*Savunma Bilimleri Dergisi*
*The Journal of Defense Sciences*
Mayıs/May 2019, Cilt/Volume 18, Sayı/Issue 1.
ISSN (Basılı) : 1303-6831 ISSN (Online): 2148-1776

# Siber Saldırıların Uluslararası Hukuktaki Güç Kullanımı Kapsamında Değerlendirmesi

Ramazan GÜREŞCİ*

***Öz***

*Geçtiğimiz son yirmi yılda teknoloji kullanımının olağanüstü hızda artmasıyla birlikte ortaya çıkan sanal alanda, toplumlar ve hükümetler siber tehditler karşısında saldırıya duyarlı hedefler olmaya başlamışlardır. Siber saldırıların, klasik silah gücünün verdiği zarara eşdeğer birçok zararı verebilecek kapasiteye ulaşmasıyla nükleer santraller, askerî sistemler veya petrol boru hatları gibi sayısız ulusal kritik altyapı hedef hâline gelmiştir. Yaşanan gelişmeler klasik anlamdaki tehdit algısına yönelik olarak açık temel bir paradigma değişimini yansıttığı için uluslararası hukuk bu durumu dikkate almak zorunda kalmıştır. Uluslararası hukuk açısından temel sorun, siber saldırıların bir takım hak ve yükümlülükler bağlamında nasıl düzenleneceğidir. İlgili makalede siber saldırılar, uluslararası hukukta güç kullanımı çerçevesinde değerlendirilecektir. Uluslararası hukukta güç kullanımı devletlerin hangi durumlarda kuvvete meşru olarak başvurması veya yasaklanması durumunu düzenlemektedir. Uluslararası hukukta esas olarak, egemen devletin diğerinin ülke bütünlüğüne ve siyasi bağımsızlığına karşı kuvvet kullanması bazı istisnalar haricinde kesin olarak BM şartnamesiyle yasaklanmıştır. Bu bakımdan, klasik kuvvet kullanma ile aynı sonuçları doğurabilecek siber saldırılar, diğer koşulları sağlaması durumunda aynı şekilde uluslararası hukukun mevcut kuralları kapsamında değerlendirilebilir. Ancak, ilgili kuralların siber tehditlere yönelik ihtiyacı karşıladığı noktasında yetersiz olduğu da bilinen bir gerçekliktir. Tarihte nükleer veya kimyasal silahlar gibi yeni silahların kullanımına ilişkin uluslararası hukuk bir takım hak ve yükümlülükler getirmiştir. Siber saldırıların konvansiyonel silahlarla kıyas yapılmasının olası*

* Arş.Gör., Kütahya Dumlupınar Üniversitesi, İktisadi ve İdari Bilimler Fakültesi, Siyaset Bilimi ve Uluslararası İlişkiler Bölümü, Devletler Hukuku Kürsüsü, ramazan.guresci@dpu.edu.tr

Geliş Tarihi/Received:08.08.2018
Kabul Tarihi/Accepted:06.11.2018
Araştırma Makalesi/Research Article

*olmadığı ya da abartı olacağı iddia edilebilir, ancak her ikisinin de aynı etkiyi doğurma kapasitesine ulaşması bu iddiaları zayıflatmaktadır. Siber saldırılar için işleyen mevcut kurallardan yola çıkarak bir takım yeni hukuki düzenlemelerin gelmesi gerekli gözükmektedir. Çalışmanın temel amacı uluslararası hukuktaki kuvvet kullanımına ilişkin kuralların siber saldırılara yönelik olarak uygulanmasında ihtiyaçları ne derece karşıladığını ortaya koyarak çözüm yolları üretmeye çalışmaktır.*

***Anahtar Kelimeler:*** *Siber Savaş, Kuvvet Kullanımı, Uluslararası Hukuk, Jus ad Bellum.*

# The Evaluation of Cyber Attacks with Regards to the Use of Force in International Law

**Abstract**

*In the last two decades, the usage of technology has dramatically increased. This has created a new domain where both governments and civilians have become vulnerable against serious cyber threats. These threats are able to induce myriad consequences, including physical damage as the traditional weapons do. In this context, a substantial part of national critical infrastructure, most particularly, nuclear plants, military systems or pipelines have become targets. Hence, it is a clear paradigm shift that traditional understanding of the threat has fundamentally changed and international law must take the new threats into account. The main question for international law is how to govern or deal with these issues. This study particularly examines the applicability of the use of force in international law to cyber warfare. The use of force in international law regulates when states are able to legally resort to force. To resort to force against another state's territorial integrity and political independence, apart from exceptions, is strictly restrained in the UN Charter. In this context, it is fair to say that cyber-attacks that led to same kinetic consequences as use of force should be similarly treated in international law. However, it is evident that the existing regulation and practices are not adequate for the application to cyber warfare. The historical experience illustrates that novel weapon systems should be restricted by international law as in chemical and nuclear weapons. It can be asserted that cyber capacity cannot be compared to the weapon systems, but similar destructive consequences capacity like any other*

*weapons weakens these claim. A cyber-specific agreements should be achieved by considering international customary law as a starting point. The main consideration of the study is to raise whether the existing regulations in use of force are enough to meet the needs for cyber warfare and attempts to develop possible solutions against the legal ambiguity.*
***Keywords:*** *Cyber Warfare, Use of Force, International Law, Jus ad Bellum.*

## Giriş

1990'lardan itibaren teknolojide yaşanan gelişmelerin, başta bilgi ve iletişim alanı olmak üzere, teknolojinin ve toplumların gelişip dönüşmesinde ciddi roller üstlendiği açıktır. Kamu veya özel sektör ayrımı yapmaksızın enerji, su kaynakları, sağlık, askerî veya haberleşme gibi birçok kritik altyapı sistemlerinde teknolojinin etkin olarak kullanımı son çeyrek yüzyılda olağanüstü hızda artarak yaygınlaşmıştır. Rekabet, verimlilik, akademik çalışma, askerî güç, şeffaf yönetim veya ifade özgürlüğü gibi önemli konularda birçok avantaj sağlayan dijitalleşme, aynı zamanda siber operasyonlar vasıtasıyla sayısız güvenlik zafiyetini beraberinde getirmektedir.

Siber operasyonlar, devletin ve özel sektörün mahrem bilgilerinin ele geçirilmesi, askerî komuta-kontrol sistemlerinin devre dışı bırakılması veya manipüle edilmesi, merkez bankası gibi kritik ekonomik altyapıların çökertilmesi; ulaşım, elektrik, su, haberleşme gibi temel ihtiyaçlardan mahrum bırakılıp toplumsal ayaklanmaların desteklenmesi gibi sayısız ekonomik, politik ve sosyal musibetlere neden olabilmektedir. Bunun yanında sınır tanımaksızın, oldukça ucuz maliyetle ve asimetrik fizikî zarar verebilme kapasitesine de ulaşan siber saldırılar, kritik eşiği aşması neticesinde uluslararası güvenlik ve hukuk uzmanlarının yakın ilgisine mazhar olmuştur. Hâlihazırda uluslararası gündemi oldukça meşgul eden siber konusunun, kısa vadede uluslararası gündemin daha yukarı sıralarını işgal edeceğini öngörmek güç değildir. Bütün bunlar cereyan ederken, en temel tartışmalardan biri de siber operasyonların uluslararası hukuk bağlamında ne şekilde ele alınacağı konusudur.

Doktrindeki tartışma temel olarak iki ana eksen üzerinde devam etmektedir: İlk olarak, mevcut uluslararası hukuk kurallarının benzeşim (analogy) yoluyla siber operasyonları kapsayabileceği ve böylece herhangi bir düzenleme yapmaya gerek kalmaksızın uluslararası hukuk sınırları içerisinde kalarak, olası bir hukuk

boşluğunu dolduracağı savunulmaktadır (1). Buna karşılık diğer görüş ise, mevcut uluslararası hukuk rejiminin konvansiyonel tehditlere cevap verecek şekilde tasarlandığını, dolayısıyla siber saldırlar karşısında bir anlam ifade etmediğini, ifade etse dahi yetersiz kaldığından yola çıkarak siber alanın bir kargaşa ortamı olarak kaldığını savunmaktadır. Çözüm olarak ise, konuya ilişkin çok taraflı özel düzenlemeler yapılması gerektiğini, aksi takdirde hâlihazırdaki hukuki boşluğun devam edeceğini savunmaktadır (2).

Uluslararası hukukta kuvvet kullanmanın siber saldırılar bağlamında ele alacağı bu çalışma iki ana bölümden oluşmaktadır. İlk bölümde, konunun bütünlüğü açısından internetin işleyiş prensiplerine ilişkin olarak temel bilgiler aktarılacaktır. İkinci bölümde ise, mevcut uluslararası hukuk kuralları çerçevesinde, kuvvet kullanımının (Jus ad Bellum) hangi durumlarda yasaklandığı veya meşru sayıldığı, uluslararası hukuk normları açısından değerlendirilerek, siber saldırılara yönelik olarak uygulanabilirliği ortaya koyulmaya çalışılacaktır. İlgili tartışmaların neticesinde bu çalışmada, mevcut hukuk mekanizmasının işletilmesinin önünde herhangi bir engel görmemekle birlikte hâlihazırdaki ve muhtemel sorunları çözme konusunda yetersiz olduğu sonucuna varılmıştır. Özellikle saldırıyı yapan kişilerin kimler olduğunu tespit noktasındaki zorluklar uluslararası iş birliğini zorunlu kılmaktadır. Bu bağlamda, hâlihazırdaki kuvvet kullanmaya ilişkin uluslararası hukuk rejiminden yola çıkarak uluslararası toplumun konuya ilişkin katılımcı bir şekilde özel düzenlemeleri hayata geçirmeleri gerekmektedir. Aksi takdirde zaman geçtikçe problem daha karmaşık hâle gelerek çözümü daha zor bir hâl alacaktır.

## İnternetin Temel Yapısına Dair Değerlendirme

Bu bölümde, ayrıntılı teknik bir değerlendirmeden daha ziyade internetin temel çalışma prensipleri ve belli başlı güvenlik zafiyetleri üzerinde durularak konudaki bütünlüğün sağlanması amaçlanmaktadır.

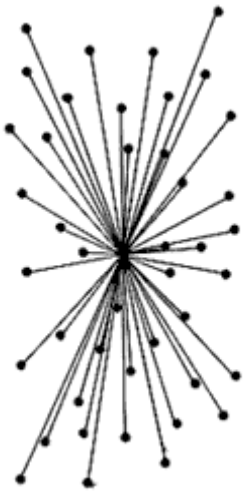
### a. İnternetin Tarihi ve Temel Çalışma Prensipleri

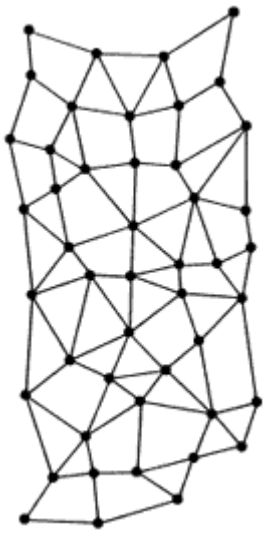
İkinci Dünya Savaşından sonra cereyan eden nükleer savaş tehlikesi içerisinde, dönemin batı dünyasının başat gücü olan ABD, olası bir nükleer saldırıya maruz kaldıktan sonra, karşılık olarak ikinci vuruş kapasitesini geliştirmek amacıyla araştırmalara başlamıştır (Ryan, 2010, s. 12). Zira çok çeşitli

senaryolar içerisinde en çarpıcı olan, muhtemel bir Sovyet nükleer saldırısı ile 26 saat içerisinde ABD'nin 30-150 milyon insanını kaybederek % 30-70 endüstri kapasitesinin yok olabileceğinin öngörülmesidir. Potansiyel saldırının yarattığı zarar sonrasında karşı hamlenin ne şekilde yapılması gerektiği o dönem Amerika'sının en önemli gündem maddesini oluşturmuştur. Bu bağlamda, olası bir Sovyet müdahalesine karşı, geride kalan stratejik askerî gücün kesintisiz şekilde komuta-kontrol altında tutulması gerektiği, dönemin birçok Amerikalı askerî ve güvenlik uzmanları tarafından karşı hamlenin ön koşulu olarak belirlenmiştir (USA National Security Council, 1963). Diğer bir deyişle, olası nükleer çatışma durumunda askerî birlikler ve komuta-kontrol arasında iletişimin kesintisiz olarak nasıl sağlanacağı konusu çözülmesi gereken en temel problemi oluşturmuş ve soğuk savaş boyunca çok farklı disiplinlerden uzmanlar ilgili konu üzerine ciddi olarak eğilmişlerdir.

O dönemdeki kitle haberleşme aracı olarak kullanılan radyo sinyalleri ve merkezî telefon bağlantısı, olası nükleer saldırıya karşı son derece savunmasız olarak değerlendiriliyordu. Bu bağlamda, nükleer saldırı sonrasında radyo sinyalleri saatlerce kesilebilir, ya da merkezî santralin hedef alınmasıyla telekomünikasyon sistemi devre dışı kalabilirdi (bk. Şekil-1) (Baran, 1964). Tam olarak bu gerçeklik, bugünkü anlamda internetin icat edilmesindeki ve gelişmesinin altındaki temel nedeni oluşturmaktadır. Polonya asıllı mühendis Paul Baran (1964), beyin hücrelerinin çalışmasından esinlenerek yeni kurulacak iletişim ağını, merkezi telekom sisteminden farklı olarak, olabildiğince dağınık ağ şeklinde tasarlamıştır (bk. Şekil-2). Baran'nın tasarladığı yeni sistemde, her bir ağ yüzlerce mahallî merkez (Node) üzerinden tek bir merkeze bağımlı olmaksızın birbirleri ile bağlantı kurması ve yerel merkezlerin bir bölümü zarar görmesi durumunda dahi tüm iletişim sisteminin devre dışı kalması engellenerek bağlantının süreklilik arz etmesi üzerine tasarlanmıştı. Kısacası bugünkü internet, milyonlarca ağın tek merkeze bağlı olmaksızın bir araya gelmesiyle oluşan ağın tümüdür. İlk olarak 1969 yılında ABD Savunma Bakanlığının desteğiyle; ARPANET olarak bilinen ve California, Santa Barbara (UCSB) Glen Culler and Burton Fried Üniversitelerini merkez (node) olarak belirleyen ağ bugünkü internetin temelini oluşturmaktadır (bk. Şekil-3). Şekilde görüldüğü üzere, sonrasında mevcut ağ genişletilerek, milyonlarca ağdan meydana gelen günümüz interneti hayat bulmuştur.

**Merkezi Telekomunikasyon Sistemi** **Dağıtılmış Telekomunikasyon Sistemi**



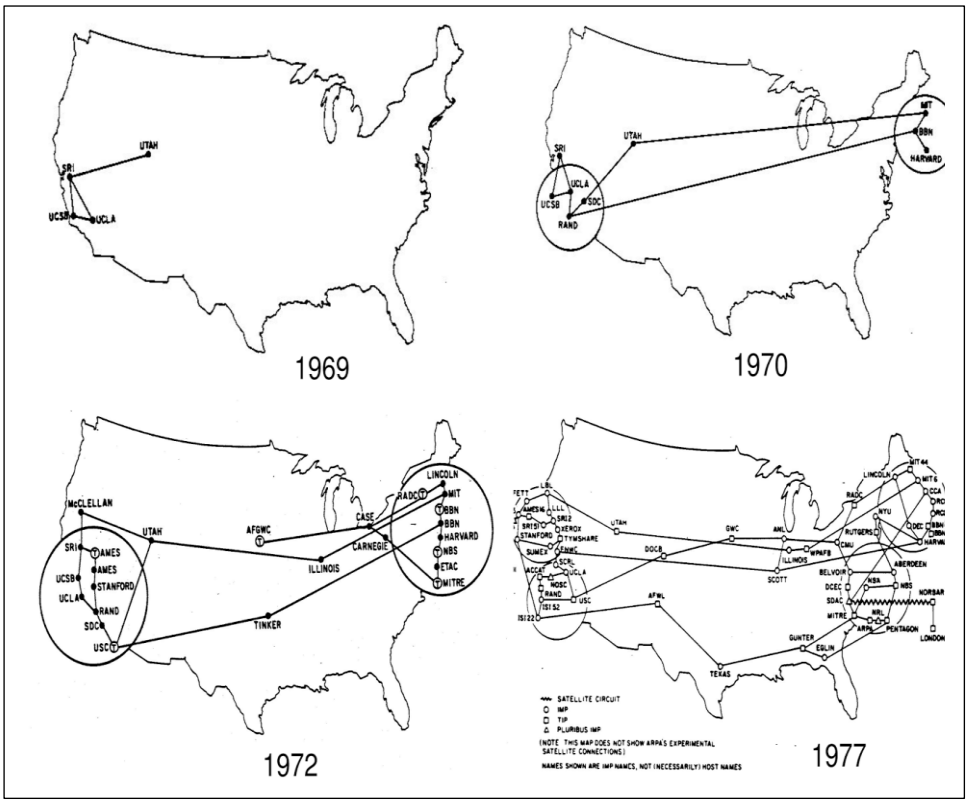


**Şekil-1** **Şekil-2**

**Kaynak:** RAND**,** http://www.rand.org/about/history/baran.html

**Şekil 3:** İnternet Ağının Gelişimi 1969-1977

**Kaynak:** https://ag01research.wordpress.com/author/alizeegallet/page/10/



İnternetin güvenlik açıklarına ilişkin değerlendirmeye geçmeden önce, konu bütünlüğü açısından internetin temel çalışma prensiplerine ilişkin birkaç teknik noktayı daha kısaca açıklamak faydalı olacaktır. İlk olarak, her bilgisayarın ve internet sitesinin sahip olduğu, bir anlamda kimlik numarasına benzetebileceğimiz IP/TCP olarak bilinen İnternet Protokol Numarası, bilgisayarlar arasında ortak bir dil oluşturmak suretiyle iletişim kurmayı sağlayarak milyonlarca bilgisayarı ortak platformda, yani internet ortamında buluşturmaktadır. İnternet üzerinden sağlanan bilgisayarlar arasındaki bilgi alışverişi 'packet-switched' denilen yöntemle yapılmaktadır. Bu yöntem vasıtasıyla, bilgiler önce parçalara ayrılmakta sonra ise ulaştığı yerde tekrar bir bütün olarak görülebilmektedir. Bu bilgi parçacıkları yollandığı anda yukarıda Şekil-2 de görüldüğü üzere merkezi olmayan internet sistemindeki en müsait ağ üzerinden karşı tarafa giderek, merkezi sistemin (Şekil-1) aksine, olası çakışma ve yavaşlamanın önüne geçmektedir (Lipson, 2002, s.5-7).

Bir siteye ulaşmak istediğinizde o sitenin IP adresini yani kimlik numarasını ezberlemek yerine DNS olarak adlandırılan yöntemle her bir harf karakteri numara karşılıklarına dönüşmekte, bu sayede klavye üzerinden harfler aracılığıyla internet sitelerine kolaylıkla ulaşmamızı sağlamaktadır. Örneğin, 194.27.43.67 IP adresi www.dpu.edu.tr ye karşılık gelmektedir. İnternet üzerinden yapılan siber müdahalelerin büyük çoğunluğu DNS sistemi üzerinden DDOS (Distributed Denial of Service Attack) denilen doğrudan zarar vermekten ziyade hizmeti engelleyen müdahale türünden oluşmaktadır. Hedef siteye eş zamanlı olarak kapasitesinin çok üzerinde istek göndermek suretiyle siteye erişim engellenebilmektedir. Şimdiye kadar anlatılan internetin çalışma sistemi günümüzde büyük ölçüde yenilenmediği için birçok güvenlik zafiyetlerine yol açabilmektedir.

### b. İnternet ve Güvenlik Açıklarına Dair Değerlendirme

İnternetteki güvenlik açıklarından faydalanarak binlerce farklı siber operasyon yöntemi olmasına rağmen, bu çalışmada siber operasyonlar kuvvet kullanımı açısından yapacağımız değerlendirmeye uygun olarak iki grup altında tasnif edilecektir. Bu anlamda, siber müdahaleler, fizikî zarar vermeden hizmeti engellemeyi ve fizikî zarar vermeyi hedefleyen saldırılar olmak üzere iki genel kategoriye ayrılmaktadırlar (USA National Reasearch Council, 2009, s. 1). Ayrıca, '*Siber saldırı*' kavramı yaygın olarak kullanılmasına rağmen uluslararası hukuk literatüründeki '*saldırı*' kavramı ile karışmasını engellemek için Micheal Schmit'in

yapmış olduğu '*siber saldırı*' (cyber attack) ve '*siber operasyon'* (cyber operation) ayrımı bu çalışmada da benimsenmektedir. Buna göre, siber saldırılar teknolojinin kullanılmasıyla hedefe doğrudan fizikî zarara sebep olan saldırılar için kullanılırken, siber operasyonlar fizikî zarar sebep olmak zorunda olmayan daha genel siber olaylar için kullanılmaktadır (Schmitt ve Vihul, 2014). İlgili terminolojik ayrım, ileride ele alacağımız kuvvet kullanımı konusunda kavram karışıklığını önlemek amacıyla uygun görülmüştür.

Siber operasyonlar, internetin tasarımına ilişkin problemlerden kaynaklanmaktadır. İnternetin keşfinden itibaren bağlantının güvenli olmasından daha ziyade iletişimin sürekli olarak sağlanması amaçlandığı için güvenlik ikinci planda kalmıştır. İnternetin ilk zamanlarında sadece güvenilir kullanıcıların dâhil olduğu yerel bir sistem olarak tasarlanırken zamanla bu kadar karmaşıklaşacağı hesap edilememiştir. Mevcut sistemde, kullanıcıların kendi bilgisayarındaki IP adresini yani kimliğini istediği gibi değiştirerek siber operasyonların kaynağını farklı ülkelerden gösterebilmektedir (Lipson, 2002, s.12). Bir örnek üzerinden ifade etmek gerekirse, Rusya hükümeti ya da desteklediği bir hacker grubu tarafından siber alan kullanılmak suretiyle ABD'yi hedef alan bir operasyon olduğunu varsayalım. Saldırganların IP adresini değiştirmek suretiyle operasyonu İran üzerinden yaparak görünürde Rusya'nın operasyonla olan illiyet bağını ortadan kaldırıp Rusya'nın uluslararası sorumluluğunu muğlaklaştırmaktadır. Ayrıca, istismar edilen ülke sayısı artabilir ve bu durumda teknik takip çok daha zorlu bir süreç hâline gelebilmektedir. Örneğin, 2007 yılında Estonya'yı hedef alan DDOS saldırıları, şimdiye kadar ki en geniş ve koordineli siber operasyonlardan biri olarak 178 farklı ülke üzerinden yapıldığı tespit edilmiştir (Tikk, Kaska ve Vihul, 2010, s.17). Bu saldırıyla, ülkenin en büyük haber sitelerine, internet bankacılığına, borsasına, kamu sitelerine erişim günlerce engellenerek çok büyük ekonomik kayba neden olunmuştur. Ayrıca, siber operasyonu düzenleyenler, hedef ve istismar edilen ülkeler arasında çözümsüz anlaşmazlıkların olduğu ülkeleri tercih etmekte, nitekim hedef ülke saldırıyı aydınlatmak için soruşturmada iş birliği talep ettiğinde istismar edilen ülke dahi çoğunlukla olumsuz cevap vermektedir. Nitekim Estonya'ya karşı yapılan siber operasyonun en büyük destekçisi hatta faili olarak iddia edilen Rusya hükümeti, Estonya hükümetinin tüm çağrılarına rağmen hukuki ve teknik soruşturma iş birliğini kabul etmemiştir (Tikk, Kaska ve Vihul, 2010, s.27). Genel olarak, bu saldırılar internet aracılığıyla casus yazılım yüklenmiş veya yüklü olan yazılımın açıklarını kullanarak sıradan kullanıcıların sahip olduğu

binlerce bilgisayarı komuta edebilmektedir. Kontrol edilen bilgisayarlar sayesinde aynı anda hedeflen ağın kapasitesinin çok üzerinde siteye istek göndererek erişim engellenebilmektedir. (Joubert, 2012). Harici olarak yönetilerek siber operasyonların parçası hâline dönüşen bilgisayarların çoğunun yapılan operasyonlardan habersiz oldukları için bu kişilerin hukuki sorumluluğuna ilişkin muğlak bir alan oluşmaktadır.

Hedeflenen ağı ya da bilgisayarı internet bağlantısı üzerinden veya casus yazılım ile uzaktan doğrudan yönetebilir hâle getirilmesi siber saldırılarda başvurulan en yaygın yöntemdir. DDOS gibi fiziki zarar vermeyen operasyonların aksine, fiziki zarar verebilme kapasitesine sahip olup genelde hedef kritik altyapıyı yönetmek için kullanılan "Supervisory Control and Data Acquisition (SCADA) olarak bilinen sistemleri hedef almaktadır. Güvenlik endişeleri bağlamında kritik altyapı hizmetlerinin önemli kısmının internet bağlantısı bulunmamaktadır. Ancak, saldırılar USB gibi taşınabilir aygıtlar üzerinden özel yazılımlarla bilgisayarı internet ortamına bağlayarak organize edilmektedir (Reuters, 2010). Genelde, hedeflenen birimin içerisinde çalışan bir kişiyle anlaşmak ya da birime casus yerleştirmek suretiyle hedeflenen sistem dışardan müdahaleye açık hâle gelebilmektedir. Örneğin, 2010 yılında geliştirilen ve İran'ın nükleer kapasitesine karşı yapılan STUXNET saldırısı bunun en açık pratiğini teşkil etmektedir. STUXNET adlı virüs bir şekilde nükleer üretim yapan tesislerin içerisindeki sisteme bulaştırılarak, nükleer santraldeki uranyum üretim başlıklarının motor hız kapasitesinin çok üzerinde artırma yönünde komutu vererek, en az 2000 başlığı kullanılmaz hale getirmiştir. Bu saldırının nükleer üretimi en iyi ihtimalle birkaç yıl geri atmasının yanında doğrudan fiziki zararla sonuçlanması oldukça önem arz etmektedir (Albright, Brannan ve Walrond, 2010).

Sonuç olarak, SCADA'lara yönelik saldırılarda faillerin bulunması, içeriden yapıldığı takdirde çok zor olmasına karşılık bir ölçüde mümkündür. Ancak, DDOS gibi internet üzerinde yapılan operasyonlarda, internetin anonim yapısından dolayı operasyona müdahil ülkelerin iş birliği yapmasıyla ortaya çıkabilmektedir. İş birliği ise birçok kez ulusal menfaatler gereği ya da siber operasyonların devlet destekli (State-Sponsored) yapılmasından dolayı reddedilmektedir. Bu yüzden çalışmanın bundan sonraki bölümünde operasyonu yapanların tespitine ilişkin etkin, teknik veya siyasi bir çözümün bulunması durumunda uluslararası hukuktaki güç kullanımına ilişkin nasıl hukuki değerlendirme yapılması gerektiği açıklanmaya

çalışılacaktır. Bu bağlamda, öncelikle kuvvet kullanımına ilişkin hukuk kuralları ortaya konulacak ve bunların siber saldırılar için ne şekilde uygulanacağı tartışılacaktır.

## Uluslararası Hukukta Kuvvet Kullanmanın Yasal Zemini ve Siber Saldırılar İçin Değerlendirilmesi

İkinci Dünya Savaşı'ndan sonra, barışın kalıcı olmasını temin etmek amacıyla kurulan ve hemen hemen tüm devletlerin taraf olduğu BM'nin kurucu anlaşmasının 2 (4) maddesi: *'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'* uluslararası arenada, kuvvete başvurmanın yasaklanmasına dair temel hukuki çerçeveyi çizmektedir (Gray, 2008, s. 30). Bir egemen devletin toprak bütünlüğü ya da siyasal sistemine karşı kuvvet kullanmayı (Use of Force) ya da kuvvet kullanma tehdidinde bulunmayı açık olarak yasaklamıştır. İlgili madde aynı zamanda Uluslararası Adalet Divanında görülen birçok davada teamül hukuk kuralı (Customary Law) olarak kabul görmüş (Harris, 2004, s. 886) ve Uluslararası Hukuk Komisyonu da benzer şekilde teamül hukuk kuralı olduğunu kabul etmiştir (United Nations, 1966). *Kongo'daki Askerî Faaliyetler Davası'nda* (2005, para 75) Birleşmiş Milletler kurucu anlaşması, kuvvet kullanma konusunda temel hukuki düzenleme olduğunu vurgulamıştır. Ayrıca, Nikaragua davasında aynı hüküm bir buyruk kuralı (Jus Cogens) olarak görülmüştür. Son olarak, Kuvvete başvurmanın BM kurucu anlaşmasına paralel şekilde yasaklaması, birçok bölgesel ve ikili anlaşmada da yer almıştır (Roscini, 2014, s. 242).

Kuvvet kullanımına ilişkin hukuki değerlendirmelerde ilgili hükmün temel olarak alındığı ve uluslararası toplumda geniş ölçüde kabul gördüğü aşikârdır. Ancak maddenin ihtivasına ilişkin özellikle kavramlar özelinde şiddetli tartışmalar da BM'nin kurulduğu tarihten itibaren yaşanmıştır (Gündüz & Günel (ed), 2015). Bu makalede kavramları açıklarken ekseriyette teamül hukuku ve mahkeme kararları dikkate alınarak, söz konusu kararların siber saldırılar için uygulanmasının mümkün olup olmayacağı ortaya konulacaktır. Diğer bir ifadeyle pozitif hukuk bakış açısıyla değerlendirme yapılacaktır. Bu bağlamda iki koşulun sağlanması gerekmektedir; öncelikle BM kurucu anlaşmasının devletler arasında

yapılmış olması sebebiyle siber saldırının failinin ***devlet olması*** ve ilgili fiilin ***kuvvet kullanımı ya da kuvvet kullanımı tehdidi*** olarak değerlendirilmesi gerekmektedir. Dolayısıyla BM şartı, doğrudan kuvvet kullanmanın yanında fiili müdahaleye varmayan tehdit içeren durumları da yasaklamıştır. Şimdi, ilgili maddede yer alan aktörlerin kim olduğuna ve "*kuvvet kullanma"* ve "*kuvvet kullanma tehdidi"* kavramlarının muhtevasına ilişkin tartışmalara açıklık kazandırmaya ve bunları siber saldırılar için uygulamaya çalışalım.

### a. Aktör Sorunu

İnternetin yukarıda belirtiği üzere merkezi olmayan yapısını kullanarak yapılan siber saldırılar ekseriyetle devlet dışı aktörler tarafından yürütülmektedir (Hollis, 2011, s. 387). Buna karşın BM'nin kurucu anlaşması taraflarının egemen devletler olması dolaysıyla anlaşma hükümlerinin siber saldırılar için bağlayıcı olmadığı görüşü ileri sürülebilir. Ancak, devletlerin siber alana yakından ilgi duyarak faaliyet yürüttüğü ve hatta birçoğunun kendi siber ordusunu oluşturduğu bilinen bir gerçektir. Buna rağmen devletler uluslararası sorumluluk müessesesini devre dışı bırakmak için faaliyetleri yürütenlerin, ajanların ya da çalışanların devlet ile bağını gizli tutmaktadır (Hollis, 2011, s. 388).

Bahsi geçen gizliliğin, devletin uluslararası hukuktan kaynaklanan yükümlülüklerine teknik olarak halel getirmeyeceğini, BM tarafından teamül hukukunun kodifiye edilmesiyle oluşturulan sorumluluğa ilişkin anlaşma taslağının 5. maddesi açık şekilde belirtilmiştir (Uluslararası Hukuk Komisyonu, 2001). İlgili maddede, devlet organı olmayan fakat kamu gücünü kullanarak haksız fiilleri işleyen kişi veya kişilerin yaptığı eylemlerin devlete isnat ettirilebileceği açıkça yer almıştır. Ayrıca Eski Yugoslavya Uluslararası Ceza Mahkemesi de *Tadic Davası* (1999, para 131) ilgili maddeye teamül hukuku olarak başvurmuştur. Mahkeme, doğrudan devlete bağlı olmayan paramiliter kuvvetlerin yukarıda bahsedilen ilgili madde kapsamındaki bağını ortaya koymak için *genel kontrol* (overall control test) olması durumunda devletin sorumluluğunun doğabileceğini ortaya koymuştur. Kısacası, hükümetler tarafından resmî bağı olmadan desteklenerek başka egemen bir devlete karşı yapılan siber saldırıların, diğer koşulları sağlaması kaydıyla, bu maddenin bağlayıcılığından kurtulması oldukça zordur.

### b. Kavram Sorunu

"Kuvvet kullanma" ve "kuvvet kullanma tehdidi" kavramlarının açık olarak herhangi bağlayıcı tanımı yapılmadığı için kavramları anlamlandırırken ve siber saldırıları kapsayıp kapsamadığını tartışırken, yine teamül hukuku ve mahkeme kararları temel alınacaktır.

BM'nin kuruluşundan itibaren, gelişmekte olan ve gelişmiş ülkeler arasında "*kuvvet*" ifadesine farklı anlamlar yüklenmesi en önemli anlaşmazlık konularından biri olmuştur. Gelişmiş ülkeler ya da dönemin Batı Bloğu BM şartının 2. maddesindeki *kuvvet* ifadesinin 51. maddesinde olduğu gibi sadece fiziki olarak askerî saldırıları kapsaması gerektiğini savunmuşlardı. Doğu Bloğunu oluşturan gelişmekte olan ülkeler ise, ekonomik ve siyasi yaptırımları da egemenlik ihlali olarak gördükleri için söz konusu ihlallerin *kuvvet kullanımı* kapsamında değerlendirilmesi gerektiğini savunmuşlardı (Gray, 2015, s. 621). Tartışmaları aydınlatmak amacıyla BM Genel Kurulu çalışma başlatmıştır. Bu bağlamda, BM Genel Kurulunun *2625 sayılı Dostça İlişkiler ve İşbirliğine İlişkin Deklarasyonu* (1970) "*kuvvet"* kavramını açıklarken, gelişmiş ülkelerin başvurdukları doğrudan askerî müdahale tezinin aksine kavramı daha geniş yorumlayarak dolaylı yollardan askerî müdahalede bulunmayı da "*kuvvet kullanımı"* kapsamı içerisinde değerlendirmiştir. Ancak bildirge, ekonomik ve politik yaptırımlar vasıtasıyla baskı kurmayı prensip olarak yasaklamasına rağmen ilgili eylemleri kuvvet kullanma kapsamına almamıştır. Divan bildirgeye paralel şekilde N*ikaragua Davası'nda (1986, para 191-195, 228-229)*, kuvvet kullanımı ifadesinin sadece silahlı saldırılar (Armed Attack) ile sınırlı olmayacağını karara bağlamıştır. Bu bağlamda, egemen bir devlete karşı savaşmak için isyancıları eğitmenin ve silahlandırmanın da kuvvet kullanımı olarak sayılacağı vurgulanmıştır. Ancak sadece isyancıları ekonomik olarak finanse etmenin bu kapsamda tutulamayacağını da özellikle belirtmiştir.

Mahkeme ve BM genel kurulunun kararlarından, her ekonomik yaptırımın kuvvet kullanma olarak değerlendirmesi güç olmakla birlikte ilgili maddedeki kuvvet kullanma teriminin *dinamik* özelliği ve doğrudan kuvvet kullanılmayan durumlar için de uygun olduğu sonucu kolaylıkla çıkarılabilir. Ayrıca, Viyana Anlaşmalar Hukuku Sözleşmesinin 31 (1) maddesi "*Bir antlaşma, hükümlerine antlaşmanın bütünü içinde ve konu ve amacının ışığında verilecek alelade manaya uygun şekilde iyi niyetle yorumlanır*" şeklinde öngörmüştür. Dolayısıyla küresel barış ve güvenliği tehdit edecek her türlü yeni gelişme, ilgili madde kapsamında

değerlendirilebilir. Örneğin, Arap-İsrail savaşında petrol üreten OPEC ülkeleri, İsrail'e yardımlarından ötürü ABD ve Avrupa Ekonomik Topluluğuna karşı petrol ambargosu uygulamıştır. Ambargoya maruz kalan gelişmiş batılı devletler, yaptırımın dünya ekonomisini büyük bir krizle karşı karşıya bırakacağını ileri sürerek, *kuvvet* kavramının sadece silahlı saldırıları kapsadığı tezinin aksine, petrol yaptırımı kararının da kuvvet kullanımı ile eşdeğer olup olmadığını tartışmışlardır (Brosche, 1974). İngiliz diplomat Sinclair, BM genel kurulunda "her politik ve ekonomik baskının ülkelerin egemenliğinin ihlali olarak görülmeyeceği ancak enerji gibi temel ihtiyaçtan mahrum bırakmanın kuvvet kullanmaya dâhil olması gerektiğini ileri sürmüştür. Böylece, bir anlamda kendi ülkesinin tezini çürüterek kuvvet kullanımının dinamik yapısını açıkça kabul etmiştir (Harris, 2004, s. 890). Sonuç olarak, egemen bir devlete karşı doğrudan fiziki müdahale kuvvet kullanımı olarak görülmemeli, ayrıca silahlı saldırı ile aynı etki ya da sonuca neden olan diğer durumlar da kuvvet kullanımı kapsamında değerlendirilmelidir.

Kuvvet kullanmanın dinamik yapısı göz önünde bulundurulduğunda, yapısı itibariyle fiziki gücü içermeyen ancak silahlı saldırı ile aynı derecede somut zararlara sebep olabilen siber saldırılar, kuvvet kullanmaya eşdeğer olabilirler (Brownlie, 1963, s. 362). Örneğin; kimyasal, biyolojik ve radyolojik silahlar da yapısı itibariyle silahlı saldırılar gibi yıkıcı olmamasına rağmen kuvvet kullanımı kapsamında değerlendirilmektedir. Siber saldırılar bağlamında yukarıda ele aldığımız 2010 İran'ın nükleer kapasitesine yönelik yapılan STUXNET virüs saldırısı, bunun açık örneğini teşkil etmektedir. Dolayısıyla, siber saldırılar açık bir şekilde doğrudan fiziki zararlara yol açabilme eşiğini geçmiş ve ciddi zararlar verebilme kapasitesine ulaşmıştır. Mesela doğalgaz hattının sabote edilmesi, nükleer merkezlerin imha edilmesi, hava trafiğinin felç edilip binlerce kişinin sabotaja uğraması gibi yüzlerce zarara sebep olan bir saldırı metodunu uluslararası hukuk kurallarından muaf olarak düşünmek imkânsızdır. Dolayısıyla, oldukça etkili fiziki zarara, yaralamaya ya da ölüme yol açan siber saldırıların devletler tarafından doğrudan yapılması ya da yapılan eylemin devlete isnat ettirilmesi durumunu da kuvvet kullanımı altında değerlendirebiliriz.

Bir diğer tartışma ise maddede yer alan "kuvvet kullanma tehdidi" ifadesiyle neyin kastedildiğidir. Uluslararası Adalet Divanının "*Nükleer Silahlara İlişkin Danışma Görüşünde* (1996, para 39,47)" kuvvet kullanma tehdidini "*mevcut ya da meydana gelebilecek bir olaya karşı kuvvet kullanma niyetine ilişkin bir sinyal*

*verilmesi*" olarak tanımlamıştır. Buna karşın divan, ABD'nin Nikaragua sınırına doğru konuşlanan askerlere ait eylemlerinin kuvvet kullanma tehdidi kapsamındaki eşiği aşmadığını karara bağlamıştır (*Nikaragua Davası*, para 227). Mahkeme sadece ABD askerinin sınırda tatbikat yapmasını bu kuralın ihlali için yeterli görmeyerek, kuvvet kullanma tehdidinin daha açık bir şekilde olması gerektiğini zımni olarak kabul etmiştir. Harris, 1956 yılında İngiltere ve Fransa'nın Mısır-İsrail arasındaki çatışmanın 12 saat içinde bitirilmesi, aksi takdirde askerî müdahalede bulunacağına ilişkin olarak verdiği ültimatomun bu tehdit kapsamında değerlendirilebileceğini belirtmiştir (Harris, 2004, s.891). Yani mahkeme kararından yola çıkarsak, ABD örneğindeki tatbikatın yapıldığı sırada, ABD açık bir şekilde Nikaragua devletine benzer şekilde belli bir sürede ve dayatılan şartlar yerine getirilmezse ordusunun müdahalede bulunacağına dair bir sinyal vermiş olsaydı, kuralın ihlali sayılabilirdi.

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

### c. Meşru Kuvvet Kullanma İstisnaları

Kuvvet kullanımını düzenleyen maddenin son kısmı 'Birleşmiş Milletlerin amaçlarıyla bağdaşmayacak şekilde kuvvet kullanma ya da tehdidinde bulunma' ifadesini içermektedir. Bu kapsamda, BM'nin amaçları incelendiğinde iki farklı şekilde meşru kuvvet kullanımına kapı aralamaktadır: *Meşru müdafaa hakkı* ve *BMGK kararları* (Gray, 2015, s. 4). Esasında, devletlerin sınırlı süreyle kendilerini

savunma mecburiyetleri haricinde kuvvet kullanma haklarından BM güvenlik konseyi lehine vazgeçtikleri görülmektedir.

BM kurucu anlaşmasının 51.maddesine istinaden; üye devletlerden birine karşı yapılacak olan "silahlı saldırı" karşısında, BMGK uluslararası barış ve güvenliği tesis etmeye yönelik önlemler alıncaya kadar saldırıya uğrayan tarafa tek başına ya da başka bir devletin yardımıyla kolektif olarak meşru müdafaa kapsamında kuvvet kullanarak karşılık verme hakkını tanımaktadır. Bu maddedeki "silahlı saldırı" kavramının kapsamına ilişkin yine bağlayıcı bir tanım olmadığı için teamül hukuk kuralları yardımcı olmaktadır. *Nikaragua Davası'nda* (1986, para 195), mahkeme diğer bir egemen devlete yönelik doğrudan şiddete başvurma durumunda ya da egemenliği ihlal edenlere yönelik silah ve lojistik destek gibi yardımların yapılmasını da askerî müdahale kavramının içine dâhil ederek geniş bir yorum yapmıştır. Ancak buradan her silah ve lojistik yardımı bu kategoriye koymak meseleyi basitleştirmeye yol açar ki, nitekim mahkeme aynı paragrafta devletin etkin olarak çatışmaya dâhil olmasından bahsetmektedir. Kısaca, kuvvet kullanma kavramında olduğu gibi somut olarak sonuçlara etki etmekten bahsedilmektedir.

Diğer taraftan, meşru müdafaa hakkını kullanan tarafın karşılık verme hakkını sınırlayan *gereklilik ve orantılılık ilkesi* maddede doğrudan yer almamasına karşın teamül kuralı olarak geniş ölçüde kabul görmektedir. İlgili ilkeler, kuvvete son çare olarak başvurulması gerektiği ve kullanılan kuvvetin orantılı olmasını öngörmektedir (Pazarcı, 2006, s. 516). Somutlaştırmak gerekirse, kendisine yapılan bir saldırı karşında, karşılık olarak tüm ülkeyi işgal edip kendi egemenliğini ilan etmek açık bir şekilde orantılılık ilkesinin ihlali ya da barışçı yolla çözüm söz konusuyken hâlâ kuvvet kullanarak karşılık vermek istemesi, gereklilik ilkesinin ihlali olacaktır.

Adalet divanı, aslında silahlı saldırıyı kuvvet kullanma fiiline yakın bir şekilde değerlendirmiş, ancak kuvvet kullanmayı biraz daha geniş manada ele almıştır. Siber saldırlar sonuçları açısından düşündüğümüzde, bir silahlı saldırıya eşdeğer olabilecek zarara, ölüme ya da yaralanmaya yukarıda açıklandığı üzere sebep olabileceği için maddenin kapsamına girdiği oldukça açıktır. Ancak meşru müdafaa hakkını kullanırken karşı tarafa yapılacak müdahale açısından uyulması gereken gereklilik ve orantılılık evrensel savaş ilkeleri, internetin asker-sivil ortak kullanım alanları açısından düşünüldüğünde birçok belirsizliklere neden olmaktadır

Bu ilkeler, savaşın ikincil yıkıcı etkilerini bertaraf etmek ve sivillerin savaşa katılmasıyla savaşın genişlemesini veya terörist faaliyetlerde bulunmasını engellemek için ortaya konulmuştur (Greenwood, 2008, s. 11). Fakat elektrik şebekeleri, tren sistemleri, hava yolu taşımacılığı, köprüler gibi sayısız altyapı sistemleri birçok ülkede asker-sivil unsurların kullandığı ortak bir alanı oluşturmaktadır. Örnek vermek gerekirse, ABD'nin askerî birimlerinin kullandığı internet altyapısının yüzde 95'i sivillerle müşterek kullanılmaktadır (Brochgrave, 2001, s. 10). ABD'nin olası zarar verici siber saldırısına karşı diğer bir devletin meşru müdafaa hakkının kullanılması durumda, sivillerin doğrudan etkilenmesi kaçınılmaz olacaktır. Bu durum, ülkede politik belirsizlik, ayaklanma veya iki ülke arasındaki savaş riskini körükleme gibi sayısız krizi derinleştirecek ikincil etkilere neden olabilir. Buradaki orantılılık ve askerî gereklilik ilkesinde iki farklı görüş hâkim olmaktadır. İlk olarak, sorunların çözümü için doğrudan güç kullanımına meyilli devletler askerî gerekliliği ön plana çıkarıp sivil unsurlarının da meşru hedef olduğunu savunurken, diğer taraftan, bu durumun şiddet atmosferini tırmandırması sebebiyle orantılılık ilkesine vurgu yapmaktadırlar. Özellikle çatışma hâlinde bu ikisi arasında dengeyi kurmak oldukça zorlu bir süreç olmasına rağmen mutlaka asgari müşterek bir yol sağlanması gerekmekte, aksi takdirde bu durum, küresel çapta felaketlere yol açma potansiyelini barındırmaktadır.

BM kurucu anlaşması VII. Bölüm Madde 39 ile "*uluslararası barış ve güvenliğin bozulduğu ya da tehdit altında olduğu hâllerde*" güç kullanma tekeli sadece BM Güvenlik Konseyine verilmiştir. Meşru müdafaa hakkını kullanan egemen devlet bile, sadece BMGK müdahil olana kadarki süreçte meşru olarak karşı tarafa yönelik kuvvet kullanabilir. Diğer bir deyişle tek taraflı güç kullanımı neredeyse yasaklanmış ve güç kullanma tekeli sadece BMGK'ye verilmiştir. Burada uluslararası barış ve güvenliğin tehlikeye düşmesi hâlinde BMGK tarafından müdahale edilmesi öngörülmüş ancak barış ve güvenliğin tehlikeye düşmesi tanımlanmayarak kurulun yetkisine bırakılmıştır. Sonuç olarak, daimî beş ülkenin herhangi bir tehdit konusunda birleşip karar alması yeterli olacağı için siber saldırıların kuvvet kullanımı kapsamında nasıl değerlendirileceği kurulun münhasır yetkisinde olacaktır.

## Sonuç

Siber operasyonlar gelişmiş teknolojinin sağladığı imkânlar sayesinde klasik askerî müdahale ile elde edilebilecek birçok etkiyi yapma kabiliyetine ulaşmıştır. Özellikle operasyonlar, internetin güvenlik açıklarından ya da network sistemlerine dışarıdan yapılan müdahalelerle gerçekleşmektedir. Yapılan müdahalelerin sorumlularının ortaya çıkarılması internetin anonim yapısından kaynaklı olarak pek çok kez mümkün olmamaktadır. Ancak bu eksiklik, uluslararası hukuk tarafından konunun nasıl ele alınması gerektiğine bir engel teşkil etmez. Bu bağlamda, klasik tehdit algısında ciddi değişimlerin yaşanmasına sebep olan siber saldırıların uluslararası hukuktaki güç kullanma açısından değerlendirilmesi kaçınılmaz olmuştur.

Uluslararası hukukta güç kullanımının yasaklanmasına ilişkin düzenlemenin ihtivasına ilişkin olarak ciddi ayrışmalar yaşanmaktadır. Bazı araştırmacıların ilgili düzenlemeyi dar yorumlamasına karşın, 2.Dünya Savaşından sonra yaşanan gelişmelerin çözümüne ilişkin olarak mahkeme kararları incelendiğinde dinamik yapıda olduğu rahatlıkla anlaşılabilir. Bu bağlamda mevcut düzenlemelerin siber saldırılar için geçerli olacağına yönelik bir kuşku olmamasına rağmen mevcut ve potansiyel sorunları çözme noktasında eksik kaldığı da bir gerçekliktir. Bu kapsamda, mevcut uluslararası hukuk normlarından yola çıkılarak siber alana yönelik çok taraflı bir düzenlemenin yapılması daha sağlıklı olacaktır.

## Extended Summary

### Introduction

The reliance on technology has dramatically increased since 90s. This has created a realm that is vulnerable against increased cyber threats. A considerable part of national infrastructures, most particularly communication means, national health care systems, and commercial affairs, have started to be threatened by cyber operations, which clearly leads to a paradigm shift. It has fundamentally changed the understanding of traditional threats in national security naturally. Therefore, the recent international law discussions have taken into account the legal status of cyber operations. A terminological clarification is necessary at this point. Micheal Schmitt’s distinction between “cyber operation” and “cyber-attack” is

acknowledged in this study. According to it, cyber-attack has to include acts of violence while cyber operations do not have to content the violent consequences. The two mainstream approaches have come out in this regard. On the one hand, in order to avoid lawless or chaotic situation the existing rule of international law should be implemented in cyber issues by analogy to other conflicts. On the other hand, establishing a cyber-specific regulation is obligatory due to the insufficiency and inconsistency of the existing law. This study revisits the discussion mentioned above specifically from the point of use of force in international law.

## An Overall Assessment of the Internet's Technical Structure and Its Security Vacuums

The constant progress in digital infrastructure has brought about a number of advantages for economic prosperity, efficient academic researches, powerful military forces, transparent governments, and free societies. Hence, the dependency on network information systems in society and government such as in communication, health care, economics, and national service infrastructures has dramatically increased. However, nothing comes without a price, and here the costs are various significant vulnerabilities. Especially, the rapid adoption of unsafe technology makes a major contribution to this situation.

In the early days of the Internet, its design was based on the requirements of the project members of the Internet. Now, the problem is that we still continue to work mainly under the same framework. Easy accessibility to improve life standards, instead of focusing on security aspects, has been prioritized while cyber technology widely used by the society. Briefly, while these developments significantly increase the efficiency and productivity in many aspects, it has fundamentally changed power and security approaches about its usage in the conduct of hostilities. The focal point of military power has been rapidly turned into information technology from the traditional kinetic power. Therefore, this has also resulted in a high dependency on the network infrastructure for military forces, which is too vulnerable against cyber operations.

There are different types of cyber operations and they need to be classified in accordance with the use of force international law to avoid confusion. In this context, cyber operations should be categorised under two types: physically destructive or not. The physically harmless cyber intervention mostly originates

from the structure of Internet. Aggressors are able to modify Internet Protocol Numbers under the current system, hence a cyber-aggressor is able to divert the origin of operations either creating a new IP number or falsifying someone else.

In short, although cyber destructive capacity is reaching a critical threshold, the perpetrators are not identified due to the anonymity of Internet structure. Besides the technical reasons, there is an obvious lack of cooperation among state parties because the investigation of aggressors might be blocked due to the political interests. The technical traction of state-sponsored cyber operations is almost impossible due to the unwillingness to cooperation with the victimized country. This study continues to examine the issue by assuming that a functional solution for the attribution problem is found among states.

## Use of Force in International Law and Its Application to Cyber Warfare

After the Second World War states are obligated not to resort the use of force under the UN charter, which also largely illustrate the customary law. The Article 2(4) of the Charter requires that all member states must refrain from "threat" or "use of force" against any states. According to the article, two conditions have to be met. First, the use of force must be attributed to a state. The second, actions must be amounted to "threat" or "use of force". However, the applications of these conditions in the context of cyber issues creates two main problems. The first problem is about revealing the legal connection between cyber aggressors and states. The second problem is about defining the meaning of terms that 'threat' and 'use of force' in the cyber context.

The two exceptions to the prohibition on the use of force are largely acknowledged: Exercising self-defence pursuant to the Article 51 and the enforcement measures by Security Council under the Chapter VII. In terms of self-defence, it is necessary to draw a legal framework for the term 'armed attack' from the Article 51 and from the "necessity" and "proportionality" criteria in customary law. Physical damage-oriented cyber-attacks meet the armed attack criteria. However, exercising necessity and proportionality criteria for cyber-attacks is considerably difficult due to the dual-used structure of Internet, meaning both governments and civilians use the same infrastructure. The other exception is straightforward. If the Security Council acknowledges a situation amounts to the threat to peace, the breach of the peace or the act of aggressions, it acts according

to the Chapter VII. In the context of cyber-attacks, it means that the Security Council is a sole authority to decide what cyber-attacks are considered as a case of the use of force.

## Conclusion

This study argues that the existing regulations are not sufficient for dealing with cyber warfare. The study has not technically recognized any obstacle against the applicability of the current use of force regulations, yet they are not clear and sufficient enough to use in the context of the cyber warfare. Therefore, the current regulations should be reviewed and enhanced to create a new cyber-specific regulation by the international community, which should be as inclusive as possible.

## Son Not

1)Ayrıntılı bilgi için bk., Harold H Koh (2012), International Law in Cyberspace, 54 Harvard International Law Journal 1, s.3; Michael N. Schmitt, (2002), Wired Warfare: Computer Network Attack and Jus In Bello, 84 Rev. Int. Croix-Rouge, s.368; Eric Talbot Jensen (2003), Unexpected Consequences from Knock-On Effects: A Different Standard for Computer Network Operations, 18 AM. U. INT'L L. REV., s.1148; Philip A. Johnson, (2002), Is it Time for a Treaty on Information Warfare?, 76 INT'L L. STUD. s.440; Yoram Dinstein, (2013), Cyber War and International Law: Concluding Remarks at the 2012 Naval War College International Law Conference, 89 INT'L L. STUD., s.283.

2)Ayrıntılı bilgi için bknz., Duncan B. Hollis, (2007), Why States Need an International Law for Information Operations, 11 Lewis & Clark L. Rev., s.1023; Davis Brown, (2006), A Proposal for an International Convention to Regulate the Use of Information Systems in Armed Conflict, 47 Harv. Int'l L.J., s.181; Jeffrey T.G. Kelsey, (2008), Hacking Into International Humanitarian Law: The Principle of Distinction and Neutrality in the Age of Cyber Warfare, 106 Michigan Law Review, s.1431.

## Kaynakça

### Kitaplar

Brochgrave**,** Arnaud De., Cardash, Sharon L., Cilluffo, Frank J. ve Ledgerwood, Michèle M. (2001). *Cyber threats and Information Security: Meeting the 21st Century Challenge*, Washington: CSIS Press.

Brownlie, Lan. (1963). *International Law and the Use of Force by States*. Oxford: Clarendon Press.

Dam, Kenneth W., Lin, Herbert S., Owens, ve William A. (2009). *Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities***,** Washington; National Academy press.

Gray, Christine. (2008). *International Law and Use of Force*. Newyork: Oxford University Press.

Gray Christine. (2015). *The Use of Force and The International Legal Order*. İçinde M.D Evan. *International Law* (ss.612-650). London: Oxford Press.

Greenwood, Christopher. *Historical Development and Legal Basis***.** İçinde Dieter Fleck. *The Handbook of International Humanitarian Law* (ss.101-150). Newyork: Oxford Universiy Press.

Gündüz, Aslan. (2015). *Milletlerarası Hukuk. İstanbul*. (ed. Reşat Volkan Günel), İstanbul: Beta Yayıncılık.

Harris, DJ. (2004). Cases *and Materials on International law*. London: Thomason Sweet & Maxwell.

Pazarcı, Hüseyin. (2006). *Uluslararası Hukuk*. Ankara: Turhan Kitapevi.

Roscini Marco. (2014). *Cyber Operations and the Use of Force in International Law*. Oxford: Oxford Press.

Ryan, Johnny. (2010). A *History of the Internet: And the Digital Future*. *London*, England: Univ of Chicago Press.

### Makaleler

Brosche, Hartmut. (1974). The Arab Oil Embargo and United States Pressure against Chile: Economic and Political Coercion and the Charter of the United Nations. *Journal of International Law*, 7(1), 3-35.

Brown, Davis. (2006). A Proposal for an International Convention to Regulate the Use of Information Systems in Armed Conflict. *Harvard International Law Journal*, 47(1), 179-201.

Dinstein, Yoram. (2013). Cyber War and International Law: Concluding Remarks at the 2012 Naval War College International Law Conference. *International Law Studies,* 89, 276-287.

Hollis, Duncan B. (2007). Why States Need an International Law for Information Operations. *Lewis & Clark Law Review*, 11, 1023-1061.

Jensen, Eric Talbot. (2003). Unexpected Consequences from Knock-On Effects: A Different Standard for Computer Network Operation. *The American University International Law Review*, 18(5), 1046-1087.

Johnson, Philip A. (2002), Is it Time for a Treaty on Information Warfare?. *International Law Studies*, 76, 439-455.

Joubert, Vincent. (2012). Five Years after Estonia's Cyber Attacks. *NDC Research Papers*, 76(1), 1-8.

Kelsey, Jeffrey T.G. (2008). Hacking Into International Humanitarian Law: The Principle of Distinction and Neutrality in Age of Cyber Warfare, *Michigan Law Review*, 106(7), 1427-1452.

Koh, Harold H. (2012). International Law in Cyberspace, *Harvard International Law Journal*, 54(1), 1-12.

Schmitt, Michael N. (2002). Wired Warfare: Computer Network Attack and Jus In Bello. *International Review of the Red Cross*, 84, 365-389.

**Andlaşmalar**

Birleşmiş Milletler. *Viyana Antlaşmalar Hukuku Sözleşmesi*. (23 May 1969). UNTS 331.

Birleşmiş Milletler. *BM Kurucu Anlaşması*. (24 Ekim 1945). 1 UNTS XVI.

**Mahkeme Kararları**

*Nükleer Silahlara İlişkin Danışma Görüşü*. (1996). ICJ Rep, 35 I.L.M. 809.

*Kongo'daki Askerî Faaliyetler Davası*.(2005). ICJ 168 (Dem. Rep. Congo v. Uganda).

*Nikaragua'daki Askerî ve Yarı Askerî Faaliyetler Davası*.(1986). ICJ. 14. (Nicar. v. U.S.).

*Tadic Davası*. (1999). ICTY. IT-94-1-A.

**Online Raporlar**

Birlemiş Milletler.(1966). *Uluslararası Hukuk Komisyonu Yıllığı*. Vol 2.

USA National Security Council. (1963). *A Study on the Management and Termination of War with the Soviet Union***.** https://nsarchive2.gwu.edu/nukevault/ebb480/docs/doc%2011A%20war%20termination.pdf

Tikk, Eneken, Kaska, Kadri, ve Vihul, Liis. (2010) *International Cyber Incident: Legal Considerations*, Cooperative Cyber Defence Centre of Excellence. https://ccdcoe.org/publications/books/legalconsiderations.pdf

Albright, David., Brannan, Paul. ve Walrond , Christina. (2010). *Did Stuxnet Take Out 1,000 Centrifuges at the Natanz Enrichment Plant?*, ISIS Report. http://isis-online.org/isis-reports/detail/did-stuxnet-take-out-1000-centrifuges-at-the-natanz-enrichment-plant/

Ulaştırma Bakanlığı. (2013). *Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı.* https://www.btk.gov.tr/uploads/pages/2-1-strateji-eylem-plani-2013-2014-5a3412cf8f45a.pdf

Ulaştırma Bakanlığı. (2016). *2016-2019 Ulusal Siber Güvenlik Stratejisi. http://www.udhb.gov.tr/doc/siberg/2016-2019guvenlik.pdf*

**Diğer İnternet Kaynakları**

Albright, D., Brannan, P. ve Walrond, C. (2010). *Did Stuxnet Take Out 1,000 Centrifuges at the Natanz Enrichment Plant*. http://isis-online.org/isis-reports/detail/did-stuxnet-take-out-1000-centrifuges-at-the-natanz-enrichment-plant/

Baran, Paul (1963). *The Origins of the Internet.* http://www.rand.org/about/history/baran.html

ICANN. *What Does ICANN Do?.* https://www.icann.org/resources/pages/what-2012-02-25-en

Lipson, H. F. (2002). *Tracking and Tracing Cyber Attacks: Technical Challanges and Golobal Policy Issues.* http://www.dtic.mil/dtic/tr/fulltext/u2/a408853.pdf

Routers. (2010). *What is Stuxnet?* http://www.reuters.com/article/2010/09/24/us-security-cyber-iran-fb-idUSTRE68N3PT20100924

Schmitt, Michael N. ve Vihul, Liis. (2014). The Nature of International Law Cyber Norms. https://ccdcoe.org/sites/default/files/multimedia/pdf/Tallinn%20Paper%20No%20%205%20Schmitt%20and%20Vihul.pdf>, accessed 25 May 2015.

**Diğer**

Howard F. Lipson (2002). *Tracking and Tracing Cyber-Attacks: Technical Challenges and Global Policy Issues*. Doktora Tezi.

BM Genel Konseyi 2625 sayılı Kararı. (1970). *Devletler Arasında Dostane İlişkiler ve İşbirliğine Dair Milletlerarası Hukuk İlkleri Bildirisi.*

Uluslararası Hukuk Komisyonu. (2001). Devletin Haksız Fiilden Kaynaklanan Uluslararası Sorumluluğuna İlişkin Sözleşme Taslağı.