*The Turkish Yearbook of International Relations*,
Volume 53 (2022), p. 21 - 40

# Siber Uzayda Kuvvet Kullanma Yasağı ve Yasağın İstisnalarının Geçerliliğinin Tallinn Rehberi Kapsamında Değerlendirilmesi

**Cemre Çise Kadıoğlu Kumtepe***

## Özet

Bu çalışmada, devletlerin siber uzayda egemenlik tesis edip edemeyeceği ve siber uzayda kuvvet kullanımına yönelik uluslararası hukuk kurallarının uygulanabilirliği ele alınmıştır. Siber uzayda kuvvet kullanmanın kapsamının belirlenmesine yönelik yaklaşımlar ve bu konuda var olan uluslararası hukuk kuralları üzerinde durulmuştur. Devlet dışı aktörlerin siber eylemlerinden doğan sorumluluk incelenmiş ve kuvvet kullanma yasağının istisnası olan meşru müdafaa hakkının uygulanabilirliği tartışılmıştır. Çalışmanın sonucunda, uluslararası hukuk kurallarının siber uzayda kuvvet kullanımına uygulandığı ve kuvvete başvurma yasağının istisnaları siber uzayda da geçerliliğini koruduğu görülmüş, siber uzayda silahlı saldırının tanımı, meşru müdafaanın kapsamı ve yönlendirileceği taraf açısından gri alanlar nedeniyle bu kuralların sınırlı şekilde uygulanması gerektiği sonucuna varılmıştır.

## Anahtar Kelimeler

Siber saldırı, kuvvet kullanma, meşru müdafaa hakkı, Tallinn Rehberi.

---

* Doktora öğrencisi, University of Leicester, cckkl@leicester.ac.uk,
ORCID: 0000-0002-9573-727X
Makale geliş tarihi : 17.02.2022
Makale kabul tarihi : 26.07.2022

# Evaluation of Prohibition Against Use of Force and Validity of its Exceptions in Cyberspace Within the Scope of Tallinn Manual


## Abstract

In this study, whether states can establish sovereignty in cyberspace and the applicability of international law rules for the use of force in cyberspace is discussed. The approaches to determining the scope of the use of force in cyberspace and the existing international law on this subject are analyzed. The responsibility arising from the cyber actions of non-state actors is analyzed and the applicability of the right of self-defense, which is an exception to the prohibition of use of force is discussed. As a result, it is seen that the rules of international law are applicable to the use of force in cyberspace and the exceptions to the prohibition of resorting to force are still valid in cyberspace, and it has been concluded that these rules should be applied restrictively because of the gray areas with the definition of armed attack, the scope of self-defense and the party to whom the self-defense will be directed in cyberspace.



## Keywords

Cyber-attack, use of force, right of self-defense, Tallinn Manual.


## Giriş

2007'de Estonya'nın İkinci Dünya Savaşı'nda ölen askerin mezarını taşıması üzerine Estonya'nın bankalara ve devlete ait siber altyapılarına Rusya kaynaklı siber saldırının gerçekleştirilmesinin ardından, siber saldırıların hukuki niteliği ve uluslararası hukukun sunacağı çözümler önem kazanmıştır. Çoğu zaman bilgisayar sistemlerini hedef alan küçük çapta saldırılar olsa da önemli düzeyde fiziksel zarara yol açan siber saldırıların da gerçekleştirildiği görülmektedir. 2010 yılında İran'ın nükleer tesislerine yapılan Stuxnet saldırıları buna örnek olarak verilebilir (Fildes, 2010). 12 Nisan 2021'de yine İran'ın nükleer tesislerine yönelik İsrail kaynaklı olduğu iddia edilen saldırılar söz konusudur (Corera, 2021). Bu saldırılara karşı devletlerin resmî açıklamalar veya benzeri tepkilerden kaçındıkları gözlemlenmektedir.

4 Mayıs 2021 tarihinde ise Belçika parlamentosuna, üniversitelere ve çeşitli bilim kuruluşlarına siber saldırı düzenlenmiş, hiçbir veri çalınmadan sadece kişilerin internete erişimi engellenmiştir. Bu saldırının neticesinde aşı merkezleri de etkilenmiştir. Saldırı taktiği sürekli değiştiğinden saldırının önüne geçilmesi de zorlaşmıştır (Euronews, 2021). Her ne kadar kaynağı belirlenemese de saldırlar, Belçika parlamentosunun Çin'in Uygurlara yönelik politikaları hakkındaki

tartışmalarına denk geldiğinden gözler Çin'e çevrilmiştir **(**Quach, 2021). Siber saldırıların politik amaçlarla devlet dışı aktörler tarafından kullanıldığı görülmekte veya kaynakları tam olarak bilinmeyen ancak siyasi ilişkiler çerçevesinde olası şüphelilerin işaret edildiği siber saldırı senaryoları ortaya çıkmaktadır. Bu tür senaryolar, siber uzayın ve siber saldırıların uluslararası hukuk kuralları çerçevesinde ele alınmasını gerekli kılmaktadır.

Önceleri internet ve siber uzayın devlet egemenliğine tabi olmadığı düşünülmekteyken, günümüzde devletlerin siber uzayda da belli bir düzeyde egemenlik alanları olduğu görüşü benimsenmiştir. Bunun neticesinde, uluslararası hukuk kurallarının siber uzayda geçerli olup olmadığı konusundaki tartışmalar bu sorunun olumlu olarak çözülmesiyle sonuçlanmıştır. Ancak siber uzay geçerli uluslararası hukuk kurallarının çözemeyeceği yeni ve oldukça karmaşık hukuki problemleri beraberinde getirmiştir. Bununla birlikte yeni kuralların geliştirilmesi oldukça zor olduğundan uluslararası hukuk kuralları kıyas yoluyla siber uzaya uygulanmaktadır.

Siber uzayın, kötücül davranışların serbestçe sergilenebileceği hukuksuz bir alan olmadığında görüş birliği bulunmaktadır. Siber faaliyetler de Birleşmiş Milletler madde 2(4) ve örf ve adet hukuku kuralları çerçevesinde kuvvet kullanma olarak nitelendirilebilmektedir. Mallara doğrudan fiziksel zarar veren ya da kişilerin ölümüne ve yaralanmasına neden olan siber saldırılar kuvvet kullanma ve hatta silahlı saldırı olarak kabul edilmekle birlikte, bu türden olmayan ve doğrudan kuvvet kullanma olarak nitelendirilemeyen siber saldırılar konusunda belirsizlik söz konusudur (Hoisungton, 2009: 447). Bu konuda, 2013 yılında NATO çatısı altında Uluslararası Uzman Grubu tarafından uluslararası hukuk kurallarının siber savaşlara uygulanabilirliğini inceleyen Tallinn Rehberi yayımlanmıştır (Tallinn Rehberi, 2013). Tallinn Rehberi siber çatışmaları düzenleyen doksan beş adet kurala yer vermiştir. Kurallar egemenlik, devletin sorumluluğu, *jus ad bellum*, insancıl hukuk ve tarafsızlık konularını ele almaktadır. Rehber yeni kurallar getirmemekte, yürürlükteki kuralların siber uzay bağlamından nasıl yorumlanması gerektiği konusunda yol göstermektedir. Kriterler 2017 yılında güncellenerek kapsamı silahlı çatışma düzeyinde olmayan zararlı siber faaliyetleri kapsayacak şekilde genişletilmiştir (Tallinn Rehberi 2.0, 2017).

Siber uzaydaki faaliyetler neticesinde, devletlerin ve devletlerin ajanlarının hukuken sorumluğu olduğu kabul edilmektedir. Siber saldırılar karşısında devletlerin her zaman başvurabileceği yöntemler bulunmaktadır. Uluslararası iş birliği ve uyuşmazlıkların çözüm mekanizmalarının işletilmesi, polis gücünün kullanılması, tek taraflı eylemlerin gerçekleştirilmesi, misilleme ve kısıtlayıcı önlemler alınması devletlerin siber saldırı karşısında alabileceği önlemlerdendir. AB'nin Ağ ve Bilgi Güvenliği Direktifi ile üye devletler arasında iş birliğini teşvik

etmesi siber saldırılara karşı uluslararası iş birliğine örnek olarak verilebilir (European Commission, 2017). Teoride devletler arasında siber saldırılar neticesinde çıkacak uyuşmazlıklar bakımından Uluslararası Adalet Divanı'na da başvurulabileceği belirtilmektedir (Christakis, 2021). ABD, Kuzey Kore'nin Sony Pictures'a yönelttiği iddia edilen siber saldırılar neticesinde tek taraflı siber yaptırımlar uygulamıştır (BBC, 2015). Yine, AB diplomatik yaklaşımlar ve barışçıl karşı önlemlerin uygulanması için Siber Diploması Araç Kutusu'nu geliştirmiştir (Moret ve Pawlak, 2017).

Bunların dışında, yalnızca başka bir devlet tarafından uluslararası hukukun ihlal edilmesi durumunda verilebilecek tepkiler bulunmaktadır. Devletler her zaman alabilecekleri önlemlere ek olarak barışçıl karşı önlemler alabilirler ve şartları bulunuyorsa silahlı saldırı durumunda meşru müdafaaya başvurabilirler. Meşru müdafaa hakkının doğup doğmadığının anlaşılabilmesi için öncellikle siber uzayda kuvvet kullanmanın kapsamının belirlenmesi ve Birleşmiş Milletler madde 51 kapsamında değerlendirme yapılması gerekmektedir.

Bu çalışmada, siber uzaydaki egemenlik alanları üzerinde kısaca durulduktan sonra uluslararası hukuk kuralları ve özellikle BM Anlaşması m. 2(4) kapsamında kuvvet kullanma yasağının siber uzayda geçerliliğine değinilmektedir (BM Anlaşması, 1945: m.2(4)). Siber uzayda kuvvet kullanmanın kapsamı, doktrindeki farklı bakış açıları ile getirilen güncel kriterler ışığında değerlendirilmektir. Son olarak, bu kurallar ışığında devletin kuvvete başvurma yasağının istisnası olan meşru müdafaa hakkının siber uzayda da geçerli olup olmadığı tartışılmaktadır. Uluslararası hukuk kurallarının siber uzayda kuvvet kullanımına uygulandığı ve kuvvete başvurma yasağının istisnalarının siber uzayda da geçerliliğini koruduğu görülmekle birlikte, siber uzayın özellikleri neticesinde silahlı saldırının tanımı, meşru müdafaanın kapsamı ve yönlendirileceği taraf açısından gri alanların fazlalığı nedeniyle sınırlı şekilde uygulanması gerektiği sonucuna varılmaktadır.

## I. Siber Uzayda Egemenlik Sorunu

Siber güvenlik sadece sivil kullanıcılar ve kaynaklarla değil, askeri güçlerle de ilgili olup devletler arasında çatışmalara yol açabildiğinden siber uzayda egemenlik tartışmaları gündeme gelmekte; siber uzay egemenliğe ilişkin yerleşik kurallar çerçevesinde ele alınmaya çalışılmaktadır (Mueller, 2018: 3). Devlet yasal olarak kendi ülkesinin sınırları içerisinde kuvvet kullanabilmektedir. Siber uzayın aslında gerçek dünyanın bir parçası olduğu dolayısıyla devletin egemenliğiyle sınırlandırılması gerektiği görüşü ileri sürülmüştür (Franzese, 2009: 1-17). İlerleyen bölümlerde detaylandırılacağı üzere Tallinn Rehberi'nin uluslararası hukukta egemenliğe yönelik genel ilkeleri aynen benimsediği görülmektedir. Tallinn Rehberi devletlerin siber uzayda egemenlik tesis etmelerinden ziyade

kendi sınırları içerisinde bulunan siber altyapı ve eylemler üzerinde egemenlik yetkisine sahip olduğunu vurgulayarak bu konudaki genel bakış açısını dile getirmektedir (Tallinn Rehberi, 2013: Kural 1). Bu bağlamda devletler sınırları içindeki siber altyapı ve eylemler üzerinde egemenlik tesis etmekte ve ülkesinde internete erişimi sınırlamak gibi önlemlere başvurabilmektedir (Lotrointe, 2012: 829).

Ayrıca, bir devletten diğer devletin sınırları içerine yapılan siber operasyonların niteliklerine göre müdahale, saldırı veya silahlı saldırı boyutlarına ulaşabileceği, duruma göre devletin meşru müdafaa hakkının söz konusu olabileceği belirtilmektedir (Tallinn Rehberi, 2013: Kural 1, Yorum 6-7). Bu unsurlar göz önünde bulundurulduğunda siber uzayın hepsinde olmasa da eylemlerin yapıldıkları yer, sonuçlarının doğduğu yer ve altyapının bulunduğu yer gibi devletin ülkesine fiziksel olarak bağlanabilecek şekilde egemenlik hakkının siber uzaya da uzandığını söylemek mümkündür.

Bunlara karşın, siber uzayda egemenlik tesis edilemeyeceği belirtilmekte, edilse bile bunun internetin değerli yönlerini körelteceği belirtilmektedir (Mueller, 2018: 5). İnternet protokollerinin sınırları aşan niteliği neticesinde devlet kuramının siber uzayda geçerliliğini kaybedeceği ileri sürülmektedir (Mueller, 2018: 6). Böyle bir ortamda hem devlet aktörleri hem de saldırganlar aynı şekilde hareket edebileceklerdir. Bu eleştiriler çerçevesinde, müdahaleler, tehditler ve zararlı yazılımlar devletlerin sınırlarından bağımsız şekilde dünyanın herhangi bir yerinden yönlendirilebileceğinden devlete karşı kuvvet kullanılıp kullanılmadığının belirlenmesi de imkânsız bir hal alacaktır. Ancak devletlerin siber uzayda da geçerli menfaatleri bulunduğundan siber eylemler üzerinde kontrol kurmayı beklemeleri oldukça doğaldır. Bu nedenle siber uzayda egemenlik tesis edilemeyeceğini belirten yaklaşım, siber uzayda egemenlikle sağlanabilecek kararlılık ve düzenin gerekliliğini göz ardı etmektedir (Franzese, 2009: 10-11). Bu yaklaşımı eleştirenler devletlerin milli güvenlik gerekçesiyle siber uzayda varlıklarını ortaya koymaları gerektiğini savunmaktadır (Franzese, 2009: 13).

Egemenlik konusunda bir başka yaklaşım, siber uzayın açık denizler ve dış uzay gibi egemenlik tesis edilmeyen bölgelerdeki egemenlik anlayışının siber uzay için de geçerli olmasıdır (Mueller, 2018: 6). Evrensel ortak varlıkların özellikleri siber uzaya uygulanamadığından bu yaklaşım da büyük ölçüde eleştirilmektedir. Evrensel ortak varlıklar uluslararası bir sözleşmeye tabidir ve bu sözleşme çerçevesinde haklar ve kısıtlamalar düzenlenmektedir. Bu bölgelerin tanımlanabilir sınırları söz konusudur ve devletler münhasır egemenlik iddialarını bir kenara bırakma konusunda anlaştığından tek bir devlet bu bölgeler üzerinde kontrol hakkına sahip değildir (Franzese, 2009: 17). Özellikle sınırların

belirlenebilir olması siber uzaya uygulanamadığından, siber uzayın evrensel ortak varlıklar gibi ele alınması da uygun görünmemektedir.

Devletlerin siber uzayda egemenlik konusundaki tutumları da farklılık göstermektedir. Örneğin, Çin her devletin milli çevrimiçi alanlarını kurmaya, içerikleri ve sınırları içindeki veri akışını tamamen kontrol etmeye hakkı olduğunu savunmaktadır. 2017 yılında Siber Uzayda İş birliği Hakkında Uluslararası Strateji (International Strategy on Cooperation in Cyberspace) belgesinde Çin özetle şu ana ilkeleri benimsemiştir:

- Birleşmiş Milletler Şartı devletler arası ilişkileri tüm yönleriyle kapsamaktadır, buna siber uzay da dahildir,
- Ülkeler birbirlerinin siber gelişme, düzenleme ve politikalarını seçme haklarına saygı duymalıdır,
- Hiçbir ülke siber hegemonya kurmaya çalışmamalı, diğer ülkelerin iç ilişkilerine katılmamalı, milli güvenliklerini tehdit edecek siber eylemlerde bulunmamalı veya desteklememelidir,
- Siber uzayda egemenliği tesis etmek hükümetlerin sadece siber uzayı hukuka uygun şekilde idare etme sorumluluğunu ve hakkını ifade etmekle kalmaz, aynı zamanda ülkelerin hükümetler, işletmeler ve sosyal gruplar arasındaki sağlam ilişkileri oluşturmasını sağlar.
- Siber uzay tüm insanlığın ortak etkinliklerini gerçekleştirdiği bir alan olarak tüm ülkeler tarafından yönetilmelidir. Bu yapılırken çok taraflı yaklaşım benimsenmeli, uluslararası toplumun tüm üyeleri eşit söz sahibi olmalıdır. (Ministry of Foreign Affairs of the Republic of China, 2017).

Amerika Birleşik Devletleri de Çin'in çok taraflı (*multilateral*) yönetimine benzer şekilde çoklu paydaş (*multistake holder*) *status quo*'sunun korunması gerektiğini savunmakta, şirketlerin, teknik uzmanların, sivil toplum örgütlerinin, toplulukların ve hükümetlerin katılımıyla düzenlenen özel bir yönetişimin gerektiğini belirtmektedir. Böylelikle verilerin serbest dolaşımı ve şeffaflık gibi ilkelerin hakim kılınması hedeflenmiştir. Başlarda ülkeler daha fazla hükümet kontrolü gerektiğini ileri sürse de 2015 itibariyle bu denge değişmiş, çoğunluk çoklu paydaş yönetişiminin ideal olduğunda karar kılmıştır (Brotman, 2015).

Bununla birlikte, ABD 2011 yılında Birleşmiş Milletler Şartı ile uyumlu olacak şekilde siber uzayda belirli saldırılar neticesinde doğacak doğal meşru müdafaa hakkını kullanacağını açıklamıştır (White House, 2011). Buradan yola çıkarak, hem kendi egemenliğine saygı duyulması gerektiğini hem de gerektiğinde başka ülkenin egemenlik alanında meşru müdafaada bulunacağını ima ederek siber uzayda devletlerin egemenlik hakları olduğunu benimsediğini söylememiz mümkündür.

Sonuç itibariyle devletlerin yaklaşımı ise ülkeleri içindeki eylemler, altyapı ve eylemlerin kendileri üzerindeki etkileriyle sınırlı olmak üzere egemenliğe sahip oldukları yönündedir. Dolayısıyla siber uzayda egemenlik hakkının olup olmadığı varsa sınırlarının ne olduğu belirlenememekle birlikte; genel eğilim devletin egemenliğinin kendi ülkesi sınırlarında veya ülke toprağı kabul edilen yerlerde gerçekleşen eylemler ya da siber eylemlerin burada doğan sonuçları bakımından belirli bir düzeyde kullanılabileceği yönündedir. Bununla birlikte, kuvvet kullanımına yönelik uluslararası hukuk kurallarının ne derece uygulanabileceği ve bu kuralların sonuçları ayrı bir tartışma konusu olarak karşımıza çıkmaktadır.

## II. Siber Uzayda "Kuvvet Kullanma" Tanımı ve Kapsamı

### A. Kuvvet Kullanımına İlişkin Uluslararası Hukuk Kurallarının Siber Uzayda Uygulanabilirliği

Uluslararası hukukta kuvvet kullanma BM Anlaşması m. 2(4) ile yasaklanmıştır. Bu maddeye göre *"Tüm üyeler, uluslararası ilişkilerinde gerek herhangi bir başka devletin toprak bütünlüğüne ya da siyasal bağımsızlığa karşı, gerek Birleşmiş Milletlerin Amaçları ile bağdaşmayacak herhangi bir biçimde kuvvet kullanma tehdidine ya da kuvvet kullanılmasına başvurmaktan kaçınırlar.*" (BM Anlaşması, 1945: m. 2(4)). Bu madde aynı zamanda örf ve adet hukuk kuralını yansıtmakta ve *Nicaragua* kararında ortaya konulduğu üzere *jus cogens* kural niteliği taşımaktadır. (UAD, *Nikaragua v ABD*)

Bu bağlamda kuvvet kullanma yasağının siber uzayda geçerliliğini koruyup korumadığı tartışma yaratmıştır. Bu konu siber uzay gibi mekânsal ya da kavramsal olarak değil eylemlerin niteliği – yani siber operasyonlar – bazında ele alınmıştır. Bazı düşünürler var olan hukuk kurallarının uygulanamayacağını, bu kuralların siber uzayda ortaya çıkan sorunlara cevap vermede yetersiz kaldığını dolayısıyla siber konuları ele alan bir anlaşma yapılması gerektiğini savunmuştur. Diğer bir grup düşünür ise hukuk kurallarının kıyasen uygulamaya elverişli olduğunu, kuvvet kullanımına ilişkin yürürlükte olan düzenlemelerin siber saldırı/savaş kavramlarına da uygulanabileceğini ileri sürmüşlerdir (Boer, 2013: 9).

BM Anlaşması'nın amaçlarından biri m. 2(4)'te yansıtıldığı üzere uluslararası barış ve güvenliği sağlamaktır. Düzenlemenin bu amacı göz önünde bulundurulduğunda, kuvvet kullanma yasağının siber saldırıları da kapsayacak şekilde yorumlanması gerektiği açıktır. Uluslararası Adalet Divanı da *Nükleer Silahlar* görüşünde bu konuya açıklık getirmektedir. Nükleer Silahlar konusunda UAD'den m. 2(4) belirtilen kuvvet kullanma yasağı ve ilgili m. 52 ve m. 42'nin nükleer silahlara uygulanması konusunda görüş belirtmesi istenmiştir. UAD, bu ilgili maddelerin kullanılan silahın türünden bağımsız olarak her kuvvet

kullanımına uygulanacağını belirtmiştir (*Nükleer Silahlar*, 1996: para.39). Geleneksel silahlar yerine bilgisayar gibi bilişsel araçların kullanılmasının kuvvet kullanımı nitelendirmesinde önemsiz olduğu anlaşılmaktadır (Tallinn Rehberi, 2013: 42). Kuvvet kullanma tehdidi veya kuvvet kullanmaya yol açan eylemler yasaklanmış olup bunların gerçekleştirilmesinde kullanılan araçlar yasağın belirlenmesinde önemini kaybetmektedir (Delibasis, 2006: 7).

BM Anlaşması m. 2(4)'te kuvvet kullanma tehdidini ve kuvvet kullanmayı yasaklamış ancak kuvvetin veya kuvvet kullanımının tanımı yapılmamıştır. Yargı kararlarında da tatmin edici bir tanımlama bulunmamaktadır. Bunun sonucunda kuvvet kullanma yasağının kapsamı tartışmalı hale gelmiştir. Yasağın sadece silahlı kuvvet kullanılmasıyla mı sınırlı olduğu yoksa zorlayıcı ekonomik ve diplomatik tedbirlerin de bu yasağın kapsamına girip girmediği konusunda farklı görüşler ortaya atılsa da yasağın siyasi ve ekonomik zorlamaları kapsamadığı görüşü ağır basmıştır (Goodrich, Hambro ve Simons, 1969: 49; Yayla, 2013: 205).

Kuvvet kullanma yasağının konvansiyonel olmayan fiziksel güç kullanımını kapsadığı da genel olarak kabul görmektedir. Buradan yola çıkılarak her ne kadar geleneksel askeri gücün ortaya çıkardığı kinetik etkileri söz konusu olmasa da kimyasal ve biyolojik silahlar da kuvvet kullanımı olarak değerlendirilmektedir (Foltz, 2012: 8).

Kuvvet kullanmanın kapsamına silahlı saldırı, saldırı, silahlı saldırı ve saldırı seviyesine ulaşmayan kuvvet kullanımı ve müdahale girmektedir. Eylemlerin doğru tanımlanması özellikle silahlı saldırı fiillerinin meşru müdafaa hakkını doğurması bakımından kritiktir. Saldırının tanımı, BM Genel Kurulu'nun 1974 tarihli 3314 (XXIX) sayılı kararının 3. Maddesinde, bu maddede sayılan eylemlerle sınırlı olmayacak şekilde yapılmıştır. Bu tanıma daha çok askeri nitelikte ve geleneksel silahlar vasıtasıyla yapılan eylemler dahil edilmiştir (BM Genel Kurulu, 1974). Diğer eylemler açısından benzer bir tanımlama yapılmamıştır. Siber operasyonların kuvvet kullanımına dahil olup olmadığı da tartışmaları devam ettirmiştir. ABD başta olmak üzere teknolojik açıdan avantajlı devletler m.2(4)'ün siber saldırıları da kapsayacak şekilde geniş yorumlanması gerektiği görüşündedir (Yayla, 2013: 206).

Siber operasyonlar ise çok farklı şekillerde meydana gelebildiğinden kapsamının belirlenmesi oldukça güçtür. İnternet sitesine yapılan sıradan bir saldırı şeklinde olabileceği gibi önemli ulusal verilerin tutulduğu sistemlere girilmesi veya sistemlere erişilerek silahların ortaya çıkarabileceği fiziksel zararlar verilmesi şeklinde de gerçekleşebilir. Benzer şekilde birçok siber saldırı aslında adi suçlar ve casuslukla alakalıdır. Bunları gerçekleştirenler uluslararası hukukun tanımladığı şekilde savaş içerisinde değildir (Lewis, 2010: 1). Bu durumda her olgu bazında değerlendirme yapılması gerekmektedir.

Genel itibariyle siber uzayın kötücül eylemlerin serbestçe vuku bulduğu, hukuksuz bir alan olarak görülmemesi gerekmektedir (Koh, 2012: 3; Schmitt, 2012: 17). Siber eylemler de duruma göre kuvvet kullanma teşkil edebilecektir. Dolayısıyla hem *jus ad bellum* hem de *jus in bello*'nun siber operasyonlara uygulanacağının kabulü gerekmektedir (Tallinn Rehberi, 2013: 5; Koh, 2012: 3). Bu nedenle hangi eylemlerin kuvvet kullanımı teşkil ettiği ve uygulanacak kuralların ele alınması gerekmektedir. Eylemlerin kuvvet kullanımı olup olmadığının belirlenmesinde farklı kriterler kullanılmaktadır. Bunlar hedef temelli yaklaşım, vasıta temelli yaklaşım ve etki temelli yaklaşım, olarak sınıflandırılmaktadır. Bu konuda en geniş kapsamlı ve detaylı çalışma Tallinn Rehberi olduğundan buradaki nitelendirmeler de önem arz etmektedir.

### B. Siber Saldırının Nitelendirilmesi

#### 1. Hedef Temelli Yaklaşım

Bu yaklaşıma göre siber operasyonun hedefinin niteliğine göre eylem tanımlanmalıdır. Örneğin, kritik öneme sahip bir bilgisayar sisteminin siber saldırıda hedef alınması, siber operasyonun saldırı veya silahlı saldırı olarak nitelendirilmesine yol açabilecektir. Bu değerlendirmenin neticesinde silahlı saldırı olduğuna kanat getirilen kritik alt yapı sistemlerine yapılan siber saldırılar, fiziksel ve kinetik anlamda meşru müdafaa kapsamında karşı saldırı yapmanın önünü açacaktır (Yayla, 2013: 214). Bu yaklaşıma karşı, devletin önemli ve esas altyapılarının ne olduğu konusunda tartışma yaşanabileceği ve dolayısıyla belirsizlik olduğu eleştirileri yöneltilmektedir (Foltz, 2012: 11).

#### 2. Vasıta Temelli Yaklaşım

Yukarıda açıklanan silahın niteliğinden bağımsız olarak kuvvet kullanımının yasaklanmış olduğu görüşünün yanında, siber saldırıların klasik anlamda silah kullanılmadığı için silahlı saldırı kapsamında değerlendirilmeyeceği; *Nikaragua* davasında benimsenen yeterli ağırlık (*sufficient gravity*) ölçütüne ulaşırsa silahlı saldırı olarak değerlendirilmesi mümkün olacağı savunulmaktadır (Yayla, 2013: 212, 213).

Vasıta temelli yaklaşımın sıkı sıkıya benimsenmesi sonucunda, siber araçlar geleneksel silahlı güçlerin özelliklerini taşımadığından barışı ciddi ölçüde zedeleyen siber operasyonların kuvvet kullanımı olarak nitelendirilmemesi söz konusu olabilir (Foltz, 2012: 9). Bununla birlikte, doğru komutla elektronik sinyallerin bomba, mermi, füze ve diğer geleneksel silahlar gibi kullanılması söz konusu olmaktadır (Delibasis, 2006: 8). Çoğunluk görüş, geniş çapta düzeni bozacağı endişesiyle vasıta temelli yaklaşımın katı şekilde uygulanmaması

gerektiğini düşünmektedir (Foltz, 2012: 9). Bunun sonucunda uluslararası toplum siber operasyonların gerçek sonuçlarıyla ilgilenmektedir (Delibasis, 2006: 8). Dolayısıyla etki temelli yaklaşımın ağırlık kazandığını söylememiz mümkündür.

## 3. Etki Temelli Yaklaşım

Etki temelli yaklaşıma göre kuvvet kullanımı olup olmadığını belirlemek için siber operasyonların doğurduğu sonuçların dikkate alınması gerekmektedir. Siber operasyonun tek başına egemenliğin ihlali olarak görülmemesi gerektiği; ölüm veya fiziksel zarara neden olmayan operasyonların silahlı saldırı boyutuna ulaşmayacağı ileri sürülmektedir (Lewis, 2010: 2; Güreşçi, 2019: 87). Etki temelli yaklaşımda mevki, etkiler, kasıt gibi birçok unsur önem kazanmaktadır. Nükleer santralın patlamasına yol açan operasyonlar, yoğun nüfuslu bölgeye yakın barajın açılarak zarara neden olunması, hava trafiğini etkileyerek kazalara neden olunması en yaygın örnekler olarak verilmektedir. Fiziksel etkileri bu boyuta oluşan eylemlerin kuvvet kullanımı olarak nitelendirilmesi oldukça doğaldır (Koh, 2012: 4).

Bununla birlikte, bazı gri alanlar da bulunmaktadır. Birçok siber operasyon esas olarak ekonomiyi hedef almakta ve oldukça ağır sonuçları ortaya çıkmaktadır. Etki temelli yaklaşımla bu tür siber operasyonların kuvvet kullanımı olarak nitelendirilmesinin önü açılabilmektedir. Dolayısıyla bu yaklaşım ekonomik zorlamayı kuvvet kullanımı olarak değerlendirmeyen geleneksel yoruma uygun olmayacağından eleştirilmektedir (Hoisungton, 2009: 449).

Diğer kriterler arasında en çok benimsenen yöntemin etki temelli yaklaşım olduğunu belirtmekle birlikte siber operasyonlar ele alınırken her bir unsurun ayrıca değerlendirilmesinin önem arz ettiği kanısındayız. Bu bağlamda Tallinn Rehberi ve aşağıda açıklanacak olan Schmitt kriterleri – tahdidi (*exhaustive*) olmasa da yol gösterici olmaktadır.

## 4. Siber Uzayda Kuvvet Kullanılıp Kullanılmadığını Ortaya Koyan Tallinn Rehberi'nin Değerlendirilmesi

Tallinn Rehberi, siber uzayda uluslararası hukuk ilkelerinin uygulanabileceğini göstermekte ve var olan hukuk kurallarının nasıl uyarlanabileceğini yorumlamaktadır. Tallinn ilkeleri *jus ad bellum* ilkelerinin kıyasen uygulanabileceğini vurgulamakta, kuvvet kullanma yasağının siber uzayda da geçerliliğini koruduğunu belirtmektedir (Tallinn Rehberi, 2013: 5).

Tallinn kriterleri de kuvvet kullanma ve silahlı saldırı fiillerinin farkına dikkat çekmektedir (Tallinn Rehberi, 2013: Kural 11, Yorum 11). Siber saldırının silahlı saldırı düzeyinde olup olmadığı ölçü ve etkisine göre değerlendirilecektir (Tallinn

Rehberi, 2013: Kural 13). Kişilerin ölümüne ya da yaralanmasına yol açan veya maddi zarar veren kuvvet kullanımı silahlı saldırı eşiğine ulaşmaktadır. Bununla birlikte istihbarat toplanması, siber hırsızlık, hayati önem taşımayan sistemlere kısa veya dönemsel saldırıların silahlı saldırı olarak nitelendirilemeyeceği belirtilmiştir (Tallinn Rehberi, 2013: Kural 13, Yorum 6). Devletin önemli ve esas altyapılarına yönelik tamamen yok edici nitelikte olmasa da ağır sonuçlar doğuran siber eylemlerin de silahlı saldırı düzeyinde olduğu düşünülmektedir (Tallinn Rehberi, 2013: Kural 13, Yorum 9). Dolayısıyla etki temelli ve hedef temelli yaklaşımın birlikte ele alındığı görülmektedir.

Belçika saldırısında olduğu gibi doğrudan fiziksel zarara neden olmayıp bireylerin pandemi sırasında aşıya erişimlerinin engellenmesi neticesinde dolaylı olarak birçok kişinin sağlık hakkına müdahale edildiği durumlarda bunun silahlı saldırı olup olmayacağına etki temelli yaklaşımla kesin bir cevap vermek mümkün gözükmemektedir. Devletin çok önemli altyapıları hedef alındığından vasıta temelli yaklaşım benimsendiğinde silahlı saldırı olarak nitelendirilmesi olasıdır. Bu noktada devletlerin pratiği ve bu saldırıları nasıl algıladıkları yönündeki açıklamalarını takip etmek gerekmektedir.

Operasyonun kuvvet kullanımı olarak nitelendirilmesi için söz konusu devlet tarafından askeri gücün kullanılmasının gerekmediği belirtilmiştir (Tallinn Rehberi, 2013: Kural 11, Yorum 4). Bu ilkenin temelleri *Nikaragua* davasına dayanmaktadır. *Nikaragua* davasında UAD başka bir devlete karşı hareket eden gerillaların sadece finanse edilmesinin kuvvet kullanma eşiğine ulaşmadığını ancak bu güçlerin silahlandırılması ve eğitilmesinin kuvvet kullanma olduğunu belirtmiştir. Bu karardan yola çıkarak Rehber, bir eylemin kuvvet kullanma olması için fiziksel sonuçlarının hemen ortaya çıkması gerekmediğini savunmaktadır. Dolayısıyla, etki temelli yaklaşımın yumuşatıldığı anlaşılmaktadır. Yine *Nikaragua* kararından yola çıkılarak, silahlı bir gruba kötü amaçlı yazılım sağlanması kuvvet kullanma olabilecekken, bu gruba sığınak sağlanmasının kuvvet kullanma olmayacağı görüşü benimsenmiştir (Tallinn Rehberi, 2013: Kural 11, Yorum 4-5).

Tallinn Rehberi, kuvvet kullanımına karar verilmesinde rehberin de editörlüğünü üstlenen, uluslararası hukuk profesörü ve NATO Siber Savunma Merkezi üyesi Prof. Michael N. Schmitt tarafından sunulan kriterlerin değerlendirilmesini önermektedir. Bu kriterler sınırlı sayıda olmayıp olaya göre göz önünde bulundurulmak üzere hazırlanmıştır. Schmitt kriterleri şu şekilde sıralanabilir: sonuçların ağırlığı, sonuçların ortaya çıkma hızı, siber operasyon ile sonuçlar arasındaki illiyet bağı, hedeflenen sistemlere yayılma düzeyi, etkilerin ölçülebilirliği, siber saldırının askeri nitelikte olup olmadığı, devletin ne derece müdahil olduğu ve eylemlerin uluslararası hukukla açıkça yasaklanıp yasaklanmadığı olarak sıralanmaktadır (Tallinn Rehberi, 2013: Kural 11, Yorum

9). Bu kriterler sınırlı sayıda olmadığından, devletler politik ortamı, saldırganın kimliği ve siber operasyon geçmişini, hedefin niteliğiyle herhangi askeri gücün ileride kullanılacağına işaret edip etmediğini de göz önünde bulundurabileceklerdir (Tallinn Rehberi, 2013: Kural 11, Yorum 10).

Sonuç itibariyle siber operasyonun kuvvet kullanımı olup olmadığı, eğer öyleyse silahlı saldırı düzeyine ulaşıp ulaşmadığının belirlenmesinde çeşitli yaklaşımlar getirilmiştir. Bu yaklaşımlardan birinin benimsenmesi doğru sonuç vermeyebilecektir. Ancak Tallinn Rehberi çeşitli yaklaşımları var olan uluslararası hukuk kuralları çerçevesinde bir potada eriterek önemli bir rehber sunmaktadır. Bu rehber devletler için yol gösterici nitelikte olup kesin sonuçlar önermediğinden siber operasyonları genel olarak sınıflandırmak yerine olay bazında değerlendirme yapılması gerekmektedir.

## III. Devletin Sorumluluğu ve Devlet Dışı Aktörlerin Faaliyetlerinden Doğan Sorumluluk

Siber saldırıların önemli bir özelliği kim tarafından yapıldığının belirlenmesinin zor olmasıdır. Çoğu zaman devlet dışı aktörlerin siber saldırıları düzenlediği bilinmektedir. Siber saldırılarda kullanılan teknoloji saldırının kaynağının ve hatta saldırının arkasındaki niyetin belirlenmesini oldukça zorlaştırmaktadır (Hoisungton, 2009: 452; Yayla, 2013: 206). Bazı durumlarda saldırıların gerçekleştiği lokasyon veya ülke belirlenebilse de bu zamana kadar hiçbir devlet siber saldırıları üstlenmemiştir. Siber operasyonlar açısından atfedilme oldukça önem arz etmektedir. Bunun sonucunda ne zaman ve hangi şartlar altında devletlerin sorumlu tutulacağı sorunu ortaya çıkmaktadır. Meşru müdafaa hakkının siber uzayda geçerli olup olmadığının belirlenebilmesi için öncelikli olarak siber saldırıyı gerçekleştiren devletin veya devlet dışı aktörlerin eylemlerinden sorumlu olacak devletin belirlenmesi önem arz etmektedir.

Eylemleri gerçekleştiren kişi ve grupların belirlenmesindeki teknik sorunlar bir kenara bırakıldığında uluslararası hukuk kurallarının devlet dışı aktörlerin eylemlerinden sorumluluğa ilişkin kuralların siber operasyonlar bakımından da uygulanabileceği savunulmaktadır (Koh, 2012: 7).

BM Anlaşması m. 2(4)'te belirtilen kuvvet kullanma yasağı genellikle bireylerden ziyade sadece devletlere uygulanmaktadır. Uluslararası Hukuk Komisyonu Devletlerin Uluslararası Hukuka Aykırı Fiillerinden Sorumluluğu başlıklı tasarıda eylem veya ihmalin devlete atfedilebildiği veya devletin uluslararası yükümlülüğünü ihlal ettiği durumlarda sorumluluğun doğacağı belirtilmektedir (International Law Commission, 2001: m.2). Metnin ikinci kısmı eylemlerin devlete atfedilebilirliğini düzenlemektedir. Devletin organlarının veya devletin organı olmasa da devletin vermiş olduğu yetkiye dayanarak hareket

edenlerin eylemlerinden devlet sorumlu tutulmaktadır (International Law Commission, 2001: m.3-4). Siber uzayda da bu ilkelerin geçerli olduğu düşünülmektedir. Devletin organlarının veya doğrudan devletin organı olmayıp devletin yetki verdiği kişilerin uluslararası hukuku ihlal eden siber eylemlerinden devletin sorumluluğu söz konusu olacaktır (Tallinn Rehberi, 2013: Kural 6, Yorum 6-8).

Devletin kendi eylemi olarak tanıdığı durumlara ek olarak, devlet dışı kişi veya gruplar devletin yönlendirmesi veya kontrolüyle hareket ediyorlarsa bu eylemler devlete atfedilmektedir (International Law Commission, 2001: m.8, 11). Devlet dışı aktörler bakımından *Nikaragua* davasında devletlerin sorumluluğu belirlenirken etkin kontrol testi (*effective control*) uygulanmıştır. Buna göre, devletin yönergesi veya yönlendirmesiyle hareket eden silahlı grupların eylemlerinden devletin sorumluluğu doğmaktadır. Bununla birlikte, organize grupların eylemlerinden sorumluluk *Tadic* davasında da ele alınmıştır (*Tadic*, 1999). Devlete doğrudan bağlı olmayan grupların eylemlerinden doğan sorumluluğun belirlenmesinde etkin kontrol yerine devletin gruplar üzerinde genel kontrolü (*overall control test*) olup olmadığının değerlendirilmesi gerektiği belirtilmiştir. Bu teste göre devletin finansal, lojistik, diğer yardım ve destekleri dışında eylemlerin planlanması ve gözetilmesinde rol oynaması aranmaktadır. Böylelikle organize gruplar açısından daha geniş kapsamlı bir test benimsenmektedir. *Tadic* kararına göre organize olmayan grupların veya bireylerin eylemlerinden devletin sorumluluğu ise *Nikaragua* kararında belirtilen etkin kontrol testiyle belirlenmelidir.

Devlet dışı aktörlerin siber eylemlerinden sorumluluk bağlamında, bu kişi ve gruplar devletin yönlendirmesi veya kontrolüyle hareket ediliyorsa devletin sorumluluğunun doğacağı kabul edilmektedir. Bu konuda *Nikaragua* ve *Tadic* kararlarında benimsene testlerin kabul edilmesi gerektiği savunulmaktadır (Tallinn Rehberi, 2013: Kural 6, Yorum 10). Sorumluluğun kişilerin bulunduğu ülkeden bağımsız şekilde belirlenmesi ileri sürülmektedir. Bu durumda A ülkesinde bulunan kişilerin, B ülkesindeki bilgisayarları kullanarak D devletinden aldığı yönergelerle C ülkesine siber saldırıda bulunması halinde sorumluluk D devletine ait olacaktır (Tallinn Rehberi, 2013: Kural 6, Yorum 12). Bunlara ek olarak, devlet dışı aktörlerin eylemleri devlete atfedilemese bile devletin bu aktörlerle iş birliği yapması başlı başına uluslararası hukukun ihlali olabilecektir. Örneğin, B devletine karşı kendi başına ayaklanan gruba siber saldırı için destek veren A ülkesi doğrudan bu grubun eylemlerinden sorumlu olmamakla birlikte, *Nikaragua* kararından yola çıkıldığında, sırf yardım etmiş olması uluslararası hukukun ihlali anlamına gelebilecektir (Tallinn Rehberi, 2013: Kural 6, Yorum 13).

Bu kurallardan yola çıkıldığında, birey ve gruplar üzerinde devletin benimsenen testler çerçevesinde belirli düzeyde kontrolünün olduğu belirlendiği takdirde o devletin siber operasyonlar bakımından sorumlu olacağını söylememiz mümkündür (Koh, 2012: 7). Bununla birlikte teknik olarak siber eylemin kaynağının ve aktörlerinin belirlenmesindeki zorluk bu kuralların uygulanmasının önünde önemli bir engel teşkil ettiği düşünülebilir. Ancak, Birleşik Krallık, ABD, Danimarka ve Avustralya NotPetya saldırısını Rus hükümetine atfederken; Kanada sadece Rusya kaynaklı olduğunu belirtmiştir (Foreign and Commonwealth Office, National Cybersecurity Centre ve Wimbledon, 2018; Communications and Security Establishment, 2018). ABD WannaCry saldırısını Kuzey Kore'ye atfetmiştir (Bossert, 2017). AB üye devletlerinden bazıları ve Birleşik Krallık başta olmak üzere devletlerin yeterli siber istihbarat alt yapısının olduğu; siber saldırıların atfedilmesinin mümkün olduğu belirtilmektedir (Ivan, 2019).

## IV. Kuvvete Başvurma Yasağının İstisnalarının Siber Uzayda Geçerliliği

Kuvvete başvurma yasağının istisnası olarak devletlerin meşru müdafaa hakkı gündeme gelmektedir. Meşru müdafaa hakkı örf ve adet kuralı olup, BM Anlaşması m.51'de de yer almaktadır (Sur, 2020: 294). BM Anlaşması m.51, devletlerin silahlı saldırıya hedef olmaları halinde Güvenlik Konseyi devreye girinceye dek bireysel ya da ortak doğal meşru savunma hakkına sahip olduğunu belirtmektedir. Dolaysıyla barış ve güvenliği tehdit eden silahlı saldırı söz konusu ise meşru müdafaa hakkı söz konusu olacaktır. Silahlı saldırının niteliği ise bu hakkın kullanılması açısından önem arz etmemektedir. Siber uzayda da devletlerin egemenlik iddialarının devam ettiği görülmekte, bu nedenle tehdit edildiklerinde doğal meşru müdafaa hakkına dayanarak karşılık verebilecekleri savunulmaktadır (Lotrointe, 2012: 839). Bu durumda siber eylemlerin silahlı saldırı düzeyinde olması gerektiği açıktır. Siber eylem kuvvet kullanımı olarak nitelendirilse bile silahlı saldırı düzeyine ulaşmıyorsa meşru müdafaa hakkını doğurmayacaktır (Tallinn Rehberi, 2013: Kural 11, Yorum 11). Silahlı saldırı olup olmadığı ise, eylemin ölçü ve etkisine göre belirlenecektir (Tallinn Rehberi, 2013: Kural 13).

Siber eylemler açısından silahlı saldırının kapsamına yönelik tartışmalar netlik kazanmamıştır. Bununla birlikte, insanların ölümü, yaralanması veya maddi zararların açığa çıkması durumunda siber eylemlerin silahlı saldırı olarak değerlendirileceği; bununla birlikte siber hırsızlık, verilerin ele geçirilmesi, hayati önem taşımayan siber sistemlere zarar verilmesinin silahlı saldırı olmadığı konusunda görüş birliği bulunmaktadır (Tallinn Rehberi, 2013: Kural 13, Yorum 6). Silahlı saldırının belirlenmesinde fiziksel etkiler en önemli kriter olarak karşımıza çıkmaktadır. Hedef temelli olarak bakıldığında kritik milli altyapılar

açısından meşru müdafaa hakkının olması gerektiğini savunanlar bulunmaktadır (Jensen, 2002; Tallinn Rehberi, 2013: Kural 13, Yorum 9).

Devlete atfedilen, devlet dışı aktörlerin eylemleri açısından ve devletin sorumluluğunun doğduğu diğer durumlarda da meşru müdafaa hakkı söz konusu olacaktır. Devletin doğrudan kontrolüyle hareket etmeyen aktörlerin siber saldırılarına karşı meşru müdafaa hakkının doğup doğmadığı tartışmalıdır. Bu noktada hakkın doğacağını iddia edenler ABD'nin 9/11 olayları sonrasında El-Kaideye karşı bu hakkı ileri sürmesi neticesinde gelişen devlet pratiğinin siber uzaya da uygulanabileceğini savunmaktadır. Bu konunun netleşmesi için daha fazla devlet pratiğine ihtiyaç duyulduğu aşikardır.

Siber saldırılara karşı kullanılacak meşru müdafaa hakkının gerekli ve orantılı olması gerekmektedir. Gereklilik, silahlı saldırıya karşı sadece kuvvet kullanmanın mümkün olduğu durumları değil, diğer yöntemlerin yeterli olmayacağı durumlarda da kuvvet kullanımını kapsamaktadır. Bununla birlikte, siber saldırılara karşı pasif şekilde (örneğin, güvenlik kalkanı koymak) veya kuvvet kullanma düzeyine gelmeyecek karşı siber eylemlerde bulunmak mümkünse hem siber hem kinetik kuvvet kullanımı gerekli olmadığından hukuka aykırı olacaktır (Tallinn Rehberi, 2013: Kural 14, Yorum 3). Verilecek karşılık aynı zamanda orantılı olmadır. Saldırıya karşı kullanılacak gücün düzeyi, kapsamı, yoğunluğu ve süresi önem kazanmaktadır. Bununla birlikte, siber saldırıya sadece siber yöntemlerle karşılık verilmesini zorunlu kılmadığı; eğer gerekliyse silahlı saldırıyla karşılık verilebileceği belirtilmektedir (Tallinn Rehberi, 2013: Kural 14, Yorum 5). Bu görüş oldukça tehlikeli sonuçlara yol açabilecektir. Keza bu görüşe karşı çıkılmakta ve hatta siber yöntemlerden bazılarının kullanılmaması gerektiği yönünde uluslararası prensipler geliştirilmektedir. Bunlardan biri Paris Çağrısı, özel sektör dahil olmak üzere devlet dışı aktörlerin kendilerinin veya diğer devlet dışı aktörlerin amaçlarına uygun şekilde aktif savunma tekniği olan geri saldırıda (*hack-back*) bulunmasının önüne geçilmesi gerektiğini belirtmektedir (Paris Call, 2018). Devletlerin ve özel kişilerin bu prensibi uygulamaya geçmesi için ilkenin detaylandırılması ve kapsamının netleştirilmesinin gerektiği; bu yönde çalışmaların olacağı dile getirilmektedir (Paris Call, 2018). Bu bağlamda, her ne kadar devletlerin meşru müdafaa hakkına yönelik olup olmadığı konusunda açıklık bulunmasa da geri saldırı gibi siber yöntemlerle karşılık verilmenin önüne geçilmesinin istenmesi, fiziksel kuvvet kullanımının da kapsam dışında bırakılacağına işaret etmektedir.

Meşru müdafaa için aranan bir diğer unsur siber saldırının gerçeklemiş olmasıdır (BM Anlaşması, 1945: m.51). Buna ek olarak, saldırının gerçekleşmek üzere olması yani yakın olması durumunda da hakkın kullanılabileceğine yönelik önleyici meşru müdafaa tartışmaları siber uzayda da devam etmektedir. İstisnanın sadece silahlı saldırı durumunda geçerli olduğunu savunanlara karşı olası bir silahlı

saldırıyı önlemek için meşru müdafaanın söz konusu olacağı görüşünü benimseyenler bulunmaktadır. Caroline testinin uygulanması neticesinde, önleyici meşru müdafaanın halihazırda başlamış bir silahlı saldırı açısından söz konusu olabileceği, bu durum siber saldırılar açısından da geçerliliğini koruyacağı ileri sürülmektedir (Delibasis, 2006: 11). Bu konuda var olan kuralların yetersiz olduğu söylenebilir. Bu nedenle madde 2(4)'ün daha geniş kapsamlı yorumlanması veya tehdide verilecek cevap konusunda yeni yöntemler geliştirilmesi gerektiği belirtilmektedir (Hoisungton, 2009: 441). Özellikle kritik altyapıyı hedef alan siber saldırılara karşı devletin doğal meşru müdafaa ve hatta önleyici meşru müdafaa hakkını tanıyacak şekilde hukuk kurallarının gelişmesi gerektiği savunulmaktadır (Hoisungton, 2009: 453).

ABD ve Çin'in açıklamaları ışığında devletlerin siber saldırılara karşı meşru müdafaa haklarını savunduklarını söylememiz mümkündür. Meşru müdafaanın şekli açısından da ABD'nin yaklaşımı önem arz etmektedir. En son silahlı kuvvete başvuracağı belirtilse de bunun da bir seçenek olduğu gözden kaçırılmamalıdır.

Geleneksel silahlı saldırılar bakımından hala netliğe kavuşmamış bu koşulların siber saldırılara uyarlanması oldukça güçtür. Gereklilik ve yakınlık şartlarının siber saldırılara uyarlanması, orantılılık şartına göre daha kolay olacaktır (Delibasis, 2006: 12). Ancak sınırları iyi belirlenmezse siber saldırılara karşı sahada kinetik olarak silahlarla karşılık verilmesi söz konusu olabilecektir. Siber saldırılar neticesinde insanların öldüğü, yaralandığı, çok önemli fiziksel zararların meydana geldiği durumların silahlı saldırı olarak algılanması ve buna karşı gerek siber gerek orantılı kinetik yöntemlerle meşru müdafaa hakkının kullanılması hukuka uygun gözükmektedir. Siber saldırının kesin bir şekilde silahlı saldırı etkisi yaratmadığı ve bu şekilde nitelendirilmesinin zor olduğu durumlarda ise meşru müdafaa hakkının ardına sığınılarak geri dönülemez sonuçlara neden olunmasının önüne geçilmesi adına siber saldırılarda meşru müdafaa hakkının kullanılmasına temkinli yaklaşılması gerekmektedir.

## Sonuç

Devletlerin siber uzayda da fiziksel olarak sınırlarıyla bağlantılı olacak şekilde egemenlik hakkı olduğu kabul edilmekte; devletler bu şekilde hareket etmektedir. Siber uzayın da uluslararası hukuk kurallarına tabii olduğu ağırlıklı olarak kabul edilmektedir. Devletlerin egemenliğini ve uluslararası barış ve güvenliği tehdit ettiği düşünülen siber saldırılar günümüzde yeni bir tür kuvvet kullanma yöntemi olarak karşımıza çıkmaktadır. Hangi siber eylemlerin kuvvet kullanımı niteliğinde olduğunun belirlenmesinde çeşitli yaklaşımlar benimsenmiştir. Bunlar arasında en doğru sonuçları Tallinn Rehberi'nde karma şekilde benimsenen ilkelerin olduğunu söylememiz mümkündür. Bu ilkeler doğrultusunda siber saldırının

etkileri silahlı saldırının doğuracağı şekildeyse ve devletin kritik ulusal altyapılarına müdahale ediyorsa silahlı saldırı düzeyinde olduğu kabul edilebilecektir.

Siber eylemleri silahlı saldırı olarak belirlemek devletlerin kuvvet kullanmanın istisnası olan meşru müdafaa haklarını kullanmalarının önünü açmaktadır. Silahlı saldırı düzeyindeki siber operasyonun mağduru olan devletin doğal hakkı olan meşru müdafaaya; hatta bazı düşünürler tarafından önleyici müdafaaya da başvurabileceği kabul edilmektir. Bu durumda meşru müdafaanın var olan uluslararası hukuk kuralları uyarınca gerekli, yakın tehdide karşı ve orantılı olması gerekmektedir. Silahlı saldırı düzeyinde olan siber saldırıya karşı benimsenecek yöntem siber olabileceği gibi geleneksel kuvvet kullanma şeklinde de gerçekleşebileceği düşünülmektedir. Bu noktada orantılılık ilkesinin katı bir şekilde uygulanması hayati önem taşıyacaktır. Meşru müdafaanın kime yönlendirileceği de önem arz etmektedir; zira Siber saldırıların çoğunlukla devlet dışı aktörler tarafından gerçekleştirildiği görülmektedir. Devletin sorumluluğuna ilişkin kurallar burada da uygulama alanı bulmaktadır. Ancak saldırının kaynağını belirlemek teknik olarak zor olduğundan meşru müdafaanın yönlendirileceği devletin (veya devlet dışı aktöre karşı yapılabileceği kabul edildiği takdirde bu aktörün) belirlenmesi sorun çıkarmaktadır.

Sonuç itibariyle, siber uzayda uluslararası hukuk kuralları geçerliliğini korumakta ve kıyasen uygulandığında belli bir noktaya kadar sorunlara ışık tutmaktadır. Bununla birlikte hem teknik olarak yetersizlikler hem de süregelen uluslararası hukuk tartışmalarının netlik kazanmamış olması nedeniyle gri alanlar bulunmaktadır. Bu alanlar uluslararası düzenlemelerle belirlilik kazanana kadar, siber eylemlerin objektif şekilde silahlı saldırı olarak nitelendirilebileceği ölüm, fiziksel zarar ve kritik altyapıların zarar görmesi gibi durumlarla sınırlı şekilde; siber eylemi gerçekleştiren devletin ve devlet dışı aktörün eylemlerinin atfedilebildiği devletin belirlenebildiği durumda orantılılık ilkesi katı bir şekilde gözetilerek ihtiyatlı şekilde uygulanması gerektiği kanaatindeyiz.

## Kaynakça

BBC (2015), "Sony cyber-attack: North Korea faces new US sanctions", https://www.bbc.co.uk/news/world-us-canada-30661973 (Son Erişim: 8.09.2021).

BM, Birleşmiş Milletler Anlaşması, 24 Ekim 1945, 1 UNTS XVI, https://inhak.adalet.gov.tr/Resimler/SayfaDokuman/2212020141836bm_01.pdf (Son Erişim: 8.05.2021) (BM Anlaşması).

BM Genel Kurulu, 3314 (XXIX) sayılı karar, 1974, (Definition of Aggression), http://hrlibrary.umn.edu/instree/GAres3314.html (Son Erişim: 7.05.2021).

Boer, Lianne J. M. (2013), "Restating the Law as It Is: On the Tallinn Manual and the Use of Force in Cyberspace" *Amsterdam Law Forum***,** 5: 4–18.

Bossert, Thomas P. (2017), "It's Official: North Korea Is Behind WannaCry", https://www.wsj.com/articles/its-official-north-korea-is-behind-wannacry-1513642537 (Son Erişim: 8.09.2021).

Brotman, Stuart N. (2015), "Multistakeholder Internet governance: A pathway completed, the road ahead", Center for Technology Innovation at Brookings, https://www.brookings.edu/wp-content/uploads/2016/06/multistakeholder-1.pdf (Son Erişim: 8.05.2021).

Christakis, Théodore (2021), "The Hague Academy of International Law Online Summer Courses: The International Law of Cybersecurity", https://www.hagueacademy.nl/wp-content/uploads/2021-ONLINE-PROG RAMME-1.pdf (Son Erişim: 23.07.2021).

Communications Security Establishment (2018), "CSE Statement on the NotPetya Malware", https://cse-cst.gc.ca/en/information-and-resources/news/cse-statement-notpetya-malware (Son Erişim: 8.09.2021).

Corera, Gordon (2021), "Iran nuclear attack: Mystery surrounds nuclear sabotage at Natanz", BBC News, 12.04.2021, https://www.bbc.com/news/world-middle-east-56722181 (Son Erişim: 7.05.2021).

Delibasis, Dimitrios (2006), "State Use of Force in Cyberspace for Self-Defence: A New Challenge for a New Century", *Peace Conflict and Development: An Interdisciplinary Journal*, 8: 1–50.

Euronews (2021), "Belgium's parliament and universities hit by cyber attack", 5.05.2021, https://www.euronews.com/2021/05/05/belgium-s-parliament-and-universities-hit-by-cyber-attack (Son Erişim: 7.05.2021).

European Commission (2017), "EU cybersecurity initiatives: working towards more secure environment", https://ec.europa.eu/information_society/newsroom/image/document/2017-3/factsheet_cybersecurity_update_january_2017_41543.pdf (Son Erişim: 8.09.2021).

Fildes, Jonathan (2010), "Stuxnet worm 'targeted high-value Iranian assets'", BBC News, 23.09.2010, https://www.bbc.com/news/technology-11388018 (Son Erişim: 7.05.2021).

Foltz, Andrew C. (2012), "Stuxnet, 'Schmitt Analysis,' and the Cyber 'Use of Force' Debate", *Air War College Air University,* Vol. 67.

Foreign & Commonwealth Office, National Cyber Security Centre, and Lord Ahmad of Wimbledon (2018), "Foreign Office Minister condemns Russia for NotPetya attacks" https://www.gov.uk/government/news/foreign-office-minister-condemns-russia-for-notpetya-attacks (Son Erişim: 8.09.2021).

Franzese, Patrick W. (2009), "Sovereignty in Cyberspace: Can It Exist?", *Air Force Law Review*, 64.

Goodrich, Hambro ve Simons (1969), *Charter of the United Nations: Commentary and Documents* (New York, Columbia University Press).

Güreşçi, Ramazan (2019), "Siber Saldırıların Uluslararası Hukuktaki Güç Kullanımı Kapsamında Değerlendirmesi", *Savunma Bilimleri Dergisi*, 18: 75–98.

Hoisungton, Matthew (2009), "Cyberwarfare and the Use of Force Giving Rise to the Right of Self-Defense", *Boston College International and Comparative Law Review*, 32: 439–455.

International Court of Justice (ICJ), Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion of 8 July 1996 (*Nükleer Silahlar*).

International Court of Justice (ICJ), Nicaragua v. United States of America, Military and Paramilitary Activities, Judgement of 27 June 1986 (UAD, *Nikaragua v ABD*).

International Criminal Tribunal for the former Yugoslavia (ICTY), Prosecutor v. Dusko Tadic (Appeal Judgement), IT-94-1-A, ,15 July 1999 (*Tadic*).

International Law Commission, Responsibility of States for Internationally Wrongful Acts, 2001, https://legal.un.org/ilc/texts/instruments/english/draft_articles/9_6_2001.pdf (Son Erişim: 8.05.2021).

Ivan, Paul (2019), "Responding to Cyberattacks: Prospects for the EU Cyber Diplomacy Toolbox", https://www.epc.eu/content/PDF/2019/pub_9081_responding_cyberattacks.pdf (Son Erişim: 8.09.2021).

Jensen, Eric Talbot (2002), "Computer Attacks on Critical National Infrastructure: A Use of Force Invoking the Right of Self Defense" *Stanford Journal of International Law*, 38:207.

Koh, Harold Hongju (2012), "International Law in Cyberspace", *Harvard International Law Journal*, 5: 1–12.

Lewis, James A. (2010), "A Note on the Laws of War in Cyberspace", *Center for Strategic International Studies*.

Lotrointe, Catherine (2012), "State Sovereignity and Self-Defense in Cyberspace: A Normative Framework for Balancing Legal Rights" *Emory International Law Review*, 26: 825–919.

Ministry of Foreign Affairs of the Republic of China (2017), "International Strategy on Cooperation in Cyberspace (Siber Uzayda İşbirliği Hakkında Uluslararası Strateji)", https://www.fmprc.gov.cn/mfa_eng/wjb_663304/zzjg_663340/jks_665232/kjlc_665236/qtwt_665250/t1442390.shtml (Son Erişim: 7.05.2021).

Moret, Erica ve Pawlak, Patryk (2017), "The EU Cyber Diplomacy Toolbox: towards a cyber sanctions regime?", https://www.iss.europa.eu/sites/default/ files/EUISS Files/Brief%2024%20Cyber%20sanctions.pdf (Son Erişim: 8.09.2021).

Mueller, Milton (2018), "Sovereignty and Cyberspace: Institutions and Internet Governance" *Essay from the Lecture at University of Indiana October 3rd 2018*: 1–8.

Paris Call (2018), "The Call and the 9 Principles", https://pariscall.international/en/principles (Son Erişim 13 Eylül 2021).

Quach, Katyana (2021), "Belgian parliament halts China Uyghur 'genocide' debate after DDoS smashes ISP offline", The Register, 5.05.2021, https://www.theregister.com/2021/05/05/belnet_belgium_ddos/ (Son Erişim: 7.05.2021).

Schmitt, Michael N. (2012), "International Law in Cyberspace: The Koh Speech and Tallinn Manual Juxtaposed", *Harvard International Law Journal***,** 54: 13–37.

Siber Savaşlara Uygulanacak Uluslararası Hukuk Hakkında Tallinn Rehberi (*Tallinn Manual on the International Law Applicable to Cyber Warfare*) (2013), Cambridge University Press (Tallinn Rehberi).

Siber Savaşlara Uygulanacak Uluslararası Hukuk Hakkında Tallinn Rehberi 2.0 (*Tallinn Manual 2.0 on the International Law Applicable to Cyber Warfare*) (2017), Cambridge University Press (Tallinn Rehberi 2.0).

Sur, Melda (2020), *Uluslararası Hukukun Esasları* (İstanbul: Beta).

White House (2011), "International Strategy for Cyberspace", https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf (Son Erişim: 8.05.2021).

Yayla, Mehmet (2013), "Uluslararası Hukukta Siber Saldırılara Karşı Kuvvet Kullanma", *Türkiye Barolar Birliği Dergisi*, 107: 199–220.

# The Turkish Yearbook of International Relations

## Dizinler

Her veri tabanından dergilerin dizin güncelliği kontrol edilmelidir. DergiPark sorumluluk almamaktadır.

### Diğer Dizinler

- International Political Science Abstracts SAGE
- International Bibliography of the Social Sciences (IBSS) ProQuest
- Index Islamicus
- Index Copernicus
- ASOS Index


- Dergi Ana Sayfası
- Hakkında
- Amaç ve Kapsam
- Makale Gönder
- Dergi Kurulları
- İstatistikler
- Yazım Kuralları
- Etik İlkeler ve Yayın Politikası
- Ücret Politikası
- Dizinler
- Arşiv
- İletişim
- Danışma Kurulu
- Yayın Etiği