed attack*) uğramış olması gerekmektedir. Ancak silahlı saldırının ne olduğu ne BM Şartı'nda ne de başkaca bir uluslararası andlaşmada açıkça tanımlanmamıştır. Bu nedenle kuvvet kullanımının hangi şartlarda silahlı saldırı oluşturduğunun tespiti için BM organlarının kararlarına bakmak gerekmektedir. BM Genel Kurulu tarafından 1970 yılında 2625 sayılı karar ile kabul edilen Devletler Arasında BM Şartı'na Uygun Şekilde Dostane Münasebetler Kurma ve İşbirliği Yapmaya Dair Milletler Arası Hukuk İlkeleri Hakkında Bildiri'de kuvvet kullanma yasağı ve müdahale etmeme ilkesi ile ilgili hususlara yer verilmiştir[23]. Bununla birlikte saldırının suç olduğu belirtilen bildiride saldırı ya da silahlı saldırının tanımı yapılmamıştır.

---

1945), 331-335.

21 Malcolm N. Shaw, age, 1132.

22 Uluslararası Adalet Divanı, Case Concerning Military and Paramilitary Activities in and Against Nicaragua. Merits, Judgement (27 Haziran 1986), 84.

23 BM Genel Kurulu, *Devletler Arasında BM Şartı'na Uygun Şekilde Dostane Münasebetler Kurma ve İşbirliği Yapmaya Dair Milletler Arası Hukuk İlkeleri Hakkında Bildiri* (1970) erişim: 29 Mayıs 2017, http://www.unicankara.org.tr/doc_pdf/metin_ant1.pdf.

BM Genel Kurulu tarafından alınan diğer bir kararda ise silahlı saldırıya kıyasla daha geniş bir kavram olan[24] saldırının (*aggression*) tanımı yapılmıştır. 1974 yılında alınan 3314 sayılı kararda saldırı: *"Bir devletin diğer bir devletin egemenliğine, ülke bütünlüğüne veya siyasi bağımsızlığına karşı veya Birleşmiş Milletler Andlaşması ile bağdaşmayan diğer herhangi bir tarzda silahlı kuvvet kullanması" olarak tanımlanmıştır"*[25]. Kararda kuvvetin ilk önce kullanımının bir saldırının prima facie kanıtını teşkil edeceği belirtildikten sonra saldırı fiili niteliği taşıyacak bazı eylemler tüketici olmayacak şekilde sayılmıştır. Bu eylemler, bir devletin başka bir devlete yönelik silahlı kuvvetler ile yapacağı eylemleri kapsamaktadır. İstisna olarak silahlı kuvvet kullanımına varan ölçekte silahlı çete ve grupların (devlet tarafından/devlet adına) gönderilmesi de listede yer almıştır. UAD, Nikaragua Davası Kararı'nda silahlı çeteler gönderilmesinin eylemin büyüklüğüne göre silahlı saldırı ya da sadece bir sınır olayı olabileceğini belirtmiş ancak silahlı çete veya gruplara silah, lojistik veya diğer destek sağlanmasını saldırı olarak görmemiş; eylemlerinin bir devlete atfedilebilmesi için ilgili devletin, örgütün eylemleri üzerinde etkin kontrolü olması şartını aramıştır[26]. 3314 sayılı kararda silahlı saldırının tanımının yapılmadığı görülmektedir.

BM Güvenlik Konseyinin ise kararlarında bir tekdüzelik bulunmamaktadır. 1950 yılında 82, 83 ve 84 sayılı kararlarda Kuzey Kore tarafından Güney'e yapılan saldırı "silahlı saldırı" (*armed attack*) olarak tanımlanmış[27], üye devletlerden saldırının püskürtülmesi ve barışın tekrar sağlanması için Kore Cumhuriyeti'ne yardım edilmesi talep edilmiştir[28]. 1981 yılında İsrail tarafından Irak'taki Osirak nükleer santralinin vurulması üzerine çıkartılan 487 sayılı kararda İsrail'in eylemi askeri saldırı (*military attack*) olarak tanımlanmıştır[29]. Aynı olayı BM Genel Kurulu silahlı saldırı (*armed aggression*) ve saldırı kabul etmiştir. Bu olayda İsrail'in eylemine karşı meşru müdafaa hakkından bahsedilmemiştir. Güvenlik Konseyince 1990 yılında Irak'ın Kuveyt'i işgaline karşı çıkartılan 661 sayılı kararda Irak'ın eylemi silahlı saldırı (*armed attack*) olarak nitelenmiş, bireysel ve kolektif meşru müdafaa hakkının tanındığı belirtilmiştir[30]. 1993 yılında Bosna'daki duruma ilişkin çıkan 819 sayılı kararda ise Bosnalı Sırp paramiliter grupların silahlı saldırılarını (armed attack) sonlandırması, Yugoslavya Cumhuriyeti'nin bunlara silah yardımı yapmaya son vermesi talep edilmiştir[31]. Bu kararda meşru müdafaa hakkına herhangi bir atıf bulunmamaktadır.

24 Yoram *Dinstein,* "Computer Network Attacks and Self-Defense"*, International Law Studies* 76 (2002): 100

25 Birleşmiş Milletler Genel Kurulu. *"Definition of Aggression* (A/RES/29/3314)", erişim: 5 Ocak 2017, http://www.un-documents.net/a29r3314.htm.

26 Uluslararası Adalet Divanı, *"Case Concerning Military and Paramilitary Activities in and Against Nicaragua. Merits, Judgement"* (1986), 55, erişim: 06 Ocak 2017, http://www.icj-cij.org/docket/files/70/6503.pdf.

27 "Having determined that the armed attack upon the Republic of Korea by forces from North Korea constitutes breach of the peace,…"

28 Birleşmiş Milletler Güvenlik Konseyi (BMGK), "84(1950). *Resolution of 7 July 1950*", erişim: 26 Eylül 2021, https://digitallibrary.un.org/record/112027.

29 BMGK, "Resolution 487 (1981) / *Adopted by the Security Council at its 2288th Meeting, on 19 June 1981*. " erişim: 26 Eylül 2021, https://digitallibrary.un.org/record/22225.

30 BMGK, "Resolution 661 (1990) / *Adopted by the Security Council at its 2933rd Meeting, on 6 August 1990* ", erişim: 26 Eylül 2021, https://digitallibrary.un.org/record/94221?ln=en.

31 BMGK, "Resolution 819 (1993) / *Adopted by the Security Council at its 3199th Meeting, on 16*

Daha yakın dönemde iki BMGK kararında meşru müdafaa hakkı tanınmıştır. Ancak bunlar devletlerin eylemlerine karşı değil, devlet dışı aktörlerin eylemlerine karşı çıkartılmış kararlardır. 11 Eylül 2001 saldırılarından sonra çıkartılan 1368[32] ve 1373[33] sayılı kararda terör saldırılarının uluslararası barış ve güvenliğe tehlike oluşturduğu belirtilmiş, BM Şartı'na dayalı (doğal) bireysel ve kolektif meşru müdafaa hakkı tanınmış, buna karşın bir silahlı saldırının varlığından söz edilmemiştir. Yine teröre karşı, Paris'te 13 Kasım 2016 akşamı meydana gelen terör saldırılarının hemen ardından Birleşmiş Milletler Güvenlik Konseyi tarafından Fransa'nın önerisiyle 2249 sayılı karar alınmış, Karar'ın 5. maddesinde üye devletlerden olanağı olanların, uluslararası hukuka uygun olarak, Irak ve Suriye'de DEAŞ'ın kontrolü altındaki bölgede terörist eylemlerin engellenmesi ve bastırılması için "gereken tüm önlemlerin alınması" ve Irak ve Suriye'nin önemli bir kısmında teröristlerin oluşturdukları güvenli bölgenin ortadan kaldırılması talep edilmiştir[34]. 2249 sayılı karar incelendiğinde BM Şartı'nın 7. bölümü anılmadığı gibi, işlem paragrafında "gereken tüm önlemlerin alınması" kararlaştırmak veya yetkilendirmek yerine, talep edilmektedir. Bu durum çoğunlukla Karar'ın doğrudan kuvvet kullanımı yetkisini vermediği[35], bununla birlikte açıkça kuvvet kullanımı yetkisini vermeyen Güvenlik Konseyinin zımnen de olsa (uluslararası hukuka uygun olarak) kuvvet kullanımını kabul ettiği şeklinde yorumlanmaktadır. Güvenlik Konseyinde yapılan oylama sonrasında bazı üyelerin yaptığı açıklamalar da bunu doğrular mahiyettedir. Hiçbir üye kuvvet kullanımına izin verildiği yönünde bir yorumda bulunmamış, kararın önerge sahibi Fransa dâhil meşru müdafaa hakkına atıfta bulunulmuştur[36]. Fransız temsilcisi tarafından yapılan konuşmada 13 Kasım'daki olayın Fransa'ya karşı bir silahlı saldırı olduğu, daha önce Güvenlik Konseyine bildirdikleri ve kolektif meşru müdafaa kapsamında yürüttükleri askeri faaliyetlerin artık BM Şartı'nın 51. maddesine uygun olarak bireysel meşru müdafaa kapsamında da gerekçelendirilebileceği ifade edilmiştir[37]. Konseyin diğer üyeleri de benzer açıklamalar yapmıştır. Bu kararda da (karar metninde) silahlı saldırı zikredilmemiştir.

*April 1993*.", erişim: 26 Eylül 2021, https://digitallibrary.un.org/record/164939?ln=en.

32 BMGK, "Resolution 1368 (2001) / *Adopted by the Security Council at its 4370th Meeting, on 12 September 2001*", erişim: 26 Eylül 2021 , https://digitallibrary.un.org/record/448051?ln=en.

33 BMGK, "Resolution 1373 (2001) / *Adopted by the Security Council at its 4385th Meeting, on 28 September 2001*", erişim: 26 Eylül 2021 , https://digitallibrary.un.org/record/449020?ln=en.

34 BMGK, "Resolution 2249 (2015) / *Adopted by the Security Council at its 7565th Meeting, on 20 November 2015*", Erişim: 26 Eylül 2021, https://digitallibrary.un.org/record/811987?ln=en.

35 Dapo Akande ve Marko Milanoviç, "*The Constructive Ambiguity of the Security Council's ISIS Resolution.* 21 Kasım 2015" erişim: 3 Ocak 2017, http://www.ejiltalk.org/the-constructive-ambiguity-of-the-security-councils-isis-resolution/; Ashley Deeks, *"Threading the Needle in Security Council Resolution 2249*. 23 Kasım 2015." Erişim: 4 Ocak 2017, https://www.lawfareblog.com/threading-needle-security-council-resolution-2249; Sherif Elgebeily, *"HKU Legal Scholarship Blog*. 29 Şubat 2016." Erişim: 4 Ocak 2017, http://researchblog.law.hku.hk/2016/02/sherif-elgebeily-comments-on-un.html; Mahmood Hasan, *"Opinion: Ambigious UN Resolution Adds to Complex and Dangerous Situation*. 30 Kasım 2015", erişim: 4 Ocak 2017, http://www.asianews.network/content/opinion-ambiguous-un-resolution-adds-complex-and-dangerous-situation-4572.

36 BMGK, *"Meeting Records S/PV.7565."* erişim: 4 Ocak 2017, http://www.un.org/en/ga/search/view_doc.asp?symbol=S/PV.7565.

37 Agy, 2.

Birleşmiş Milletlerin bir diğer organı olan Uluslararası Adalet Divanı, silahlı saldırı ve meşru müdafaa konusunda daha açıklayıcı kararlar almıştır. 1986 tarihli Nikaragua kararında kuvvet kullanımının, silahlı saldırı oluşturan en ağır biçimi ile daha az ağırlıkta olanlar arasında bir ayrıma gidilmesi gerektiğini belirtmiş, daha az ağırlıkta olan kuvvet kullanımı ile ilgili olarak Genel Kurulun 2625 sayılı kararına[38] atıf yapılmıştır[39]. Silahlı saldırı ise açıkça tanımlanmamış, silahlı saldırıyı oluşturan eylemlerin doğası hakkında genel bir uzlaşı olmadığı belirtilmiştir. Divan, Genel Kurulun 3314 sayılı kararına atıfla silahlı çetelerin eylemlerinin de silahlı saldırıyı oluşturabileceğini kabul etmiş, ancak bunların sınır olaylarından ayrılması için "boyut ve etki" kıstasını getirmiştir. Bundan sonra eylemin silahlı saldırı sayılması için boyut ve etkilerinin ne olması gerektiği tartışılmadan, gönderen devletin silahlı gruplara olan katkısının seviyesi ele alınmıştır. Neticede eylemin silahlı saldırı oluşturmadığı kararı bu kıstas üzerinden verilmiştir.

Uluslararası Adalet Divanının 2003 tarihli Petrol Platformları kararında meşru müdafaa ve silahlı saldırı bir kez daha gündeme gelmiştir. ABD, İran'a ait petrol platformlarına yönelik eylemlerini meşru müdafaa hakkına dayandırmış, İran'ın Amerikan gemilerine yönelik saldırılarını silahlı saldırı olarak tanımlamıştır[40]. Divan Nikaragua kararına atıfla kuvvet kullanımının en ağır biçimleri ile daha az ağır olanları arasında ayrım yapılması gerektiğini ve meşru müdafaa hakkının kullanılması için bir silahlı saldığının mağduru olunması gerektiğini belirtmiştir. Sonuçta Divan toplu olarak bile alınsa İran'ın eylemlerinin (İran'a atfedilebilirliği de sorunludur) silahlı saldırı seviyesinde olmadığına hükmetmiştir. Burada dikkat çekici olan kararın eylemlerin boyutu üzerinden değil, bölgede devam eden savaş durumu ve ABD'nin İran'a atfettiği eylemlerin Divanın ABD'ye yönelik bir kasıt içermediği kanaatine istinaden verilmiş olmasıdır. Zira Divan, bir geminin mayınlanmasının silahlı saldırı oluşturabileceğini göz ardı etmediğini, bununla birlikte geminin mayına çarpmasında İran'ın sorumluluğuna dair yeterli kanıt olmadığından silahlı saldırının oluşmadığına karar verdiğini belirtmiştir[41]. Bu kararda da Divan neyin silahlı saldırı olduğunu değil, neyin silahlı saldırı olmadığını açıklamayı tercih etmiştir.

Silahlı saldırıya ilişkin burada yer vereceğimiz son karar Nükleer Silahlar Danışma Görüşüdür. Uluslararası Adalet Divanı, nükleer silah kullanımına başvurmanın BM Şartı kapsamında değerlendirmesini yaparken, Şart'ta kuvvet kullanmanın hukuka uygun olduğu hallerin 51. madde kapsamında meşru müdafaa hali ve 42. madde kapsamında Güvenlik Konseyinin alacağı önlemler olduğunu belirtmiş, bu hükümlerin kullanılan silahtan bağımsız olarak tüm kuvvet kullanım şekilleri için geçerli olduğunu ifade etmiştir[42].

38 Bkz. d.n. 22.
39 Uluslararası Adalet Divanı, Case Concerning Military…, 91.
40 UAD, *"Case Concerning Oil Platforms, 6 Kasım 2003"*, 24, erişim: 15 Mart 2017, http://www.icj-cij.org/docket/?sum=634&code=op&p1=3&p2=3&case=90&p3=5.
41 Agk, 64
42 UAD, *"Legality of the Threat or Use of Nuclear Weapons, 8 Temmuz 1996."*, 22, erişim: 24 Mart 2017, http://www.icj-cij.org/docket/index.php?p1=3&p2=4&k=e1&p3=4&case=95.

Buraya kadar incelenen kararlardan meşru müdafaa hakkının kullanımı için ön şart olan silahlı saldırının uluslararası hukukta tanımının yapılmadığı anlaşılmaktadır. Genellikle neyin silahlı saldırı olacağından çok, somut olaylar üzerinden neyin silahlı saldırıyı oluşturduğu veya oluşturmadığının tespiti tercih edilmiştir. Bununla birlikte bir olayın silahlı saldırı olup olmadığına karar verilirken dikkate alınacak ilkeler konusunda ipuçları verilmiştir. Birincisi silahlı saldırı kuvvet kullanımının en ağır biçimidir. Kuvvet kullanımının silahlı saldırı sayılması için belirli bir boyuta ve etkiye sahip olması gerekmektedir. Buna karşın tek bir geminin mayınlanması da silahlı saldırıyı oluşturabilecektir. Son olarak silahlı saldırı seviyesine ulaşan kuvvet kullanımında, kullanılan silahın türünün önemi yoktur. Bu ilkeler sonraki kısımda siber saldırıya yönelik değerlendirmelerimizde yardımcı olacaktır.

### 2.3. Siber Saldırının Silahlı Saldırı Bağlamında Değerlendirilmesi

Bir siber saldırının silahlı saldırı olup olmadığını değerlendirmeden önce siber saldırının ne olduğunu tanımlamak gerekecektir. Çalışmamıza konu siber saldırılara yönelik bir uluslararası hukuk metni olmadığından genel kabul gömüş bir tanımdan söz etmek mümkün değildir. Doktrinde ve devletlerin uygulamalarında da bir yeknesaklık bulunmamaktadır. Yapılan tanımların ne kadar farklı olduğunu göstermek bakımından burada bazı örneklere yer verilecektir.

Basit tanımlara Avusturya'nın tanımını gösterebiliriz. Avusturya'nın Siber Güvenlik Stratejisi'nde siber saldırı *"siber uzayda bilişim teknolojileri yoluyla bir veya birkaç bilişim sistemine yönelik saldırı"* olarak tanımlanmaktadır[43]. Bu tanıma göre siber saldırının amacı bilgi sistem güvenliğini kısmen veya tamamen ortadan kaldırmaktır.

Diğer uçta ise çok kapsamlı tanımlar bulunmaktadır. Örneğin Litvanya'nın Elektronik Bilgi Güvenliği Geliştirme Programı'nda siber saldırı (olay başlığı altında)

> *"Bir bilgi sistemi veya elektronik iletişim ağına yetkisiz erişime; bir bilgi sistemi veya elektronik iletişim ağının işleyişini durdurma veya değiştirmeye (kontrolünü ele geçirme dâhil); elektronik bilginin imhası, zarar görmesi, silinmesi veya değiştirilmesine; elektronik bilginin kullanılma ihtimalinin ortadan kaldırılması veya kısıtlanmasına, aynı zamanda kamuya açık olmayan bilgilerin ele geçirilmesi, yayınlanması, dağıtılması veya yetkisiz kişilerce başka şekilde kullanılmasına neden olan veya olma ihtimali olan bir olay, eylem veya kusur"*

olarak tanımlanmaktadır[44].

43 Avusturya Cumhuriyeti, "*Austrian Cyber Security Strategy*. (2013)", erişim: 31 Mayıs 2017, https://www.bka.gv.at/DocView.axd?CobId=50999.

44 Litvanya Cumhuriyeti Hükümeti, *"Resolution 796 on the Approval of the Programme for the Development of Electronic Information Security for 2011-2019.* (29 Haziran 2011)", erişim: 1 Haziran 2017, http://www.ird.lt/doc/teises_aktai_en/EIS(KS)PP_796_2011-06-29_EN_PATAIS.pdf.

NATO ise daha kapsayıcı ancak genel bir tanımı tercih etmiştir. Terim ve Tanımlar Sözlüğünde[45] *"Bilgisayar ağı saldırısı" girdisi altında "bir bilgisayar veya bilgisayar ağındaki bilginin ya da bilgisayarın/bilgisayar ağının kendisinin bozulması, erişimin engellenmesi, aşındırılması veya imha edilmesi içi girişilen eylem"* olarak tanımlanmış, bilgisayar ağı saldırısının bir siber saldırı türü olduğu belirtilmiştir.

Tanımları daha da çeşitlendirmek mümkündür[46]. Bu çalışmanın amaçları bakımından ele alınan siber saldırılar Şekil 1'de verilen çizelgenin en sonundaki, fiziki olarak insan ve makinelere zarar veren saldırılar olduğundan, Estonya'da bulunan NATO Siber Savunma İş Birliği Mükemmeliyet Merkezinin (CCDCOE) tanımını kullanmak daha uygun olacaktır. Merkez tarafından 2008 yılında oluşturulan uluslararası uzmanlar grubu tarafından hazırlanan Tallinn Siber Savaşa Uygulanabilecek Uluslararası Hukuk El Kitabı'nda (kısaca Tallinn El Kitabı) siber saldırı: *"saldırı ya da savunma amacıyla yapılmış olsun, insanların ölmesi veya yaralanmasına ya da nesnelerin imha edilmesine yol açması beklenen siber harekâtlar"* olarak tanımlanmıştır[47]. Siber saldırının bir silahlı saldırı oluşturup oluşturmayacağı bu tanım üzerinden irdelenecektir.

1945 yılında BM Şartı hazırlanırken kuvvet kullanma yasağı kapsamında öngörülen kuvvetin, dönemin şartları itibarı ile düzenli askeri kuvvetlerce sınırın aşılarak doğrudan saldırıda bulunması olduğu, bu kapsamda kullanılacak silahların kinetik etkileri olan silahlar olduğu açıktır[48]. Bununla birlikte gelişen teknoloji karşısında gerek doktrinde gerekse Uluslararası Adalet Divanı kararlarında kuvvet kullanımı yasağının geniş yorumlandığı görülmektedir. 1970'lere gelindiğinde BM Genel Kurulunun kararıyla düzenli ordulara ek olarak silahlı örgütlerin desteklenmesi de kuvvet kullanma yasağı kapsamına alınmıştır. 1996 yılında ise Uluslararası Adalet Divanı Nükleer Silahlar Danışma Kararında kuvvet kullanma yasağı bakımından silahların ayırt edilmeyeceğine hükmetmiştir. Bütün bunlar göstermektedir ki kuvvet kullanma yasağı, genel bir yasak olarak ortaya çıkan yeni durumları da içerecek şekilde genişlemektedir.

Diğer yandan silah olarak kullanımı akla gelmeyecek nesnelerle gerçekleştirilecek eylemlerin sonuçlarına bakarak silahlı saldırı seviyesinde olayların ortaya çıkması da mümkündür. 11 Eylül saldırılarında teröristler tarafından kullanılan silahlar sivil yolcu uçaklarıdır. Ancak bunlarla düzenlenen saldırılar sonucunda binlerce kişi ölmüş ve BM Güvenlik Konseyi meşru müdafaa hakkını tanımıştır. Bir şeyi silah yapan onun normal kullanım amacı veya tasarımı değil, kullanım sonucunda ortaya çıkan sonuçtur[49]. Bu

45 *NATO Glossary of Terms and Definitions* (2013), erişim: 1 Haziran 2017, http://www.dtic.mil/doctrine/doctrine/other/aap6.pdf.

46 Siber Savunma İş Birliği Mükemmeliyet Merkezi genel ağ sitesinde bazı devletlerin ve kurumların yaptığı siber saldırı tanımlarına yer verilmektedir. İlave tanımlar için bkz. https://ccdcoe.org/cyber-definitions.html.

47 Michael N. Schmitt (düz.), *Talinn Manual on the International Law Applicable to Cyber Warfare* (Cambridge University Presss, 2013.).

48 Terry D. Gill, "The Law of Armed Attack in the Context of the Nicaragua Case", *Hague Yearbook of International Law*. (Martinus Nijhoff, 1988), 30-58

49 Carl Zemanek, *"Armed Attack"*, Ekim 2013, erişim: 2 Haziran 2017, http://opil.ouplaw.com/view/10.1093/law:epil/9780199231690/law-9780199231690-e241.

durumda BMGK ve UAD kararları ışığında siber araçların kuvvet kullanımı yasağı çerçevesinde bir silah veya yöntem olarak değerlendirilmesinin önünde bir engel görülmemektedir.

Elbette bir siber saldırının silahlı saldırı olabilmesi için insan veya mala fiziksel zarar vermesi, kuvvet kullanımının belirli bir seviyeye ulaşmış olması gerekmektedir[50]. Bu anlamda iki ayrı görüş vardır. Siber saldırının silahlı saldırı olarak kabul edilebilmesi için belirli bir seviyede fiziksel zarara yol açması gerektiğini öne sürenler olduğu gibi[51], etkileri belirli bir seviyeye ulaştığı takdirde fiziksel zararın ortaya çıkmasına ihtiyaç bulunmadığı görüşünde olanlar da mevcuttur[52]. Bu konuda fiziksel zarar var olsa bile siber saldırının doğrudan ve dolaylı sonuçları arasında ayrım yapılması gerekmektedir. Çalışmamıza konu olan saldırılar, doğrudan fiziksel hasara neden olan saldırılardır. Dolaylı olarak hasar oluşturacak saldırılar (örneğin finansal sistemlere yönelik bir saldırı sonucu ortaya çıkabilecek kriz, toplumsal olaylar vs.) ekonomik ve siyasi zorlama önlemlerine benzetilerek[53] kuvvet kullanma yasağına aykırı görülmemektedir[54].

Uluslararası Adalet Divanının meşru müdafaaya temel teşkil edecek bir silahlı saldırının varlığını araştırırken dikkate aldığı kıstas boyut ve etkidir. Bu kıstas ortaya konulurken somut bir eşik belirlenmemiştir. Bir yandan silahlı saldırının kuvvet kullanımının en ağır biçimi olduğu belirtilirken diğer yanda tek bir geminin mayınlanmasının silahlı saldırı seviyesinde olabileceği göz ardı edilmemektedir. UAD'nin bu yaklaşımı, devletlerin silahlı saldırılara karşı savunmasız kalmamaları için, daha az önemli kuvvet kullanma biçimleri ile silahlı saldırı arasındaki boşluğun çok geniş olmaması gerektiği düşüncesiyle[55] akla yatkın gelmektedir.

Siber saldırılara yönelik BM Güvenlik Konseyi veya uluslararası mahkeme kararı bulunmadığından, bir siber saldırının silahlı saldırı olup olmayacağına ilişkin değerlendirmeyi günümüzde siber saldırılar tarafından yaratılabilecek etkiyi, geçmişte silahlı saldırı olarak tanımlanmış veya tanımlanabilecek olaylar ile karşılaştırarak yapacağız.

1981 yılında İsrail tarafından Irak'taki Osirak reaktörüne düzenlenen saldırıda, tamamlanmak üzere olan reaktör zarar görmüştür. BM Güvenlik Konseyinin bu olayla ilgili aldığı kararda meşru müdafaa hakkına atıf yapılmamakla birlikte İsrail'in eylemi askeri saldırı olarak tanımlanmıştır. Bu olayda İsrail savaş uçaklarınca yapılan saldırı sonucu ortaya çıkan etki Stuxnet'in yarattığı sonuçlarla kıyaslanabilir. Fiziksel hasar veren ilk zararlı yazılım olarak tarihe geçen Stuxnet solucanı (İran tarafından doğrulanmamakla

50 Marco Roscini, *Cyber Operations and the Use of Force in International Law.* (New York: Oxford University Press, 2014), 71.

51 Yoram Dinstein, *War, Agression and Self-Defence.* (Cambridge: Cambridge University Press, 2012), 212.

52 Paul Rosenzweig, *Cyber Warfare.* (Praeger, 2013), 48.

53 James A. Green, "The regulation of Cyber Warfare under Jus ad Bellum.", *Cyber Warfare A Multidisciplinary Analysis* içinde, düz. James A. Green, (New York: Routledge, 2015), 104.

54 Sara Pangrazzi, age, 15.

55 Yoram Dinstein, War, *Agression and Self-Defence*, 2018.

birlikte) tamamen devre dışı kalmasa da İran'daki uranyum zenginleştirme tesisindeki çok sayıda santrifüjün devre dışı kalmasına yol açmıştır. Stuxnet'in verdiği zarar sadece fiziki değil jeopolitik seviyede bir zarar olarak tanımlanmaktadır[56].

Bir diğer örnek 1999 yılında NATO'nun Kosova müdahalesine ilişkindir. 2 Mayıs 1999 tarihinde gerçekleştirilen NATO bombardımanında Yugoslavya'nın yarısına elektrik sağlayan Obrenovac elektrik santraline düzenlenen saldırı Sırbistan'ın elektrik sisteminin çökmesine neden olmuştur[57]. Verilecek kararın ne olacağını önceden kestirmek mümkün olmamakla birlikte, böyle bir olay UAD önüne taşındığında Divanın bu olayı kendi içtihadında yer alan kıstaslar (boyut ve etki) doğrultusunda silahlı saldırı olarak değerlendirmesi olasılık dahilindedir. Buna eşdeğer bir siber olay 2015 yılında Ukrayna'da yaşanmış, 23 Aralık'ta Ukrayna'nın elektrik sistemine düzenlenen siber saldırı sonucunda başkent Kiev'in yarısı (700.000 ev) elektriksiz kalmıştır[58].

Son bir örnek olarak 11 Eylül saldırılarını ele alacağız. 11 Eylül 2001 günü on dokuz hava korsanı tarafından dört yolcu uçağı kaçırılmış, bu uçakların ikisi Dünya Ticaret Merkezi'nin ikiz kulelerine, biri ise Pentagon'a çarpmış, saldırılar sonucunda yaklaşık 3000 kişi hayatını kaybetmiştir[59]. Bu olaydan sonra BM Güvenlik Konseyinde alınan kararlarda ABD'nin meşru müdafaa hakkının tanındığı ifade edilmiştir. Silahlı saldırı ifadesi karar metninde yer almamakla birlikte, meşru müdafaa hakkının ortaya çıkışından silahlı saldırının gerçekleşmiş olduğunun kabul edildiği değerlendirilmektedir. Bu olayda silah olarak teröristler tarafından kaçırılan sivil uçaklar kullanılmıştır. Benzer bir olay siber saldırı ile ele geçirilmiş, silahlı veya silahsız, insansız hava araçları ile de gerçekleştirilebilirdi. 2011 yılında İran, bir ABD insansız hava aracını siber saldırı ile ele geçirerek yere indirdiğini iddia etmiştir[60]. İnsansız hava araçlarının kontrolünün uydu üzerinden sağlandığı düşünüldüğünde, siber saldırı yoluyla bunların kontrolünün ele geçirilerek 11 Eylül benzeri saldırılar gerçekleştirilmesi teknik olarak mümkündür.

Buraya kadar verilen yaşanmış olaylar, siber saldırıların boyut ve etkilerinin daha önce silahlı saldırı olarak nitelenen veya nitelenebilecek olaylar seviyesinde olabileceğini göstermektedir. Bir siber saldırı ile ilgili olarak asıl korkulan şey kıyamet günü senaryoları olarak adlandırılan, siber saldırı yoluyla nükleer santrallerin bilgisayar sistemlerinin devre dışı bırakılmasıyla nükleer patlamalara neden olacak saldırılardır. Böyle bir saldırının gerçekleşmesi halinde bunun boyut ve etki bakımından kuvvet kullanma yasağının en

56 Richard Stiennon, "A Short History of Cyber Warfare.", *Cyber Warfare A Multi Disciplinary Analysis* içinde, düz. James A Green, (New York: Routledge, 2015), 22.

57 Daniel Williams, *"NATO Bombs Serbia Into Darkness"*, 3 Mayıs 1999. Erişim: 1 Haziran 2017, http://www.washingtonpost.com/wp-srv/inatl/longterm/balkans/stories/belgrade050399.htm.

58 James Titcomb, *"Ukrainian blackout blamed on cyber-attack"*, 5 Ocak 2016, erişim: 1 Haziran 2017, http://www.telegraph.co.uk/technology/news/12082758/Ukrainian-blackout-blamed-on-cyber-attack-in-world-first.html.

59 CNN, *September 11, 2001: Background and timeline of the attacks.* 8 Eylül 2016, erişim: 1 Haziran 2017, http://edition.cnn.com/2013/07/27/us/september-11-anniversary-fast-facts/.

60 Greg Jaffe, *"Iran says it downed U.S. stealth drone; Pentagon acknowledges aircraft downing."*, 4 Aralık 2011, erişim: 1 Haziran 2017, https://www.washingtonpost.com/world/national-security/iran-says-it-downed-us-stealth-drone-pentagon-acknowledges-aircraft-downing/2011/12/04/gIQAyxa8TO_story.html?utm_term=.e53de07277c6.

ağır ihlallerinden birisini oluşturacağını inkâr etmek mümkün görülmemektedir.

### 2.4. Devlet Uygulamaları

Bugüne kadar gerçekleşmiş bir siber saldırı konusunda meşru müdafaa hakkını kullandığını öne süren bir devlet olmamıştır. Bununla birlikte bazı devletler konuyla ilgili tutumlarını bazı belge ve açıklamalarla ortaya koymuştur. Örneğin, BM Genel Kurulu muhtelif kararlarıyla (örn: 65/41, 67/27) uluslararası güvenlik bağlamında devletlerin bilgi güvenliği konusundaki görüş ve değerlendirmelerini talep etmiştir. Birleşmiş Milletlerin Bilgi ve Telekomünikasyon alanında Uluslararası Güvenlik Bağlamındaki Gelişmeler Uzmanlar Grubu, 2013 yılında hazırladığı raporda devletlerin görüşlerini inceleyerek mevcut uluslararası hukuk kurallarının ve özellikle BM Şartı'nın Bilgi ve İletişim Teknolojisi (BM bu terimi kullanmaktadır) ortamında uygulanabilir olduğunu belirtmiştir[61].

Ayrıca konuyla ilgili devlet görüşlerinin yer aldığı bir Genel Sekreter raporu bulunmaktadır. Bu rapor incelendiğinde şu hususlar öne çıkmaktadır[62]: Avustralya mevcut uluslararası hukuk kurallarının bilgi güvenliği tehditlerine uygulanabilir bir çerçeve sunduğunu, kuvvet kullanma ve saldırı yasağının bu çerçeve içerisinde olduğunu savunmakta, ABD ise siber uzaydaki bir faaliyetin meşru müdafaa kapsamında silahlı saldırı sayılmasına dair belirleyici bir sonuca varmanın zor olduğunu, bununla birlikte muğlaklık ve tartışmaya açık alanların yeni bir hukuksal çerçeveye ihtiyaç olduğu anlamına gelmediğini, bir silahlı saldırı karşısında meşru müdafaa hakkının siber saldırılar için uygulanabileceğini kabul etmektedir.

Diğer devletler tarafından BM Silahsızlanma İşleri Ofisine gönderilen rapor ve görüşlerde şu hususlara yer verilmektedir[63]:

- Kanada, BM Şartı, insancıl hukuk ve insan hakları hukukunun siber uzay için de uygulanabilir olduğunu belirtmiştir.

- Gürcistan, bilgi güvenliğine yönelik tehditlere karşı mevcut ilke, andlaşma ve örf adet hukuku kurallarının uygulanabileceğini, buna BM Şartı'nda yer alan mekanizmaların da dahil olduğunu savunmuştur.

61 Birleşmiş Milletler Genel Kurulu, *"Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, Note by the Secretary-General."*, 24 Haziran 2013, erişim: 3 Haziran 2017, http://www.unidir.org/files/medias/pdfs/developments-in-the-field-of-information-and-telecommunications-in-the-context-of-international-security-2012-2013-a-68-98-eng-0-518.pdf.

62 Birleşmiş Milletler Genel Kurulu, *"Developments in the field of infromation and telecommunications in the context of international security."*, 15 Temmuz 2011, erişim: 3 Haziran 2017, http://www.un.org/ga/search/view_doc.asp?symbol=A/66/152.

63 UNODA, *"Developments in the field of information and telecommunications in the context of international security"*, 2017, erişim: 3 Haziran 2017, https://www.un.org/disarmament/topics/informationsecurity/.

- İsveç'e göre barış ve savaş zamanında uygulanabilir uluslararası hukuk, siber uzayda da uygulanabilecektir. Söz konusu hukuk alanları egemenlik, devlet sorumluluğu, insan hakları ile meşru müdafaa ve kuvvet kullanımıdır.

- Kore Cumhuriyeti, İngiltere, Almanya ve Kanada, BM Şartının bilgi ve iletişim teknolojileri ortamında da uygulanabilir olduğuna dair tespite katıldıklarını yinelemiştir.

Siber saldırı konusuyla ilgili BM platformunda dikkat çeken bir gelişme Çin, Rusya, Tacikistan ve Özbekistan tarafından uluslararası davranış kuralları oluşturulması için verilen öneridir[64]. BM Genel Kurul Kararı tasarısı olarak sunulan taslakta bilgi ve iletişim teknolojilerinin (diğerlerinin yanında) düşmanca eylemler veya saldırı eylemi maksadıyla kullanılmaması ilkesine de yer verilmektedir. İlginç olan ise aynı ülkeler tarafından, Kazakistan ve Kırgızistan'ın da katılımıyla güncellenerek 2015 yılında verilen öneride aynı paragrafın *"bilgi ve iletişim teknolojilerinin uluslararası barış ve güvenliğin korunması görevine karşı olacak şekilde kullanılmaması"* olarak tadil edilmesidir[65].

Devletlerin siber güvenlik konusundaki yaklaşımlarını anlayabileceğimiz bir diğer belge ise ulusal güvenlik veya siber güvenlik stratejileridir. Siber güvenlik stratejisinde birçok ülke hukuki çerçeveye yer vermiş olmakla birlikte biz tekrar olmaması açısından yalnız Belçika'nın siber güvenlik stratejisinde yer alan hususlara yer vereceğiz. *Savunma için Siber Güvenlik Stratejisi* başlıklı belgede meşru müdafaa hakkının dijital ortam için de geçerli olduğu, dijital silahlı saldırıların silahlı kuvvetlerin yanı sıra organize gruplarca da gerçekleştirilebileceği, Birleşmiş Milletler Şartı'nın 51. maddesinde meşru müdafaa hakkı için silah ayrımı gözetilmediği, bir dijital saldırının belirli şartlarda silahlı saldırı kabul edilebileceği ve askeri olsun veya olmasın meşru bir tepkinin önünü açacağı belirtilmiştir[66]. Meşru müdafaa hakkı ile ilgili genel tartışmaların özeti gibi görülen bu madde ile Belçika açıkça siber saldırıların silahlı saldırı seviyesine yükselebileceğini kabul etmiş ve buna karşı meşru müdafaa hakkını tanımıştır.

CCDCOE tarafından devletlerin koyula ilgili görüşlerine yer verilen derlemede de buraya kadar yer verdiğimiz bulguları destekleyen hususlar göze çarpmaktadır. Avustralya, Estonya, Finlandiya, Fransa, Almanya, İran, İsrail, İtalya, Japonya, Hollanda, Yeni Zelanda, Norveç, Singapur, İsviçre, Birleşik Krallık ve ABD boyut ve etkileri itibarı ile belirli bir seviyede fiziksel zarara yol açan siber saldırıların silahlı saldırı olarak kabul edilebileceğini ve BM Şartı kapsamında meşru müdafaa hakkının ortaya çıkabileceğini

64 Birleşmiş Milletler Genel Kurulu, *"Developments in the field of information…*

65 Birleşmiş Milletler Genel Kurulu, *"Letter dated 9 January 2015 from the Permanent Representatives of China, Kazakhstan, Kyrgyzstan, the Russian Federation, Tajikistan and Uzbekistan to the United Nations addressed to the Secretary-General"*, erişim: 26 Eylül 2021, https://digitallibrary.un.org/record/786846.

66 Defense Strategy Department. *"Cyber Security Strategy for Defence"*, 2004, erişim: 5 Mayıs 2017, https://ccdcoe.org/sites/default/files/strategy/Belgian%20Defence%20Cyber%20Security%20Strategy.pdf.

kabul etmektedir[67]. Brezilya da bu hususu kabul etmekle birlikte, saldırının bir devlete atfedilmesi[68] konusundaki güçlük nedeniyle nispeten temkinli bir duruş sergilemektedir[69].

### 2.5. Tallinn Kılavuzunda Meşru Müdafaa ve Silahlı Saldırı

2009 yılında NATO Siber Savunma İş Birliği Mükemmeliyet Merkezinin davetiyle oluşturulan uluslararası uzmanlar grubu tarafından siber savaş hukukuna ilişkin bir kılavuz derlenmiştir. Kısaca Tallinn Kılavuzu olarak adlandırılan bu kılavuz ile siber operasyonlar ile ilgili karmaşık hukuki hususları açıklama amacı güdülmüş hem kuvvet kullanımının hukukiliği *(jus ad bellum)* hem de silahlı çatışmaların yürütülmesine *(jus in bello)* ilişkin ilkelere yer verilmiştir. Giriş kısmında, kılavuzda yer verilen kuralların mevcut hukuk kurallarına *(lex lata)* göre belirlendiği ifade edilmiştir[70].

Kılavuzda meşru müdafaa ve silahlı saldırı konusuna da değinilmiştir. Silahlı saldırıya karşı meşru müdafaa başlıklı Kural 13 şu şekilde düzenlenmiştir[71]: *"Silahlı saldırı seviyesine ulaşmış bir siber saldırının hedefi olan bir devlet (doğal) meşru müdafaa hakkını kullanabilir. Bir siber saldırının silahlı saldırı oluşturup oluşturmadığı saldırının boyutuna ve etkilerine bağlıdır."*

Uzmanlar grubu bazı siber operasyonların BM Şartı çerçevesinde silahlı saldırı olarak nitelenebilecek ağırlıkta olduğu konusunda görüş birliğine varmıştır[72]. Bu görüş Uluslararası Adalet Divanının Nükleer Silahlar Danışma Kararında yer alan silahlı saldırı için silah konusunda bir ayrıma gidilmediği hükmü ile desteklenmektedir. Yine Divan tarafından yapılan, kuvvet kullanımı ile bunun en ağır biçimi olan silahlı saldırı arasındaki ayrım vurgulanarak silahlı saldırı eşiği için boyut ve etkiler kıstasına yer verilmiştir. Uzmanlar grubuna göre insanları yaralayan veya öldüren, mala zarar veren tüm kuvvet kullanımı şekilleri boyut ve etki kıstasını karşılamaktadır[73]. Benzer şekilde bir ülkenin kritik altyapısının önemli bileşenlerine yönelik siber operasyonlar yıkıcı etkileri olmasa da silahlı saldırı sayılabilecektir. 2012 yılına kadar uluslararası toplum tarafından bir siber saldırının silahlı saldırı olarak tanımlanmadığından hareketle, o zamana kadarki siber operasyonlarda boyut ve etki sınırının aşılmadığı değerlendirmesi yapılmıştır[74].

Uzmanlar grubu arasında siber saldırı için ortaya çıkan etki konusunda kasıt

67 *"Self-Defence"*, (t.y.). Erişim: 26.02.2022. https://cyberlaw.ccdcoe.org/wiki/Self-defence#cite_note-7 .

68 Siber ortamın dağıtık yapısı nedeniyle saldırıların bir kaynağa atfedilmesi konusu önemli bir sorun alanı teşkil etmektedir. Bu çalışmanın konusu bir siber saldırının silahlı saldırı teşkil edip etmeyeceği sorusu ile sınırlandırılmış olup, siber saldırıların bir kaynağa atfedilmesi, devlet dışı unsurların eylemlerinin silahlı saldırı oluşturup oluşturmayacağı ya da devlet dışı aktörlere karşı meşru müdafaa hakkının kullanımı gibi tartışmalar çalışma kapsamı dışında bırakılmıştır.

69 Agy.

70 Michael N. Schmitt (düz.), *Talinn Manual…*, 5

71 Age, 54.

72 Age, 54.

73 Age, 55.

74 Age, 58.

aranması gerektiği konusunda fikir birliği oluşmamıştır. Çoğunluk silahlı saldırı olarak tanımlanması için kasıt aranması gerekmediği görüşünü savunmuştur. Burada grubun Uluslararası Adalet Divanının Petrol Platformları davasındaki tutumundan ayıldığı görülmektedir.

Kılavuza göre bir silahlı saldırının sınır ötesi unsuru olmalıdır. Buna göre silahlı saldırı sayılabilecek siber saldırılar devletin sınırlarının dışından, başka bir devletten veya bu devlet tarafından yönlendirilen devlet dışı aktörlerden gelmelidir. Ayrıca siber saldırının etkilerinin üçüncü bir ülkeye sirayet etmesi halinde bu ülkenin de meşru müdafaa hakkının ortaya çıkacağı belirtilmiştir.

Kılavuz 2016 yılında geliştirilerek tekrar yayınlanmıştır. Meşru müdafaa ile ilgili kural, Kural 71 olarak aynen kılavuzda yer almıştır. Ancak kuralın yorumunda bazı değişiklikler göze çarpmaktadır. Örneğin daha önceki sürümde şimdiye kadar yaşanan hiçbir siber saldırının silahlı saldırı seviyesinde olmadığı belirtilmişken, yeni sürümde bazı uzmanlar tarafından 2010 yılındaki Stuxnet saldırısının silahlı saldırı seviyesine ulaştığı öne sürülmüştür[75]. Yeni sürümde tartışılan başka bir konu ise tek başına eşiği aşmayacak saldırıların etkilerinin zaman içindeki birikiminin silahlı saldırı olarak kabul edilip edilmeyeceğine ilişkindir. Uzmanlar grubu bu konudaki belirleyici unsurun saldırıların kaynağı olduğunu belirtmiş, yeterli kanıt bulunduğu takdirde bunların birleşik bir saldırı olarak kabul edilebileceği kabul edilmiştir.

Kurala ilişkin yorumda meşru müdafaa hakkının diğer unsurları ile hakkın kullanımına ilişkin hukuk doktrininde yer alan diğer tartışmalar siber saldırı bağlamında değerlendirilmiş olmakla birlikte, çalışmanın kapsamı dışında kaldığından burada yer verilmeyecektir.

Tallinn Kılavuzu resmi bir kaynak olmamakla birlikte, uluslararası hukukta düzenleme eksiği bulunan alanlardaki diğer kılavuzlar gibi (deniz savaşına ilişkin San Remo Kılavuzu, hava savaşına ilişkin Harvard Kılavuzu gibi) derleyici niteliğinden dolayı dikkate alınmasında fayda görülmüştür. Diğer yandan, konumuz ile ilgili kılavuzda yer alan kural ve bu konu etrafındaki tartışmaların daha önce değindiğimiz BM ve UAD kararları ile büyük ölçüde uyum içerisinde olduğu düşünülmektedir.

**Sonuç**

Tarih boyunca teknoloji, özellikle askeri teknoloji her zaman hukukun önünde gitmiştir. Kullanılmaya başlanan silahlar ile bunlara yönelik hukuki düzenlemeler arasındaki boşluk zaman zaman bu silahların istismarına yol açmıştır. Devletlerin teknoloji yoluyla askeri üstünlük sağlayarak kendi kaybını azaltma çabaları, geliştirilen yeni silahların mevcut hukuk kuralları çerçevesinde değerlendirilmesini zorunlu kılmaktadır. Bugün gelinen aşamada bilgisayar sistemlerine bağımlılık siber uzayı da bir savaş alanı

75 Michael N Schmitt (Düz.), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, (New York: Cambridge University Press, 2017), 342.

haline getirmiş, siber savaş bir kuvvet kullanma yöntemi olarak ortaya çıkmıştır. Siber araçlar edinmenin kolaylığı ve saldırı kaynağının belirlenmesinin güçlüğü, siber saldırıyı askeri bakımdan zayıf devletler ve terör örgütleri için de cazip hale getirmekte, bu durum uluslararası barışa tehdit oluşturmaktadır.

Barış ve güvenliği idame etmek üzere getirilen kuvvet kullanma yasağı genel kapsamlı bir yasaktır. Her ne kadar Şartın kaleme alındığı yıllarda bu yasak, dönemin koşulları gereği sadece devletlerin düzenli orduları için öngörülmüşse de yasağın geniş yorumu yıllar içinde ortaya çıkan durumları da içine almıştır. Bu genişleme gerek BM Genel Kurulu gerekse Uluslararası Adalet Divanı tarafından teyit edilmiştir. Kuvvet kullanma yasağının istisnası olan meşru müdafaa ise dar bir istisnadır. Meşru müdafaa kapsamında kuvvet kullanımının hukuka uygun olması sıkı koşullara bağlanmıştır. Bu koşullardan ilki bir silahlı saldırının gerçekleşmiş olmasıdır.

Meşru müdafaa için silahlı saldırı koşulu getirilmekle birlikte ne BM Şartı'nda ne de daha sonra silahlı saldırının tanımı yapılmamış, bu bir anlamda hakkı kullanacak devletin inisiyatifine bırakılmıştır. Meşru müdafaanın gündeme geldiği durumlara ilişkin metinlerde neyin silahlı saldırı olabileceği veya olmayacağı ile ilgili ipuçları bulunmaktadır. Özelikle UAD kararlarında yer alan kıstaslar bir olayın silahlı saldırı olarak değerlendirilmesi hususunda temel teşkil etmektedir. Bu kıstaslara göre bir kuvvet kullanma eyleminin silahlı saldırı olabilmesi için belirli boyutta olması ve etkilerinin belirli bir eşiği aşması gerekmektedir. Bu eylemde kullanılan silahın türünün ise önemi yoktur.

Bu kapsamda değerlendirildiğinde siber araç/silahların da silahlı sadırı için kullanılması mümkündür. Geçmişte gerçekleşmiş olaylar, siber saldırıların da boyutları ve etkileri bakımından silahlı saldırı seviyesine ulaşabileceğini göstermiştir. Bu saldırılar doğrudan fiziksel hasara yol açan etkilere sahiptir. Dolaylı etkiler ya da ekonomik ve siyasi sonuçlar doğuran siber saldırılar bu kapsamda görülmemektedir. Devletlerin söylemleri de bu yaklaşımı destekler mahiyettedir. Birçok devlet gerek kendi iç belgeleri gerekse uluslararası platformlardaki açıklamalarıyla mevcut uluslararası hukukun siber uzayda da uygulanabilir olduğunu, siber saldırılara karşı meşru müdafaa hakkının kullanılabileceğini kabul etmiştir.

**Kaynakça**

Akande, Dapo ve Milanoviç, Marko. The Constructive Ambiguity of the Security Council's ISIS Resolution. 21 Kasım 2015. http://www.ejiltalk.org/the-constructive-ambiguity-of-the-security-councils-isis-resolution/ (erişim: Ocak 3, 2017).

Avusturya Cumhuriyeti. "Austrian Cyber Security Strategy.", 2013. https://www.bka.gv.at/DocView.axd?CobId=50999 (erişim: Mayıs 31, 2017).

BBC. "Hack attack causes 'massive damage' at steel works.", 22 Aralık 2017. http://www.bbc.com/news/technology-30575104 (erişim: Nisan 19, 2017).

—. "Ukraine power cut 'was cyber-attack'.", 11 Ocak 2017. http://www.bbc.com/news/technology-38573074 (erişim: Nisan 19, 2017).

Berger, Joseph. "A Dam, Small and Unsung, Is Caught Up in an Iranian Hacking Case.", 25 Mart 2016. https://www.nytimes.com/2016/03/26/nyregion/rye-brook-dam-caught-in-computer-hacking-case.html?_r=0 (erişim: Nsan 11, 2017).

"Birleşmiş Milletler Andlaşması.", 26 Haziran 1945. https://www.tbmm.gov.tr/komisyon/insanhaklari/pdf01/3-30.pdf (erişim: Ocak 01, 2017).

Birleşmiş Milletler Genel Kurulu. "Definition Of Aggression (A/RES/29/3314).", 14 Aralık 1974. http://www.un-documents.net/a29r3314.htm (erişim: Ocak 05, 2017).

—. "Devletler Arasında BM Şartı'na Uygun Şekilde Dostane Münasebetler Kurma ve İşbirliği Yapmaya Dair Milletler Arası Hukuk İlkeleri Hakkında Bildiri.", 1970, http://www.unicankara.org.tr/doc_pdf/metin_ant1.pdf (erişim: Mayıs 29, 2017).

—. "Developments in the field of infromation and telecommunications in the context of international security.", 15 Temmuz 2011, http://www.un.org/ga/search/view_doc.asp?symbol=A/66/152 (erişim: Haziran 3, 2017).

—. "Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security Note by the Secretary-General.", 24 Haziran 2013, http://www.unidir.org/files/medias/pdfs/developments-in-the-field-of-information-and-telecommunications-in-the-context-of-international-security-2012-2013-a-68-98-eng-0-518.pdf (erişim: Haziran 3, 2017).

—. "Letter dated 9 January 2015 from the Permanent Representatives of China, Kazakhstan, Kyrgyzstan, the Russian Federation, Tajikistan and Uzbekistan to the United Nations addressed to the Secretary-General.", 9 Ocak 2015, https://digitallibrary.un.org/record/786846 (erişim: Eylül 26, 2021).

—. "Letter dated 12 September 2011 from the Permanent Representatives of China, the Russian Federation, Tajikistan and Uzbekistan to the United Nations addressed to the Secretary-Genera (A/44/359)l.", 14 Eylül 2011, www.un.org/ga/search/viewm_doc.asp?symbol=A/66/359 (erişim: Mayıs 10, 2017).

Birleşmiş Milletler Güvenlik Konseyi . “Resolution 1368 (2001) / Adopted by the Security Council at its 4370th Meeting, on 12 September 2001.”, https://digitallibrary.un.org/record/448051?ln=en (erişim: Eylül 26, 2021).

Birleşmiş Milletler Güvenlik Konseyi. “84(1950. Resolution of 7 July 1950.”, https://digitallibrary.un.org/record/112027 (erişim: Eylül 26, 2021).

—. “Meeting Records S/PV.7565.”, 20 Kasım 2015, http://www.un.org/en/ga/search/view_doc.asp?symbol=S/PV.7565 (erişim: Ocak 04, 2017).

—. “Resolution 1373 (2001)/Adopted by the Security Council at its 4385th Meeting, on 28 September 2001.», https://digitallibrary.un.org/record/449020?ln=en (erişim: Eylül 26, 2021).

—. “Resolution 2249 (2015)/adopted by the Security Council at its 7565th meeting, on 20 November 2015”, https://digitallibrary.un.org/record/811987?ln=en (erişim: Eylül 26, 2021).

—. “Resolution 487 (1981)/adopted by the Security Council at its 2288th meeting, on 19 June 1981.”, https://digitallibrary.un.org/record/22225 (erişim: Eylül 26, 2021).

—. “Resolution 661 (1990)/adopted by the Security Council at its 2933rd meeting, on 6 August 1990.”, https://digitallibrary.un.org/record/94221?ln=en (erişim: Eylül 26, 2021).

—. “Resolution 819 (1993/adopted by the Security Council at its 3199th meeting, on 16 April 1993.”, https://digitallibrary.un.org/record/164939?ln=en (erişim: Eylül 26, 2021).

Birleşmiş Milletler. “Summary Report of the Eleventh Meeting of the Committee I/1.” Documents of the United Nations Conference on the International Organisation. San Fransisco”, 5 Haziran 1945, https://digitallibrary.un.org/record/1300969?ln=en, (erişim: Eylül 23, 2021).

CNN. “September 11, 2001: Background and timeline of the attacks.”, 8 Eylül 2016. http://edition.cnn.com/2013/07/27/us/september-11-anniversary-fast-facts/ (erişim: Haziran 1, 2017).

Deeks, Ashley. “Threading the Needle in Security Council Resolution 2249.”, 23 Kasım 2015. https://www.lawfareblog.com/threading-needle-security-council-resolution-2249 (erişim: Ocak 04, 2017).

Defense Strategy Department. “Cyber Security Strategy for Defence.”, 2004. https://ccdcoe.org/sites/default/files/strategy/Belgian%20Defence%20Cyber%20Security%20Strategy.pdf (erişim: Mayıs 5, 2017).

Dinstein, Yoram. “Computer Network Attacks and Self-Defense.”, International Law Studies 76 (2002): 99-119.

—. War, Agression and Self-Defence. Cambridge: Cambridge University Press, 2012.

Elgebeily, Sherif. “HKU Legal Scholarship Blog.”, 29 Şubat 2016. http://researchblog.law.hku.hk/2016/02/sherif-elgebeily-comments-on-un.html (erişim: Ocak 4, 2017).

Eset. "Truva Atı". tarih yok. https://www.eset.com/tr/trojan-horse/ (erişim: Eylül 25, 2021).

Gill, Terry D. "The Law of Armed Attack in the Context of the Nicaragua Case.", Hague Yearbook of International Law içinde, 30-58. Martinus Nijhoff, 1988.

Government of the Republic of Lithuania. "Resolution 796 on the Approval of the Programme for the Development of Electronic Information Security for 2011-2019.", 29 June 2011. http://www.ird.lt/doc/teises_aktai_en/EIS(KS)PP_796_2011-06-29_EN_PATAIS.pdf (erişim: Haziran 01, 2017).

Gray, Christine. International Law and the Use of Force. New York: Oxford University Press, 2008.

Green, James A. "The regulation of Cyber Warfare under Jus ad Bellum.", Cyber Warfare A Multidisciplinary Analysis içinde, düzenleyen: James A. Green, 96-124. Routledge, 2015.

Hasan, Mahmood. "Opinion: Ambigious UN Resolution Adds to Complex and Dangerous Situation.", 30 Kasım 2015, http://www.asianews.network/content/opinion-ambiguous-un-resolution-adds-complex-and-dangerous-situation-4572 (erişim: Ocak 04, 2017).

Hruza, Petr ve Cerny, Jiri. "Cyberwarfare.", International Conference: The Knowledge-Based Organisation. Sibiu: Nicolae Balcescu Land Forces Academy, 2017. 155-160.

International Court of Justice. "Case Concerning Military and Paramilitary Activities in and Against Nicaragua. Merits, Judgement.", 27 Haziran 1986, http://www.icj-cij.org/docket/files/70/6503.pdf (erişim: Ocak 06, 2017).

—. "Case Concerning Oil Platforms.", 6 Kasım 2003, http://www.icj-cij.org/docket/?sum=634&code=op&p1=3&p2=3&case=90&p3=5 (erişim: Mart 15, 2017).

—. "Legality of the Threat or Use of Nuclear Weapons.", 8 Temmuz 1996, http://www.icj-cij.org/docket/index.php?p1=3&p2=4&k=e1&p3=4&case=95 (erişim: Mart 24, 2017).

Jaffe, Greg. "Iran says it downed U.S. stealth drone; Pentagon acknowledges aircraft downing.", 4 Aralık 2011. https://www.washingtonpost.com/world/national-security/iran-says-it-downed-us-stealth-drone-pentagon-acknowledges-aircraft-downing/2011/12/04/gIQAyxa8TO_story.html?utm_term=.e53de07277c6 (erişim: Haziran 1, 2017).

Katz, Yaakov. "Stuxnet virus set back Iran's nuclear program by 2 years.", 15 Aralık 2010, http://www.jpost.com/Iranian-Threat/News/Stuxnet-virus-set-back-Irans-nuclear-program-by-2-years (erişim: Nisan 19, 2017).

Larson, Robert E., ve Lance Cockcroft. CCSP: Cisco Certified Security Professional Certification. McGRaw-Hill, 2003.

NATO Glossary of Terms and Definitions., 2013. http://www.dtic.mil/doctrine/doctrine/other/aap6.pdf (erişim: Haziran 01, 2017).

Norton. "What is a computer worm, and how does it work?", 28 Ağustos 2019, us.norton.com/

internetsecurity-malware-what-is-a-computer-worm.html (erişim: Eylül 25, 2021).

Pangrazzi, Sara "Self-Defence Against Cyberattacks?: Digital and Kinetic Defence in Light of Article 51 UN-Charter", (2021), 12. Erişim: 25.02.2022. https://ict4peace.org/activities/new-publication-self-defence-against-cyberattacks-digital-and-kinetic-defence-in-light-of-article-51-un-charter/

Porche, Isaac R. "Cyberwarfare Goes Wireless.", 4 April 2014, https://www.usnews.com/opinion/blogs/world-report/2014/04/04/russia-hacks-a-us-drone-in-crimea-as-cyberwarfare-has-gone-wireless (erişim: Nisan 20, 2017).

Roscini, Marco. Cyber Operations and the Use of Force in International Law. New York: Oxford University Press, 2014.

Rosenzweig, Paul. Cyber Warfare. Praeger, 2013.

Schmitt, Michael N, düz. Talinn Manual On The International Law Applicable to Cyber Warfare. Cambridge University Presss, 2013.

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

Self-Defence, (t.y.). Erişim: 26.02.2022. https://cyberlaw.ccdcoe.org/wiki/Self-defence#cite_note-7

Schmitt, Michael N., düz. Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations. New York: Cambridge University Press, 2017.

Shaw, Malcolm N. Internatioal Law. Cambrigde: Cambridge University Press, 2008.

Stiennon, Richard. "A short History Of Cyber Warfare." Cyber Warfare A Multi Disciplinary Analysis içinde, düzenleyen: James A Green, 7-32. Londra ve New York: Routledge, 2015.

Symantec Corporation. "What is the difference between viruses, worms, and Trojans?", 30 Eylül 2016, https://support.symantec.com/en_US/article.TECH98539.html (erişim: Haziran 3, 2017).

T.C. Ulaştırma Denizcilik ve Haberleşme Bakanlığı. "Ulusal Siber Güvenlik Stratejisi (2016-2019).", tarih yok, http://www.udhb.gov.tr/doc/siberg/2016-2019guvenlik.pdf (erişim: Mayıs 15, 2017).

Titcomb, James. "Ukrainian blackout blamed on cyber-attack.", 5 Ocak 2016, http://www.telegraph.co.uk/technology/news/12082758/Ukrainian-blackout-blamed-on-cyber-attack-in-world-first.html (erişim: Haziran 1, 2017).

UNODA. "Developments in the field of information and telecommunications in the context of international security.", 2017, https://www.un.org/disarmament/topics/informationsecurity/ (erişim: Haziran 3, 2017).

Weimann, Gabriel. "Cyberterrorism: How Real is the Threat?", Aralık 2004, https://css.ethz.ch/en/services/digital-library/publications/publication.html/14122 (erişim: Aralık 24, 2021).

Williams, Daniel. "NATO Bombs Serbia Into Darkness.", 3 Mayıs 1999, http://www.washingtonpost.com/wp-srv/inatl/longterm/balkans/stories/belgrade050399.htm (erişim: Haziran 1, 2017).

Zemanek, Carl. "Armed Attack.", Ekim 2013, http://opil.ouplaw.com/view/10.1093/law:epil/9780199231690/law-9780199231690-e241 (erişim: Haziran 2, 2017).