JOURNAL OF SOCIAL AND HUMANITIES SCIENCES RESEARCH

Uluslararası Sosyal ve Beşeri Bilimler Araştırma Dergisi

Open Access Refereed e-Journal & Refereed & Indexed

Article Type	Research Article	***Accepted / Makale Kabul***	16.07.2019
Received / Makale Geliş	14.04.2019	***Published / Yayınlanma***	17.07.2019

BİRLEŞMİŞ MİLLETLER ANTLAŞMASI, KUZEY ATLANTİK ANTLAŞMASI VE ULUSLARARASI HUKUK AÇISINDAN SİBER SALDIRILARIN TANIMLANMASI SORUNU

THE ISSUE OF DEFINING CYBER ATTACKS IN TERMS OF THE CHARTER OF THE UNITED NATIONS, THE NORTH ATLANTIC TREATY, AND INTERNATIONAL LAW

Dr. Hatice Kübra ECEMİŞ YILMAZ

Ankara Yıldırım Beyazıt Üniversitesi, Hukuk Fakültesi, Milletlerarası Hukuk Anabilim Dalı, Ankara / TÜRKİYE, ORCID: 0000-0001-9438-0291

ÖZET

Bu çalışmada siber saldırı, siber terörizm ve siber savaş kavramlarının açıklamaları, ayrıca uluslararası hukuk açısından bu kavramların nasıl değerlendirilmesi gereğinin üzerinde durulmuştur. Bu çerçevede uluslararası hukuk alanında siber saldırın tanımlanmasına ilişkin çalışmalar değerlendirilmiş, uluslararası hukuk kurallarının bu alanda geliştirilmesi için, hangi kurallardan yararlanılabileceği sorularına cevap aranmıştır. Siber saldırı, siber terörizm ve siber savaş kavramları değerlendirilirken hukukun temel ilkelerinden *jus ad bellum* ve *jus in bello* ilkelerinin, Birleşmiş Milletler Antlaşması 2(4), 39 ve 51. Maddelerinin, kodifikasyon çalışmaları çerçevesinde Uluslararası Hukuk Komisyonunun, Devletlerin Hukuka Aykırı Hareketlerinden Dolayı Uluslararası Sorumluluğu ile ilgili metninin 2, 3 ve 11. Maddelerinin, Kuzey Atlantik Antlaşması 3, 4, 5. Maddelerinin nasıl değerlendirilmesi gereğinin üzerinde durulmuştur.
Anahtar Kelimeler: Uluslararası Hukuk, Siber Saldırı, NATO.

ABSTRACT

In this research, concepts of a cyber attack, cyber terrorism, and cyber war are defined and how these concepts evaluate in the area of international law are emphasized. In this context, studies related to the definition of cyber attacks in international law are analyzed. In addition, questions concerning which rules can be used for developing international law rules in this field are explained. To understand concepts of cyber attack, cyber terrorism, and cyber war, the basic principles of law such as *jus ad bellum* and *jus in bello* principles, articles 2(4), 39 and 51 of the United Nations Convention, articles 2, 3 and 11 of the Responsibility of States for Internationally Wrongful Acts adopted by the International Law Commission, articles 3, 4, 5 of the North Atlantic Treaty are taken in consideration.
Keywords: International Law, Cyber Attack, NATO.

1. GİRİŞ

İnternet 1953 yılında kullanılmaya başladığında ağırlıklı olarak askeri iletişim amacıyla kullanılmıştır (Kumawat, 2016: 45- 48). İnternetin dünya çapında insanlar tarafından günlük hayat içinde veya devletlerarasında yaygın olarak kabul edilmesi 1989 yılına kadar sürmüştür (Kumawat, 2016: 45). Bu süreç içinde, internet kişisel alanlarda eğitim, sosyalleşme, oyun oynama, alışveriş yapma gibi insan hayatının her alanına işlemiştir. Benzer şekilde, devletlerarası platformda ise para transferi, savunma sistemlerini yönetme de yaygın olarak kullanılmaya başlanmıştır. Bu bağlamda internetin kişisel ve devletlerarası ilişkilerde dünyaya etki etmesinin son yıllarda katlanarak arttığı görülmektedir.

İnternetin bireyler ve devletlerarasında etkisi bu kadar artmışken, kötü niyetli olarak insanların ya da devletlerin birbirine karşı kullanımı da azımsanmayacak şekilde artış göstermektedir. Bu durum geleneksel suç tanımlarına ek olarak, siber suç kavramının ortaya çıkmasına sebep olmuştur. Siber suçlarda, siber suçlular kötü amaçlı yazılım aracılığıyla bilişim sistemlerinde siber saldırılar yaparak

sistemlerin kontrolünü ele geçirirler ve bilişim sistemlerinde saklanan hassas bilgilere erişimi sağlamış olurlar. Böylece siber suçlular, ele geçirdikleri hassas bilgileri kendi amaçlarına uygun olarak, yasadışı eylemlerde kullanırlar. Siber suç kavramı daha basit bir deyişle, resmi olmayan veya yasadışı eylemlere dahil etmek için bilişim sistemlerinin kullanılması olarak tanımlanabilir.

Günümüzde sıkça karşılaşılan siber suç örnekleri; internet dolandırıcılığı, kimlik hırsızlığı ve kredi kartı hesabı hırsızlıkları, devletlerarasında kanunsuz silah satımı ya da terörizme yasa dışı para aktarımı yani terörizm finansmanı gibi yasadışı faaliyetlerin bir bilgisayar ve internet kullanımı yoluyla işlenmesidir. Siber suçlar bireylerin kişisel hayatını etkilediği gibi, devletlerin bütünlüğü ve varlığı için ciddi tehditler meydana getirmektedir. Böylece güçlü güvenlik yöntemlerinin ve uluslararası yasaların oluşturulması, günümüz koşullarında devletlerin öncelikli ihtiyacı haline gelmiştir.

Devletlerin güvenlikleri için tehdit haline gelen siber saldırılar incelendiğinde, bazı araştırmacılar siber saldırıların savaş nedeni olduğunu kabul etmişlerdir. Yapılan siber saldırılar, savaş nedeni olan silahlı saldırı olarak kabul edildiğinde, savaş hukukunun geleneksel kuralları içerisindeki düzenlemelere tabi olması gerekmektedir. Önemli olan siber saldırıları klasik savaş hukuku kurallarına göre silahlı saldırı olarak kabul edilip edilemeyeceğinin tespitinin doğru yapılması ve kabul edilmesi durumunda savaş hukukundaki devletlerin kuvvete başvurma yasağının istisnası olan meşru müdafaa hakkının kullanıp kullanamayacağını belirleyebilmektir. Bu nedenlerden hareketle bu çalışmada, öncelikle siber saldırı, siber terörizm ve siber savaş kavramları tanımlanacak, bu bilgiler ışığında siber saldırı, siber terörizm ve siber savaş kavramlarının uluslararası hukuktaki tanımlanma sorunlarına, siber saldırının silahlı saldırı olup olmadığına, klasik anlamda devletlerin kuvvete başvurma yasağının istisnası olan meşru müdafaa hakkına siber saldırılar açısından başvurulup başvurulamayacağı, hangi koşullarda başvurulabileceği konularına yer verilmiştir. Tanımlama sorunları açıklanırken, uluslararası hukukun hangi alanında siber saldırıların düzenlenmeye çalışıldığı, Birleşmiş Milletler (BM) Antlaşması maddeleri, Kuzey Atlantik Antlaşması maddeleri göz önünde bulundurularak ve gelecek için, uluslararası hukuk açısından daha etkin düzenlemelerin nasıl yapılacağı üzerinde durulacaktır.

2. SİBER SALDIRI, SİBER TERÖRİZM, SİBER SAVAŞ KAVRAMLARI

2.1. Siber Saldırı

Bilgisayar ağları üzerinden online iletişimi sağlayan alan siber uzay olarak tanımlanmaktadır. Kara, deniz, hava ve uzay tanımlamalarından sonra siber uzay kavramı ile devletler ilgilenmekte ve devletlerin bu alanlarda gerçekleştireceği saldırıların savaş hukuku kurallarına tabi olup olmayacağı, siber uzayın devletlerin egemenlik alanlarının içerisine dahil edilip edilemeyeceği konusunda tartışmalar vardır. Bazı araştırmacılar, devletlerin siber uzay içerisinde mülkiyet haklarının olmadığını ve siber uzayın devletler tarafından ortak alan olarak kullanılmasının kabul edilmesi gerektiğini savunur (Nye, 2014: 3). Diğer araştırmacılar ise, devletlerin kendi ülkelerinde yetkileri dahilinde siber alanlarda faaliyette bulunabilmesinin, devletlerin siber uzayda egemenlik haklarını kullanabildiğini gösterdikleri düşüncesine sahiptirler (Lotrionte, 2012: 829).

Siber uzayda sadece bireyleri ve devletleri etkileyecek olumlu faaliyetler oluşacağı gibi, aynı zamanda silahlı saldırı niteliğini alan siber saldırılar gibi olumsuz faaliyetlerinde ortaya çıkabilmektedir. Nitekim, siber saldırılar, siber uzayda kişilerin ya da devletlerin bilgisayar ya da bilgisayar sistemlerine zarar vermek amacıyla yapılan saldırılar. Bu saldırıların sonucunda devletlerin ya da kişilerin açıkları bulunup, devletlerin ya da kişilerin önemli bilgileri ele geçirilir ya da önemli bilgileri silinerek yok edilebilir, ya da verilecek komutlarla sistemler kontrol altına alınabilir ve bunun neticesinde de yaralanmalara, hatta can kayıplarına bile neden olabilir. Örneğin, siber saldırılarla bir nükleer tesis sistemine girilerek, kontrollerinin yapılmasına engel olunabileceği gibi, toplumsal düzeninin oluşmasında önemli rol olan trafik ışıklarının kontrol sistemine girerek düzenin bozulmasına ya da hastane sistemindeki tahlil sonuçları değiştirilerek yaralanma, ölüm gibi sonuçlara neden olunabilir (Collin, 1996). Siber saldırıların, sadece örnekler dikkate alınarak tahdidi hükümler olarak tanımının yapılması zorluk gösterecektir.

Uluslararası hukukta siber saldırıların tanımı yapılırken siber savaş, siber terörizm, siber suç ya da siber saldırı tanımlamalarının ayırt edilmesi gerekmektedir. Bu ayırım yapılmadığında ve her siber saldırının

devletlerin birbirlerine karşı yaptığı saldırılar olarak düşünüldüğünde, bu terime savaş hukuku terimlerinin içerisinde yer verilmesi gerekecektir.

Dünya üzerine bakıldığında siber saldırıların tanımlanması, bunların uluslararası hukuk normu olarak savaş hukuku içerisine dahil edilip edilemeyeceğine karar verilebilmesi adına, bazı devletlerin kendi iç hukuklarına uygun olarak tek başlarına ya da birkaç devletin birleşip örgüt oluşturarak yaptığı düzenlemeler mevcuttur (Hathaway vd; 2012: 824). Amerika Birleşik Devletleri (ABD) Siber Komutanlığı askeri amaçlı kullanım için siber saldırıları ele almış ve resmi olarak siber saldırıları tanımlamıştır. Tanımlama yapılırken objektifliğini korumak için özellikle siber saldırılarının sınırlandırılması düşmanca hareketlerle siber sistemlere zarar vermek şeklinde yapılmıştır (Hathaway vd; 2012: 825). Şangay İşbirliği Örgütü ise siber saldırıları tanımlarken daha geniş bir tanımlama yapmış ve ulusal yaklaşımdan ziyade yeni bilgi edinme ve iletişim sistemlerinin uluslararası güvenlik düzeyinde endişeleri artırdığını, bu endişelerle birlikte sivil ve askeri alanı bozacak tehditler oluşturduğunu ve bu nedenlede mücadele edilmesi gerektiğini belirtmiştir (Agreement between the Governments of the Member States of the Shanghai Cooperation Organization on Cooperation in the Field of International Information Security, 61st Plenary Meeting). Özellikle örgüt burada siber saldırılar için zararlı bilgilerin nasıl iletildiğini açıklamakta ve siber saldırıların sosyal ve politikal sistemlere zarar verip, bu düzenleri bozacağını ifade etmektedir. Örgütün siber saldırıları tanımlarken, siyasi istikrarı da içine alarak, daha kapsamlı bir ifade kullandığı görülmektedir. Buradan da anlaşılmaktadır ki, ulusal ve uluslararası yapılanmalar siber saldırıyı tanımlarken, ortak ifade kullanmamış, uygulamada zorluk ve karmaşıklık çıkaracak biri amaç, diğeri araç bazlı ifadeler kullanılmıştır (Hathaway vd; 2012: 826-828). Tanımlama yapılırken amaç ve araç öğelerine dayalı ayrı tanımlama yapmak yerine ikisini de kapsayan bir tanım yapmak gerekmektedir.

Siber saldırıların ayırımı konusuna bakıldığında, bazı özellikler dikkate alındığında belirli gruplara ayırıldığı görülmektedir. Siber saldırılar, özneleri dikkate alınarak yapılan tanımlamalara göre, devletler ve kişiler tarafından yapılabilmektedir. Yapılan siber saldırıların nesneleri dikkate alındığında, yine bu siber saldırılar devletlere ve kişilere karşı yapılabilmektedir. Siber saldırıların sonuçları dikkate alındığında da siber saldırıların bilgisayar sistemini etkileyip doğrudan siber dünyaya zarar veren maddi zararlara, bilgisayar sistemini etkileyerek dezavantaja neden olan zararlara, bunlardan kaynaklı kişileri de etkileyerek can kaybı ya da diğer zararlara neden olabileceği görülmektedir. Bu noktada belirtilmesi gereken husus, kimlik avcılığı, internet dolandırıcılığı gibi siber suçlar devletlere karşı değil kişilere karşı işlendiği ve uluslararası güvenliği tehdit edecek unsurlar içinde yer almadığı için, uluslararası hukuk içerisine girecek siber saldırıların kapsamı ve tanımlaması içerisinde yer almayacaktır. Ancak diğer açıdan bakıldığında siber saldırıların uygulanma yöntemleri, amaçları ve hedef aldıkları gruplar dikkate alındığında, siber saldırıların terör faaliyetlerine de konu olabileceği görülmektedir. Burada siber uzayda kimlik tespitinin zor olması, ya da siber ortamda oluşan terör faaliyetlerin ortaya çıktığı mekanının tespit edilememesi gibi durumlar uluslararası hukuk açısından siber uzayda gerçekleşen siber terörizm kavramının da tanımlanıp, uluslararası hukuk açısından değerlendirilebilmesini gerekli kılmaktadır. Nitekim dünya üzerindeki ABD, Çin, Rusya, İran, İtalya, Hollanda, Macaristan gibi devletler uluslararası hukuk açısından uygulanan kuvvet kullanma yasağının siber faaliyetler açısından da uygulanabilir olduğunu belirtmişlerdir (Roscini, 2014: 44). Yine Avrupa Birliği ve BM gibi uluslararası örgütler de uluslararası hukukun siber faaliyet alanlarına da uygulanabileceğini savunmaktadırlar. Bu duruma en iyi örnek BM Uzmanlar Heyeti tarafından 2013 ve 2015 yılında yazılan raporlarda, siber uzaya uluslararası hukuk kurallarının uygulanabileceği belirtilmiş olmasıdır.

Siber saldırılara karşı uluslararası hukuk kurallarının uygulanabilmesi BM şartında yer alan kuvvet kullanma yasağının, meşru müdafaa hakkı ve silahlı saldırıya karşı uygulanacak kuralların uygulanabileceğini göstermektedir. Siber saldırılara karşı kuvvet kullanmanın ön şartı olan ve 51. Maddede yer alan "silahlı saldırı" kavramına ve siber saldırının ne zaman silahlı saldırı boyutuna geçeceği burada açıklanmayıp, bu konulara ileriki bölümlerde yer verilecektir. Ancak burada BM şartına ilave siber saldırılarla ilgili olan hukuki metin NATO bünyesinde ki Tallinn El Kitabından da bahsetmekte fayda bulunmaktadır. Burkadze' ye göre Tallinn El kitabı bağlayıcı değildir (Burkadze, 2018: 223-224). Burkadze bunu söylerken Professor Schmittin Tallinn el kitaplarını, hukukun tali, yani ikincil kaynaklarından biri olarak açıkladığını görüşüne dayanarak, tali kaynaklarında sadece varolan kuralları açıklayabilecek nitelikte olduklarını, yeni, hiç olmamış kurallara vücut verip yeni kural yaratamayacak nitelikte oldukları görüşünü bildirmektedir (Burkadze, 2018: 224). Birinci ve ikinci

versiyonu olan bu El kitabı uluslararası hukuktaki kuvvet kullanma yasağı, meşru müdafaa hakkı ile ilgili kurallar dikkate alınarak hazırlanmıştır. Tallinn El Kitabı'nın ikinci versiyonunda "Kuvvet Kullanma" bölümünün altında, 68. Kuralda Kuvvet Kullanma ve Tehdidi Yasağına, 69. Kuralda kuvvet kullanmanın (kuvvet kullanma yasağına aykırılık için siber saldırının etkisi, boyutunun göz önünde bulundurulması gerektiğini belirtiyor), 70. Kuralda kuvvet tehdidinin açıklamalarına yer verilmiştir. Yine Kural 71,72,73,74 ve 75 siber saldırıya karşı meşru müdafaayı açıklamaktadır (Tallinn Manual 2.0). Tallinn El Kitabı "Devletler ve Siber Uzay", "Güç Kullanımı", "Genel olarak Siber Silahlı Çatışma Hukuku", "Düşmanca Davranışlar", "Belirli Kişiler", "Nesneler", "Faaliyetler", "İşgal ve Tarafsızlık" başlıkları altında ilgi kurallardan oluşmaktadır (Schmitt, 2013).

2.2. Siber Terörizm

Genel olarak savaş hukuku tanımlamalarına bakıldığında kuvvet kullanımını sınırlayan ve düzenleyen *jus ad bellum* kuralları ve silahlı çatışmalar esnasında uygulanacak kuralları kapsayan *jus in bello* kuralları karşımıza çıkmaktadır (Sur, 2018: 290-291). *Jus ad bellum* ilkesi kuvvete başvurma yasağı içerisinde yer almaktadır. Ayrıca, BM Antlaşması 2(4) Maddesi, devletlerin birbirleri ile olan ilişkilerinde, devletin bütünlüğünü veya siyasi bağımsızlığına karşı, BM'nin amaçlarına aykırı her türlü kuvvet kullanımını ve tehdidini sağlayan hareket ve davranışları yapmayı yasaklamıştır. Ancak, kuvvete başvurma yasağının meşru müdafaa ve meşru müdahale şeklinde istisnaları da vardır. Bir devletin diğer devlete karşı meşru müdafaada bulunması bir silahlı saldırı ya da pek yakın ve kesin tehlike halinde mümkündür. Burada tartışmalı husus muhtemel tehlikelere karşı meşru müdafaaya başvurulup başvurulamayacağı hususudur (Robertson, 2002: 121-145; Gündüz, 2018: 126-127). Meşru müdafaa kapsamına BM Güvenlik Konseyinin de benimsediği bir hususta teröre destek olan devletlere karşı alınacak önlemler bakımından ağır ve ciddi terör hareketlerine destek mevcutsa orantılılık ilkesine aykırı olmamak kaydı ile meşru müdafaa çerçevesinde devlete karşı kuvvet kullanılabileceği görüşüdür (Sur, 2018: 290-291).

Terörizm, uluslararası hukuk alanında baskın bir konu haline gelmiştir ve uluslararası toplumun içinde zayıf devletlerin terörizmle mücadele etmesi konusunda devletlerin yanında olmayı desteklemektedir. 11 Eylül 2001 tarihinde gerçekleşen insanlığa karşı suçların en kanlılarından biri olan terör eylemi de göstermiştir ki, terörizm uluslararası düzene, insan haklarına karşı küresel çatışmanın en üst noktalarındadır. Terör faaliyetlerine uluslararası platformda bakıldığında, bu faaliyetler genellikle uluslararası antlaşmalar ile düzenlenmiş olan uluslararası hukuk kurallarının birçoğunun ihlalcileridir.

Genel olarak, terörizm, bir eylem veya korku uygulaması ve bir kişiyi veya bir grup insanı başka türlü yapamayacakları bir şey yapmaya (ya da yapmamaya) zorlama tehdidi olarak tanımlanabilir (Saraçlı, 2018). Devletler, araştırmacılar ve farklı örgütler terörizmi tanımlama konusunda bir fikir birliğine varamamış ve farklı tanımlamalar önermiş ve kullanmışlardır. Hem BM hem de ABD terörizmin tanımını yaparken genellikle belirli faaliyet alanlarını dikkate almıştır, ancak yine de buna rağmen terörizmle ilgili olarak genel bir tanımlama yapılamamış ve bu alanda genel tanımlama itibariyle hukuki boşluklar oluşmuştur.

Terörizmin tanımını tayin ederken belli elementlerin ölçüm aracı olarak kullanılması gerekir. Bunu yapmanın amacı hangi hareket ve davranışların terör hareketi olarak tanımlanıp kabul edilebileceğinin çerçevesinin belirlenmesidir. Terörizmin unsurlarından ilkinin 'şiddet' olması gerekmektedir.

Terörizmin temelinde, şiddet hareketinin yayılmasıyla toplumun geneline korku salmak ve bu salınan korkuyla birlikte vatandaşların devletlere olan güvenini sarsarak, toplum içinde kaos yaratma amacı yatmaktadır (Gençtürk, 2018: 3-4). Hangi davranışların şiddet olup olmadığına bakılması için ilk izlenilebilecek yol, şiddet suçlarının kanunlarda listelenmesidir. Hangi suç ve davranışların kanunlarda terörizm faaliyeti olarak kabul edileceği liste halinde tanımlandığında, bu listedeki davranış ve hareketleri gerçekleştirerek suç işleyenler 'şiddet' unsurunu gerçekleştirmiş kabul edileceklerdir. Listelenmiş olan şiddet hareketlerinin dışında ulusal ya da uluslararası hukuk kurallarında yapılması açıkça yasaklanmış olan davranış ve hareketlerde 'şiddet' öğesi içine oturtulacaktır. Diğer bir deyişle, terörizmdeki şiddet unsuru 'öldürme, yaralama' gibi listelenmiş şiddet oluşturan suçları kapsamakla birlikte, diğer uluslararası hukuk normlarında ciddi şekilde şiddet unsuru olarak kabul edilen hareket ve davranışları da kapsamaktadır.

Terörizmi diğer eylemlerden ayıran bir diğer unsurda ideoloji unsurudur (Gençtürk, 2018: 3-4). İdeoloji hareket noktasını oluşturur ve aynı ideolojiyi benimseyenler, aynı hedefe yönelirler. İdeoloji burada bir şekilde terörizmin gerçekleştirmek istediği, ulaşmak istediği hedefidir. Buradaki hedef genellikle devletlere meydan okuma ile ortaya çıkar. İdeoloji gerçekleştirilirken şiddet unsuru da kullanılmış olur. Artık şiddet unsuru ideolojiyi gerçekleştirmek için araç konumuna gelmiştir. Burada üzerinde durulacak bir konuda hedef unsurudur. Terörizm faaliyetlerinde gerçekleştirilmek istenen ideoloji doğrultusunda bir hedef belirlenir. Örnek olarak bir devlete saldırmak veya korkudan etkilenmesini sağlamak için binalara ya da kişisel alanlarına saldırarak hedefi insan unsuru olarak belirlemek verilebilir. Eylemin amacı, genel sivil nüfusta ciddi şekilde teröre neden olmak veya devletlerin veya herhangi bir uluslararası örgütün normalde yapacağı şeyi yapmasından kaçındırmak, ya da yapmayacağı şeyleri yapmasına zorlamak olarak tanımlanabilir. Burada iç içe geçmiş diğer bir unsurda örgütleşmedir. Bunun anlamı sempatizanlıktan kaynaklanan, iki ya da daha fazla kimsenin aynı amaç etrafında birleşmesidir. Bu örgütleşme uluslararası toplumun barış ve güvenliğini tehdit eder. Terörizmde örgütleşme ile bir şekilde devletlere meydan okuma vardır. Bu meydan okuma devletlerin iradelerini bertaraf etmek için saldırılarda bulunarak kendini gösterir.

Tüm bu açıklamalara bakıldığında terörizm kişilere ya da devletlere zarar vermeyi amaçlayan ciddi derecedeki şiddet eylemlerini; amacı etnik, siyasi, ideolojik olarak nitelendirilen telkin edici hareketleri; sivil nüfusu, belirli kişileri veya toplumdaki kişileri ciddi korku sağlayarak etkisinde bırakmaya çalışan hareketleri; devletleri ya da uluslararası örgütleri bir şey yapmaya ya da bir şey yapmaktan kaçınmaya zorlamak için tasarlanmış hareketlerin tamamını kapsamaktadır (Yılmaz, 2006: 153). Uluslararası hukuk açısından değerlendirildiğinde, uluslararası hukukta terör ve terörizm tanımlamaları için tam bir anlaşma sağlanamamıştır. Her devlet kendi menfaatine göre tanımlamaları farklı şekilde yapmıştır.

Bu nedenledir ki bu kavramları tamamen yasaklayan tek bir antlaşma metni yoktur. Ancak çeşitli uluslararası sözleşmelerle terörizm önlenmeye çalışılmış ve bu sözleşmelerin 1373 sayılı BM Güvenlik Konseyi kararı (Güvenlik Konseyi'nin 28 Eylül 2001 günü 4385 inci oturumunda kabul edilen (2001) 1373 sayılı Kararı) ile tüm devletlerin taraf olması ve hükümlerini yerine getirmesi yükümlülükleri dile getirilerek işlerlik kazanılması sağlanmaya çalışılmıştır. Terörizmin tanımlanmasında bile tam olarak birliktelik sağlanamamışken, siber terörizm kavramını açıklamak daha da zor bir hal almaktadır.

Siber terörizmi tanımlarken öncelikle siber terör kavramının da açıklanması gerekir. Siber terör kavramı; kişilere, kurumlara, uluslara zarar vermek amacıyla kullanılan bilgisayarlarla ağlara kritik alt yapılara ve sistemlere zarar verme olarak tanımlanırken, siber terörizm belirli bir politik veya sosyal amaca ulaşabilmek için bilgisayar ve bilgisayar sistemlerine zarar vererek bir devleti veya toplumu yıldırma, baskı altında tutma olarak açıklanabilir (Saraçlı, 2018).

Siber terörizme bakıldığında ağ ataklarını, zararlı yazılımları siber uzayda ortaya çıkararak, kanunsuz ve etik dışı faaliyetleri kritik altyapı ve devletlerin veya uluslararası örgütlerin kritik bilgisayar sistemlerini hedef alıp, devletlerin, uluslararası örgütlerin kritik sistemlerini durdurmak, yavaşlatmak, ekonomik zarara uğratmak suretiyle veyahut yapılan müdahalelerle devletin insanlarını korkutarak, yaralayarak, ölümlerine sebep olarak belli bir ideolojik, politik yapıyla kanunsuz olarak ortaya çıkmaktadır. Ayrıca, terörle ilişkilendirilebilecek hareketlerin siber ortamda kullanılması ya da terör örgütlerinin siber ortamı bir araç olarak kullanıp faaliyetlerini etkin bir hale getirmesi hallerinde de siber terörizm ortaya çıkmış olacaktır.

Genellikle siber terörizmin oluşması için gerekli zemin, siber terörizmi oluşturan gruplara destek olan, politik ya da siyasal hedeflerine ulaşmayı amaçlayan arka plandaki devlet veya devletler tarafından hazırlanmış olur. Arka plandaki devletler tespit edildiğinde de uluslararası alanda siber savaşların başlaması için altyapı oluşmuş olacaktır. Siber terörizm kavramı ilk kez 1980 yılında Barry Collin tarafından teröristlerin faaliyetlerini gerçekleştirmek için ya da eylemlerini kolaylaştırmak adına dijital bilgi sistemleri, ağları ya da bunların eklentilerini uluslararası derecede kötüye kullanmak olarak tanımlanmış ve bu terim kullanılmaya başlanmıştır (Collin, 1996). Ayrıca Collin'e göre siber terörizm gelecekte bankaları, ekonomik güçleri bozabilir, hava araçlarının ya da demiryolu araçlarının trafik düzenlerini bozup kazalara neden olabilir, ilaç firmalarına sızıp ilaç formüllerini bozacak niteliğe sahip olabilir (Collin, 1996). Bazı yazarlara göre siber terörizm kavramının olması için büyük dereceli yıkım ya da ölüm olaylarının olması gerekmektedir (Conway, 2002). Uluslararası siber suç ve terörizm tasarısında da siber terörizm, meşru bir otorite olmadan siber sistemlere yönelik şiddet, bozmaya da

siber sistemlere karşı müdahalede bulunularak, kişi ya da kişilerin yaralanmalarına, ölmelerine, toplumsal kargaşaya, ciddi derecede mülkiyete, ekonomik zarara neden olmaktır (A Proposal for an International Convention on Cyber Crime and Terrorism Article 1(2)).

Siber terörizmin globelleşen dünya da yayılmasını engelleyerek, bu konuda bir an önce çözüm bulunulması gerekmektedir. Çünkü siber terörizm ile ucuz bir şekilde, daha az mali kaynakla, sınır tanımadan, uzaktan terör faaliyetlerinin daha büyük kitlelere ulaşabilmesi mümkündür ve bunları yapanlarının kimliklerinin de tespiti ve ispatlanması çok güçtür. Yine siber terörizm suçu aynı anda birden fazla devlete karşı da işlenebileceği için, uluslararası hukuk açısından değerlendirilip, devletler arasında iş birlikleriyle uluslararası hukuk kapsamında bu sorunun çözüme kavuşturulması önem teşkil etmektedir.

2.3. Siber Savaş

Teknolojik çağda, siber savaşı cazip hale getiren birtakım avantajlarının olmasıdır. Siber savaşı cazip hale getiren avantajları şu şekilde sıralamak mümkündür; siber savaşın ucuz maliyetli olması, tanınma veya bulunma olasılığının düşük olması, sınır tanımaması yani istediği anda istediği mekâna rahatlıkla ulaşması, beklenmedik anda ve beklenmedik şekilde saldırıda bulunabilinmesi, böylelikle karşı tarafa savunma imkânı vermemesi ve bunu yaparken de risk faktörünün çok düşük olması, ayrıca etki alanı geniş olurken istenmediği sürece can kaybının çok az olmasıdır. Devletlerin bu yönleri dikkate alarak gerçekleştirdiği siber savaşlarına örnek 2007 Estonya ve 2008 Gürcistan Savaşlarıdır (Ashmore, 2009; O'connell, 2012: 188). Ayrıca, 2009 ABD ve İsrail'in İran' a düzenlediği Stuxnet saldırısı da siber saldırılar arasında uluslararası platformda önemli olanlardandır (O'connell, 2012: 192- 193). 2007 yılında Estonya'da gerçekleşen savaş Tallinn şehrindeki Bronz Askeri adlı anıtın yerinin değiştirilmesinden doğmuştur. NATO üyesi olan Estonya'nın internet erişimi kısıtlanmış, acil durum aramaları servisi devre dışı kalarak, insanların hayatı tehlikeye atılmıştır. Estonya'ya yapılan bu saldırının Rusya tarafından olduğunu iddia ederken, Rusya bu iddiayı kabul etmemiştir (O'connell, 2012: 192). Saldırı sonrasında Estonya siber savaş birimi oluşturmuştur. Yani burada gerçekleştirilen siber saldırı NATO müttefiklerinin ilgisini çekerek, NATO Siber Savunma Mükemmeliyet Merkezi Tallinn'de kurulmuştur. Daha sonra uzman akademisyenlerin birleşmesi ile yazılan Tallinn El Kitabı uluslararası hukukta siber savaşın yerini ve NATO müttefiklerinin bu konuda uygulayabileceği kuralları kapsamaktadır. Daha önceki siber saldırılardan farklı olarak Estonya saldırısında, sadece bir devletin değil, aynı ya da benzer yöntemler kullanılarak, gelecekte tüm devletlere zarar verilebilme ihtimali kavranmıştır.

2008 yılında Güney Oseta topraklarına yönelik Gürcistan operasyon başlatmıştır. Bunun takibinde Rusya Gürcistan'a karşı klasik savaşın yanında siber savaşta başlatmıştır (O'connell, 2012: 192- 193). Rusya Gürcistan'a yaptığı siber savaş ile devletin internet trafiğini destekleyen yönlendirici sistemini ele geçirmiş, bunun takibinde Gürcistan'da cep telefonu, banka işlemleri dahil birçok donanım kullanılamaz hale gelmiştir. Saldırı sadece Gürcistan'a yapılmayıp, Gürcistan yanlısı Rusya'ya ait sitelere de saldırı yapılmıştır. Rusya, Gürcistan Hükümetinin saldırıların arkasında Rusya'nın olduğuna dair iddialarını kabul etmemiştir.

Dünya üzerinde önemli olan bir diğer siber saldırın etkisi İran Nükleer tesislerinde ABD kaynaklı Stuxnet isimli virüs nedeni ile gerçekleşen kazalarda görülmüştür (Çelik, 2013: 137- 175; O'connell, 2012: 194 vd.). Virüsün çalışması sisteme bulaşıp, etkisi altına alıp, daha sonra da tesisleri imha etmesiyle ortaya çıkmıştır. Stuxnet'in en önemli özelliği internet bağlı olmadan da bilgisayarları veri girişi yapılan araçlarla ele geçirebilecek olmasıdır. Stuxnet saldırısına kadar yazılımlara, ağlara zarar verildiği görülürken, Stuxnet'ten sonra siber uzaydan yapılan saldırı ile fiziki olarak zararlar meydana gelmiştir. Stuxnet saldırısından sonra dünyayı nükleer savaş tehdidi ile korkutan İran, siber saldırılar açısından da dünyayı korkutmaya başlamış ve siber gücünü artırmıştır. Buna karşılık ABD de siber saldırıların uluslararası alanda da etkili olduğunu savunmuş ve İran ve diğer siber donanımlarla güçlü devletlere karşı savunmaya geçilmesi gerektiğini belirtmiştir.

Karşılaşılan noktada, teknolojik gelişmelerin artmasıyla uluslararası platformda fiziksel savaşların yerini, uluslararası siber savaşların alabileceği endişesi ortaya çıkmaktadır. Bu nedenle de uluslararası platformda siber savaşlar hakkında ortak düzenlemeler yapılmalıdır. Ayrıca yapılacak uluslararası düzenlemelere bağlı olarak da devletlerin kendi iç düzenlemelerini uluslararası hukuk kurallarına

uydurmaları gerekmektedir. Tedbirler alınmadığı sürece, küçük bir hareketle uluslararası alanda bu kadar etkili olan siber savaşlar çıkabilecek ve hukuki boşluklar nedeniyle, dünya toplumlarının sosyal hayatlarını önemli derece etkileyecek sorunlar ortaya çıkabilecektir.

3. SİBER SALDIRI, SİBER TERÖRİZM VE SİBER SAVAŞIN ULUSLARARASI HUKUKTA TANIMLANMA SORUNU

3.1. Jus in Bello ve Jus ad Bellum

Uluslararası Hukuk alanında, hangi eylemlerin ya da hangi silahlı çatışmaların savaş sayılıp sayılmayacağı konusunda objektif ölçütler olmadığı için, her devlet tarafından ortakça kabul edilen 'savaş' tanımı yapılmamıştır. Devletlerin savaşı tanımlamada ki ölçütleri, genel itibari ile kendi menfaatleri ile doğru orantılıdır. Siber savaşlar için de uluslararası hukuk alanında kesinleşmiş bir tanımı olmadığı gibi siber savaşın gerçek bir savaş mı olduğu konusunda da tartışmalar devam etmekte ve tehlikeler daha da büyümeden uluslararası hukuk alanında bu boşluğun doldurulması gerekmektedir.

Siber savaşın tanımlanmasının ve gerçek savaş statüsünün verilip verilmemesi, siber savaşa karşı silah kullanımına ilişkin uluslararası hukuk kurallarının ve teamüllerinin uygulanıp uygulanmamasını değerlendirmek açısından önem taşımaktadır.

Uluslararası silahlı çatışmalar, savaş ve savaşa varmayan silahlı çatışmalar olarak uluslararası hukukta ikiye ayrılmaktadır (Pazarcı, 2007: 529). Savaş suçlarını tanımlayan Lahey Sözleşmesinden sonra, 1949 tarihli Cenevre Sözleşmesi silahlı çatışmalar hukuku ile ilgili savaş veya savaşa varmayan silahlı çatışmalar üzerine uygulanacak kuralları düzenlemektedir. Uluslararası hukuka bakıldığında da kuvvete başvurulduğunda uyulması gereken kurallar yani *jus in bello* ilkesi ile kuvvete başvurma hakkı *jus ad bellum* arasında ayırıma gidilmiş ve silahlı çatışmalarla ilgili hukuk kurallarının uygulanması da *jus ad bellum* hakkına sahip olunmasına bağlı kılınmıştır (Pazarcı, 2007: 529).

Johnson'a göre *jus in bello* kavramı "haklı savaş" ilkesinin modern dünyaya yansıma şeklidir. Yine Johnson'a göre *jus ad bellum* ise *jus in bello*daki kurallardan bir sapmayı temsil etmektedir (Kolasi, 2017: 1-29). *Jus in bello* savaşa başvurmanın devletler tarafından bir hak olduğu kabul edilen dönemde *jus ad bellum*a kıyasen daha fazla gelişip, yayılmıştır (Kolasi, 2017: 1-29). Savaşın haklı olması tarihi dönemlerde üç şarta bağlanmıştır. Bunlardan birincisi, yapılacak olan savaşın kişisel olarak değil, belli bir otoritenin altında yürütülmesi gerekmektedir. İkincisi yapılacak savaşın haklı bir sebebe dayanması gerekir. Üçüncüsü ise, yine yapılacak olan savaşın iyi olanı desteklemek, korumak gibi ya da kötü olanı uzaklaştırmak gibi doğru bir amaca sahip olması gerekmektedir (Kolasi, 2017: 1-29; aktaran: Dinstein, 2012:66).

Savaşın haklı sebebe dayanmasını sağlayan bu kriterler zaman içerisinde *jus ad bellum* kriterleri haline gelmiştir. *Jus in bello*nun parçası olan orantılılık, savaşın son çare olması gibi kavramlarda daha sonra bu kriterlere eklenmiştir (Kolasi, 2017: 1-29; aktaran: Yalçınkaya, 2008: 127).

Modern uluslararası hukuk kurallarına baktığımızda, *jus ad bellum* ve *jus in bello* kavramları birbirinden bağımsız kavramları ifade etmektedir. *Jus ad bellum* kuvvete başvurmanın meşruluğu ile ilgili iken, günümüzde kullanılan bu terim BM Antlaşması Madde 2(4) ve VII. bölüme dayanmaktadır. Devletlerin elinde olan *jus in bellum*u takdir etme yetkisi BM Antlaşması ile BM'ye bağlanmıştır. 1928 *Briand* Paktından itibaren *jus ad bellum*un temel özelliği uluslararası alanda kuvvet yasağını geniş tutup, kuvvet kullanımını asgari düzeyde ve istisnai durumlarda kabul etmiş olmasıdır.

Jus in bello kavramına bakıldığında *jus in bello*nun görevi, çatışmaya katılmayanları veya çatışmaya katılmaktan vazgeçenleri korumak ya da onları bağışlamak, düşman güçlerini durdurmak ya da etkilerini azaltmak için kullanılacak şiddet miktarını sınırlı tutmaktır.

Yeni tür olarak ortaya çıkmaya başlayan savaşlara bakıldığında, bu savaşlarda yer alan devlet dışı aktörlerin *jus in bello*ya tabi olmasına engel bir neden olmamasına rağmen, bu aktörlerin *jus in bello*yu ihlal etme veya *jus in bello*yu hiçe sayma potansiyeli yüksektir.

Siber savaşın uluslararası hukuk ilkelerinden *jus ad bellum* yani kuvvete kullanma hakkına veya *jus in bello* yani silahlı çatışmalar esnasında uygulanacak kuralların kapsamına uygulanıp uygulanamayacağı konusu önem taşımaktadır. *Jus in bello*nun temel ilkelerine baktığımızda çatışan ve çatışmayan

arasındaki ayırımın yapılması, çatışma dışı olanlara saldırını yasaklanması, orantılılık ilkesi, savaşın son çare olması ilkeleri dikkat çekmektedir. Silahlar olarak da gereksiz acıya sebep olan, zarar veren tüm silahlar, sivil ya da asker ayırımı yapmaksızın yasaklanmıştır. Siber saldırıların da *jus in bello* ilkesinin içerisinde haklı nedene dayanarak başvurulması, orantılılık, çatışanlara uygulanıp ya da çatışmayanlara uygulanmaması ve tarafsızlık ilkelerinin kapsaması açısından bu ilkeye başvurmada sorunlar oluşabilecektir.

3.2. Siber Saldırı Silahlı Saldırı Olarak Kabul Edilebilir Mi?

Öncelikle hangi kuvvet kullanma faaliyetinin silahlı saldırı olduğunu tespit etmek gerekecektir. Hangi faaliyetlerin silahlı saldırı olduğunu tespit etmek, silahlı saldırı kavramının tanımlamasının BM şartında yapılmaması dolayısı ile önemlidir. BM Genel kurulunun 1974 tarih 3314 (XXIX) sayılı kararla saldırının tanımı yapılmış, bu karardaki hükümde, hangi eylemlerin silahlı saldırı olarak değerlendirilebileceklerine dair atıfta bulunulmuştur (Gündüz, 2018: 120). Ancak burada yapılan tanımlama bir genel kurul kararıdır ve bağlayıcı bir hukuki belge değildir (Gündüz, 2018: 120). Belgenin bağlayıcı nitelikte olmamasına rağmen Uluslararası Adalet Divanının Nikaragua Kararında bu belgeye başvurmuş olması belgenin belli noktalarda bağlayıcı olabilmesine destek göstermektedir. Kararın 4. Maddesine göre; Madde 3'ün içerisinde sayılan fiiller tahdidi değildir ve Güvenlik Konseyi, Birlişmiş Milletler Antlaşması hükümlerine göre başka fiillerin de saldırı olabileceğini tespit edebilir (Gündüz, 2018: 121). Buradan anlaşılması gereken bir devletin düzenli silahlı kuvvetleri açısından başka bir devletin topraklarını yani ülkesini işgal etmesi, kaçınılmaz olarak zaten silahlı saldırı kabul edilecektir. Ancak işgal derecesine varmadan farklı nitelikteki silahlı kuvvet kullanımı, ki burada siber saldırılar da bu gruba dahil edilebilir, silahlı saldırı sayılıp sayılamayacağı hususunda tartışmalarda yine BM Genel Kurulu kararının 3. Maddesinden faydalanılmaktadır. Ancak 4. Maddedeki açıklamaya dayanılarak, 3. Maddede sayılan durumların tahdidi olarak belirlenmemiş olması, belirli bir ağırlığa ulaşan siber saldırıların da silahlı saldırı olarak kabul edilmesine imkân tanımaktadır. Bir siber saldırı, silahlı bir saldırının eşiğini karşılıyorsa, silahlı çatışmalar hukuku otomatik olarak uygulanır ve meşru müdafaa hakkını kullanmak, hakkı işgal edilmiş bir devlet için bir seçenektir. Bir saldırı gerekli olan ölçüyü karşılamıyorsa, etkilenen devlet sadece saldırganlara karşı güç kullanma hakkına sahip olacaktır, aksi takdirde kendileri kuvvet kullanma yasağını ihlal etmiş olabilecektir. Her bir siber saldırının silahlı saldırı boyutuna ulaşıp ulaşmaması ölçüsünün ve etkilerinin Tallinn El Kitabına, uluslararası örgütlerin belgelerine, doktrinsel görüşlere yer verilerek belirlenmesi, objektif bir tanım yapılabilmesi açısından önemlidir. 2008 yılında Rusya ve Gürcistan arasındaki siber saldırılar, mevcut bir uluslararası silahlı çatışmanın bir parçası olduğu için silahlı çatışmalar hukukuna ait olduğu düşünülmüştür.

Klasik anlamda bir çatışmada, eylemler, kullanılan kuvvetin derecesine değil, etkileriyle veya sonuçlarıyla değerlendirilmektedir. Kinetik ataklar, doğrudan yaralanmaya, ölüme veya mülkün zarar görmesine ve sınırları aşmasına neden olması halinde silahlı saldırı olarak kabul edilir. Kinetik saldırılar, doğrudan zarara, yaralanmalara veya ölüme veyahut mala zarar vermeleri ve sınırları aşmaları, yani önemli derecede olmaları durumunda, silahlı bir saldırı olarak kabul edilir. Tallinn El Kitabına göre, bir siber saldırının kişisel veya maddi zarara neden olması ve bu tür bir zararın bir devletin egemenliğini ihlal etmesi durumunda, kuvvet kullanımına ilişkin bir ihlalin de meydana geleceği açıktır (Grange, 2014: 17- 18). Bu çerçevede, bir siber saldırı, Devletin kilit ağının tam kontrolünü ele geçirirse ve bu kontrol, kişilerin yaralanmasına, ölümüne veya zarar görmesine neden olursa, bu eylem, saldırıya uğrayan devletin BM 51. Maddeye dayanarak bir kuvvet kullanımı olarak meşru müdafaa hakkını tetikleyen silahlı bir saldırı oluşturacaktır (Grange, 2014: 17-18). Devlet egemenliğini ihlal edecek kadar büyük bir ölçekte fiziksel zarar meydana gelirse ve siber saldırının bir sonucu olarak fiziksel değiştirmeler gerekiyorsa, yasadışı bir güç kullanımı oluşturan silahlı bir saldırı olmuş olacaktır.

3.3. Siber Saldırılarda Meşru Müdafaa Hakkı Kullanılabilir Mi?

Bir örf adet kuralı olan meşru müdafaa hakkı BM Antlaşması Madde 51'de ele alınmıştır ve devletlerin kendi ülkelerini saldırıya karşı korumak, yine ülkelerini saldırıya karşı kurtarmak için kuvvet kullanılması bir hak olarak kabul edilmiştir (Sur, 2018: 290-291). Meşru müdafaanın koşullarının gerçekleşmesi için öncelikle bir silahlı saldırı veya pek yakın ve kesin bir tehlike olmalıdır. Yani muhtemel, olası tehlikeler meşru müdafaa için yeterli değildir. Burada önleyici meşru müdafaadan bahsedilecek olunursa bu tartışmalı bir konudur. Önleyici meşru müdafaa özüne bakıldığında klasik

anlamda ki meşru müdafaanın geniş yorumlanması ile ilgili bir durumdur. Silahlı saldırının varlığı ile silahlı saldırının olması ihtimalinin yüksek olması eş değer tutulmuştur. BM antlaşmasından önce meşru müdafaa için yapılan tanımlamalarda, önleyici meşru müdafaa hakkı gereklilik, oranlılık ve zaman bağlantısı ilkelerine uygun olması şartlarının müdafaayı da kapsamaktaydı. Ancak BM Antlaşmasından sonra madde metninde meşru müdafaa için silahlı saldırının da olması gerektiği açıkça yazılı olduğu için, önleyici meşru müdafaanın, meşru müdafaa sayılamayacağına dair de görüşler ortaya çıkmaktadır (Karadağ, 2016: 171-186).

Meşru müdafaanın koşullarına tekrar dönülecek olunursa bu koşullardan biride, müdafaanın orantılı olması gerektiğidir. Meşru müdafaa da önceki duruma getirme amacı unutulmamalı ve bu sınırlama ile meşru müdafaada bulunulmalıdır. Ayrıca BM Antlaşması Madde 51'e göre BM Güvenlik Konseyine alınan meşru müdafaa tedbirleri bildirilmelidir.

Siber saldırının silahlı saldırı kabul edilerek, meşru müdafaa hakkını doğuracağına dair üç yaklaşım bulunmaktadır. Bunlardan birincisi, araç yaklaşımı, ikincisi hedef yaklaşımı ve üçüncüsü de etki yaklaşımıdır. Araç bazlı yaklaşımda BM Genel Kurulunun 3314 sayılı kararın saldırı tanımı dikkate alınarak, siber saldırıların klasik silahlar grubuna girmemesi nedeniyle, silahlı saldırı kategorisine giremeyeceği ve meşru müdafaadan yararlanamayacağıdır. Hedef bazlı yaklaşımda, muhtemel zararlar dikkate alınacağı için meşru müdafaaya başvurmak için siber saldırılar silahlı saldırı olarak kabul edilecektir. Ancak, hedef bazlı yaklaşımda kilit nokta olarak kabul edilecek alt yapı sistemlerinin neler olduğunu tespit etmede tartışmalar ortaya çıkacaktır. Etki bazlı yaklaşıma göre, gerçekleşen siber saldırıların sonucunun yaratacağı etki oranı yoğun olursa, bu siber saldırı silahlı saldırı olarak kabul edilecek ve meşru müdafaa hakkı diğer koşullarında varlığı halinde uygulanabilecektir. Ancak meydana gelecek zararın etkisinin tespitinin hangi koşullara göre karara bağlanacağı hususu yine tartışmaya açık olacaktır (Hathaway vd; 2012).

Siber saldırılarla ilgili olarak meşru müdafaa ilkesi ele alındığında, sadece siber saldırının varlığı meşru müdafaa için yeterli değildir ve meşru müdafaa hakkının siber saldırılar üzerinde kullanılabilmesi için, siber saldırının silahlı saldırı boyutunda gerçekleşmesi gerekmektedir. Tallinn El Kitabına göre de siber saldırı silahlı saldırı boyutuna ulaştığında kullanılacak meşru müdafaa tedbirinin sadece siber uzayla sınırlı olması gerektiğine dair bir kural bulunmamaktadır. Bu nedenle başvurulacak meşru müdafaanın orantılı olması yeterli olacaktır. Ayrıca meşru müdafaanın ilkelerinden olan önceki duruma getirme amacı ele alındığında, silahlı saldırı boyutuna ulaşan siber saldırılarla ilgili uygulanacak meşru müdafaanın bu sınırlama ile kullanılması gerekmektedir.

4. BM ANTLAŞMASI VE KUZEY ATLANTİK ANTLAŞMASI KAPSAMINDA SİBER SALDIRI

4.1. Birleşmiş Milletler Antlaşması 2(4), 39, 51. Maddeleri ve Devletlerin Hukuka Aykırı Hareketlerinden Sorumluluğu Bağlamında Siber Saldırı

Bu çalışmanın amaçlarından biri hangi şartlarda ve ne zaman siber saldırıların bir askeri saldırı olarak kabul edilip, karşı devletin kendini savunma hakkına sahip olup kendini savunma için gerekli harekete geçmesi gerektiği idi. Diğer bir soru ise *jus ad bellum* ilkesine başvurmada ortaya çıkar ve *jus ad bellum* ilkesine başvurulmuş olsa bile BM Antlaşması Madde 2(4) de yer alan "*Tüm üyeler, uluslararası ilişkilerinde gerek herhangi bir başka devletin toprak bütünlüğüne ya da siyasal bağımsızlığına karşı, gerek BMin amaçları ile bağdaşmayacak herhangi bir biçimde kuvvet kullanma tehdidine ya da kuvvet kullanmasına başvurmaktan kaçınırlar.*" ifadesinin uygulanıp uygulanamayacağıdır.

Eğer siber saldırıların etkisi silahlı saldırıların etkileriyle eşdeğer kabul edilirse, burada siber saldırıları devletlerin kendilerini savunma amacıyla kullanabilmesi gerekecektir. Ancak, burada silahlı saldırılara eşdeğerlilikte nesnel kurallar olmadığı için problemler ortaya çıkacaktır. Bu gibi sorularda O'Connell' in görüşü, ortaya çıkan durumların çoğunda siber saldırıların uluslararası hukuktaki kuvvet kullanımı kriterlerini yerine getirmediğidir (Buchan ve Tsagourias, 2012: 183-186). Bu nedenle, uluslararası hukuktaki kuvvet kullanımının siber saldırılar için kullanılamamasıdır. Yine O'Connell'e göre uluslararası hukukun koruduğu iletişim, ekonomi hakları ile ilgili sözleşmelerde siber aktivitelerin düzenlenmesi, uluslararası hukuktaki kuvvet kullanımı ilkesine göre düzenlenmesinden daha fazla kabul edilebilir bir durumdur (Buchan ve Tsagourias, 2012: 184). BM Antlaşmasının 2(4) Maddesine göre,

üye devletler kuvvet kullanmaya ilişkin yetkilerinden Güvenlik Konseyi lehine vazgeçmişlerdir. Ayrıca, Uluslararası Adalet Divanının Nikaragua Kararı'ndan da anlaşılacağı gibi uluslararası hukukta kuvvet kullanmayı yasaklayan ilkeler artık uluslararası teamül hukukunun bir parçası haline gelmiş ve bu nedenle de tüm devletler için bağlayıcı olduğu kabul edilmektedir. (Nikaragua Kararı'nda 1986 tarihinde Uluslararası Adalet Divanı, bir devletin başka devlet topraklarına silahlı asker olmayan çeteleri göndermesi de, bu saldırıların düzenli ordu saldırılarıyla eşdeğer olması gerekçesiyle, BM Antlaşmasının 51. Maddesindeki silahlı saldırıları oluşturacağını kabul etmiştir. Divan Nikaragua'nın müdahalesine yapılan karşı müdahaleyi bir haklılık sebebi görmemiştir. Daha az ağırlığa sahip kuvvet kullanımı içeren kolektif karşı tedbire, silahlı saldırı karşısında kolektif meşru müdafaa hakkı vermesine rağmen, haklılık kazandırmayacağını belirtmiştir. Üçüncü devlet ABD tarafından alınan tedbirleri haklı kılmamıştır).

Buchan, bir devletin bilgisayar ağına karşı saldırının BM Antlaşmasının Madde 2(4)' ün amaçları için yasadışı bir güç kullanımını teşkil edip etmediğini değerlendirmiştir (Buchan ve Tsagourias, 2012: 184). 2010 yılında İran'a karşı siber saldırıyı örnek olarak kullanan Buchan, bir siber saldırının fiziksel hasar ürettiği (ölüm, yaralama gibi eylemleri gerçekleştirebildiği gibi, fiziksel anlamda mala zarara vermeyi de içerdiğini dikkate alarak) kuvvet yasağı kullanımını ihlal edeceği sonucuna varmıştır (Buchan, 2012: 220- 221). 2007 Estonya'daki gibi siber saldırı sadece fiziki olmayan zarar vermiş olduğunda hukuksuz olarak kuvvet kullanımı olarak nitelendirilemeyeceğini, ancak bununla birlikte, Buchan, böyle bir siber saldırının, doğada zorlayıcı olarak değerlendirilebileceği, müdahalede bulunmama ilkesini ihlal edeceğini, bu da saldırının mağdur devleti bir politika değişikliğine zorlama niyetiyle konuşlandırıldığını iddia etmektedir (Buchan ve Tsagourias, 2012: 185). Estonya, İran ve diğer devletlere karşı yapılan ve gün geçtikçe artmaya başlayan siber saldırılar, siber savaş ve siber terörizmin ciddiyetini ortaya koymaktadır.

BM Antlaşmasının 2(4) Maddesi, aynı antlaşmanın 39 ve 51. Maddelerindeki istisnalar hariç, tüm devletlere aynı şekilde uygulanır. Madde 39'a göre, Güvenlik Konseyi uyuşmazlığı inceleyerek dünya barışının ihlal edilip edilmediği veya saldırının fiilen işlenip işlenmediğini karara bağlayarak zorlama tedbirlerini uygulatabilecektir. Ancak, bu madde de aynı antlaşmanın 41 ve 42. Maddelerine atıf yapılarak alınacak önlemlerin ne şekilde alınabileceği sıralanmış, ayrıca önlemlerin yetersiz kaldığı ya da kalacağı kanısı ortaya çıkarsa da hava, deniz ve kara kuvvetleri aracılığı ile uluslararası barış ve güvenliğin korunması ve yeniden kurulması sağlanacağı belirtilmiştir. Burada barış tehdidini gerçekleştirecek eylemleri belirleyecek olan Güvenlik Konseyi ve yine gerekli saydığı her tür kara, hava, deniz kuvvetleri girişiminde bulunacak yine Güvenlik konseyi olduğu için, tarafsız olmasından şüphe etmek gerekecektir. Ayrıca siber saldırının karşılığında uygulanacak gücün kara, deniz ya da hava kuvvetleri aracılığıyla karşılanacak olması, karşı kuvvetin uygulanmasındaki oranlılık ilkesine uygun olup olmadığı da şüphelidir. BM Madde 2(4)' ün istisnası olan diğer bir madde ise Madde 51'de yer alan meşru müdafaa hakkıdır.

Uluslararası hukuk ve silahlı çatışmalar hukuku açısından konu değerlendirildiğinde BM Antlaşması'nın 51. Maddesindeki "Bu Antlaşma'nın hiçbir hükmü, BM üyelerinden birinin silahlı bir saldırıya hedef olması halinde, Güvenlik Konseyi uluslararası barış ve güvenliğin korunması için gerekli önlemleri alıncaya dek, bu üyenin doğal olan bireysel ya da ortak meşru savunma hakkına halel getirmez..." ilkesine dayanarak meşru müdafaa hakkını kullanabilmesi gerekmektedir. Burada siber saldırıların bir silahlı saldırı seviyesinde olup olmadığını tespit etmek sorunu ortaya çıkacaktır. Eğer siber saldırı olarak yapılan saldırı, silahlı saldırı niteliğinde ve ölçüsünde değilse Madde 51'deki meşru müdafaa hakkının kullanılması mümkün olmayacaktır. Aslında gelişen dünyada 'silahlı saldırı' terimini sadece klasik anlamdaki silahların kullanıldığı saldırı olarak tanımlamak eksik ve yetersiz kalacaktır. Aslında Madde 39'da Güvenlik Konseyi'nin tespit edeceği eylemleri 'saldırı' terimi ile ifade ederken bu askeri silah ve güçleri kapsarken, Madde 51' deki 'silahlı saldırı' terimi ile daha dar anlamlı bir terim kullanılmıştır.

Siber alanda gerçekleşen saldırılar göstermektedir ki, siber terörizm ve siber savaş kavramları gerçek ve saldırı zamanı ile karşı tarafa etki yaratacağı an aynı olduğu için, daha gelişen teknolojileri de ortaya koymamasına rağmen etkili kavramlardır. Siber saldırılarda kullanılan tekniklerin basit düzeyde olmaması nedeniyle, siber anlaşmazlık olduğunda etki alanı bakımından birçok devleti aynı anda siber savaşın içine dahil edebilecektir. BM Antlaşması Madde 2(4)'te açıkça belirtir ki üye olan tüm devletler

uluslararası ilişkilerinde herhangi başka devletin toprak bütünlüğüne ya da siyasal bağımsızlığına karşı ya da BM'nin amaçları ile bağdaşmayacak herhangi bir şekilde kuvvet kullanma ya da kuvvet kullanma tehdidinde bulunmaktan kaçınacaklardır. Ancak siber saldırıların BM Antlaşmasındaki ifadelerin içerisine dahil edilmesi hukuki açısından siber saldırlar tam olarak tanımlanmamışken problem yaratacaktır.

Bir devletin diğer bir devlete karşı başlattığı siber saldırılarda egemenlik hakkını açık olarak ihlal etmesi vardır. Uluslararası hukukun temel prensiplerinden biri de devletin egemenlik haklarına ve devletin bütünlüğüne saygı duymaktır. Devletlerin birbirine karşı yaptığı ve daha sonra siber terörizm veya siber savaşlara da neden olabilecek siber saldırılar, karşı devletin egemenlik alanı içerisine dahil edilen teknik alt yapısına karşı işlenilmiş olduğundan, devletin egemenliğine karşı işlenmiş sayılacaktır. Ancak, burada devletin egemenliğine karşı siber saldırının gerçekleşmiş olmasından şüphe olmamasına rağmen, siber saldırıyı işleyenin uluslararası hukuk platformuna dahil edilebilecek bir süje olup olmadığını tespit açısından zorluklar meydana gelmektedir. Eğer siber saldırı bir devlete atfedilebilirse, uluslararası hukuk bakımından da tespit alanını tanımlamak kolaylaşmış olacaktır. Bu da uluslararası alanda siber terörizm, ya da siber savaş için ön adım olan siber saldırıların bir devlet tarafından yapıldığının kabul edilmesi ile anlaşılabilir. Devletlere atfedilememe problemi, siber saldırıların hukuki olarak problem olmaya devam etmesine neden olmaktadır. Çünkü bu saldırıyı devletin içinden bir grup, devletine karşı işlediyse, bu uluslararası hukukun içerisinde yer alan bir konu olmanın dışına çıkmış olacaktır. 'Responsibility of States for Internationally Wrongful Acts' olarak isimlendirilen uluslararası hukukta devletlerin hukuka aykırı olarak gerçekleştirdiği hareketlerin sorumluluğu Uluslararası Hukuk Komisyonu tasarısına göre tanımlanırken 2. Maddesinde açıkça uluslararası hukuk açısından eylemin haksız olup olmadığının tespiti için devletin bilerek ya da ihmal ile gerçekleştiği bir davranışın, devletin uluslararası hukuktan doğan yükümlülüğünü ihlal etmesi ve bunun da uluslararası hukuk kapsamında devlete atfedilebilir olması gerektiğinden bahsetmiştir. Burada devletin egemenlik alanı içerisine saldırı gerçekleştiği için uluslararası hukuktan doğan yükümlülüğü ihlalde bir sorun olmamakla birlikte, devlete karşı isnat etmede problem olabileceği gözükmektedir. Bu nedenle de bu saldırıyı yapanın devlet tarafından yapılmasının zımni ya da açık olarak kabul edilmesi gerekmektedir. Eğer devletin davranışı kabul etmesi varsa, yine aynı belgenin 11. Maddesine dayanarak devlete atfedilemeyecek davranışı, devletin söz konusu davranışı kendi kabul etmesiyle ve benimsediği ölçüde uluslararası hukuk açısından devletin eylemi olarak kabul etmek gerekecektir.

Ancak burada sorun olan aynı belgenin 3. Maddesinde yer alan devletlerin yaptığı davranışın hukuka aykırı davranış olarak kabul edilmesi için, davranışın uluslararası hukuk kurallarına göre aykırı davranış olması gerekmektedir. Bir devletin kendi iç hukukunda davranışın hukuki olması, aykırı davranışın karakterini belirlemede ölçüt değildir. Siber saldırıların hukuka aykırı bir davranış kabul edilmesi için de uluslararası hukuk kuralları içerisinde ne zaman hukuka aykırı davranış olduğu ve olacağının tanımlanmış olması gerekmektedir. Ancak uluslararası hukukta siber saldırıların hangi aşamada uluslararası hukuka aykırı olacağı tanımlanmamıştır. Bu nedenle de uluslararası hukuk açısından gün geçtikçe artan bir korku haline gelen siber saldırıların uluslararası hukuk açısından hangi kurallara tabi olması gerektiğinin bir çerçevesinin çizilmesi gerekmektedir. Ancak burada uluslararası hukuk alanında kurallar belirlenirken, siber saldırıları sadece ceza hukuku ya da savaş hukuku gibi dar kalıplara sığdırmaya çalışmamalı, uluslararası siber güvenlik hukuku alanında yeni bir sistem oluşturulup sadece siber saldırılara yönelik, uluslararası bir metin oluşturulması gerekmektedir.

Uluslararası hukukta siber saldırılara ilişkin hukuk normları oluşturulurken, tanımlamaların devletlerin kendi sınırları içerisinde gerçekleşecek siber saldırı faaliyetleri değil, sadece uluslararasında etkin olan hukuka aykırı saldırı ve hareketler tanımlanmalıdır. Tanımlamalar yapılırken, geleceğe yönelik gelişecek teknolojiler dikkate alınmalı ve çerçeve hükümler oluşturulmalıdır. Bu çerçeve hükümler hangi hareketlerin uluslararası alanda siber saldırı olduğunu, hangi hareketlerin siber savaşa neden olacağını, devletlerin hangi hareketlerinin siber terörizme yardım etmek anlamında olduğunu tanımlamakla başlayacaktır. Tanımlamalar yapıldıktan sonra devletlerin hareket ve davranışlarının iç hukuklarına uygunluğunu dile getirerek sorumluluktan kurtulamayacağını ve tüm devletlerin iç hukuktaki siber saldırı düzenlemelerinin, uluslararası hukukta yeni oluşturacak sözleşmeye uygun olarak düzenlemeleri gerektiğini, saldırıların bir devlete ait olduğunu belirlemek içinde, devletlerin işbirliği içerisinde, ortak olarak çalışması gerektiğini ve bu ortak çalışmanın nasıl yapılması gerektiğinin tanımlamalarının yapılması gerekmektedir.

4.2. Kuzey Atlantik Antlaşması Kapsamında Siber Saldırı

Siyasi tarihin en önemli uluslararası kuruluşlarının başında gelen Kuzey Atlantik Antlaşması Örgütü (NATO), ortak bir savunma örgütü olarak Soğuk Savaşın başındaki Sovyet tehdidine karşı kurulmuştur. NATO'nun kurulmasının asıl amacı üye olan devletlerin dışarıdan gelecek, yani dış güçlerden gelecek saldırılara karşı ortak savunma yapmalarını sağlamaktır. Bu bağlamda Kuzey Atlantik Antlaşması'nın 5. Maddesinden de açıkça anlaşılacağı gibi üye devletlerden birine yapılan saldırı tüm üye devletlere karşı yapılan saldırı olarak kabul edilmektedir ve üye devlete silahlı saldırı yapılması doğrultusunda, üye olan diğer devletlerin saldırıya uğrayan üye devlete karşı BM 51. Maddesine dayanarak bireysel veya kolektif olarak yardım etme sorumlulukları vardır. Ayrıca yine aynı antlaşma, Kuzey Atlantik bölgesinin güvenliğini sağlamak ve sağlanan bu güvenliğin devamını sürdürebilmek amacıyla üye devletlere silahlı güce başvurabilme hakkı tanımaktadır.

Son derece etkili bir örgüt olan NATO kapsamında, 2018 yılında siber alanda da güvenliğin sağlanması amacıyla üye olan müttefik devletlerin gönüllü katılımları ile Siber Uzay Operasyonları Merkezinin oluşmasına ve müttefiklerin ulusal siber güçlerini nasıl bu ittifak operasyonlarına dahil edebileceklerine dair karar verilmiştir. Siber Uzay Operasyon Merkezinin oluşturulma amacı, siber uzay güvenliğinin sağlanması konusunda farkındalık yaratarak, siber uzay operasyonları ile ilgili uyumu sağlamaktır. NATO kapsamında ki siber uzay faaliyetleri daha da artmaktadır. 2018 yılının Haziran ayında Müttefikler Operasyon alanı olarak Siber Uzayla ilgili Vizyon ve Stratejiyi onaylanmıştır (Brent, 2019). 2019 yılı içerisinde de bunun müttefikler tarafından onaylanması ile tamamlanması beklenmektedir.

Kuzey Atlantik Antlaşmasının 3. Maddesi ve 5. Maddeleri dikkate alındığında, siber saldırılar silahlı saldırı boyutunda gerçekleştiğinde, antlaşmaya taraf olan müttefik devletler bireysel ya da kolektif olarak iş birliği içerisinde olabileceğinden, Siber Uzay Operasyon Merkezinin oluşturulması ile aynı anda oluşturulan Siber Savunma Taahhüdü ile de bu maddeler desteklenmeye çalışılmaktadır. Ancak temel kriterlerin kesin olarak belirlenmemiş olması, ortaya çıkacak duruma göre bu iş birliğinin sağlanacak olması, burada NATO'nun belirlediği özel kriterlere sahip olmayı gerektirecektir ve kolektif savunma otomatik bir mekanizma olmayacaktır (Burkadze, 2018: 221). Kuzey Atlantik Konseyi siber saldırıların düzeyini ve kolektif savunmayı gerektirmesi için gerekli durumları belirlerken amaç, süre, yoğunluk ve orantılılık ile gerçekleşen siber saldırının iç kaynaklardan mı dış aktörlerden mi kaynaklandığı adımlarını dikkate almaktadır (Burkadze, 2018: 221).

Burada silahlı saldırı boyutunun altında kalan faaliyetlerin de Kuzey Atlantik Antlaşmasının 4. Maddesinin dikkate alınarak değerlendirilmesi söz konusu olabilir (Brent, 2019). Antlaşmanın 4. Maddesine göre, antlaşmaya taraf olan müttefik devletlerden birinin toprak bütünlüğünün, siyasi bağımsızlık veya güvenliğinin tehdit edilmesinde, antlaşmaya taraf devletlerin birbirleri ile iletişime geçip danışma yapmaları mümkündür.

Diğer yandan, siber saldırılara NATO tarafından kolektif iş birliği oluşturmak için faaliyetlerin tespitinde sorun teşkil edebilecek husus, siber saldırının gerçekleştiği alanın tespitidir. Çünkü siber saldırının gerçekleştiği siber alanla, gerçek coğrafya aynı olmayabilir. Her ne kadar 2016 yılı Temmuz ayında gerçekleşen Warsaw Zirvesinde siber alanı, NATO'nun kendisini havada, karada ve denizde olduğu kadar etkili bir şekilde savunması gereken bir operasyon alanı olarak tanımlasa da (Burkadze, 2018: 222), siber alanın belirlenmesi açısından zorluklar olacaktır.

Bu nedenle, Kuzey Atlantik Antlaşması tek başına, yeni bir düzenlemeye sahip olmadan gelecekte şiddetini tahmin edemeyeceğimiz siber saldırılara karşı devletlerin bireysel ve kolektif savunmaları için yeterli olmayacaktır. Schmitt'in Tallinn El Kitabını da ikincil kaynak olarak tanımladığı, bu nedenle de bağlayıcı kaynak olmayacağı dikkate alındığında, gelecekte devletlerin etkin bir şekilde siber saldırılara karşı bireysel ve birlikte savunma haklarını kullanabilmeleri için yeni uluslararası bir düzenlemenin yapılması gerekecektir.

5. SONUÇ

Siber terörizm ve siber savaş uluslararası hukuk içerisinde analiz edilmesi açısından karmaşık bir yapı ortaya koymaktadır. Uluslararası hukuk ve uluslararası hukukun genel kuralları içerisinde siber terörizmi ve siber savaşı içerisine alacak makul seçenekler mevcuttur, ancak bu tür saldırıların niteliği ve hangi noktalara kadar varabileceği henüz tam anlamıyla yaşanmadığı için, devletlerin uluslararası

hukukun katkısını aktif olarak güçlendirmek için gerekli tedbirleri alması bakımından eksiklikler ortaya çıkmaktadır. Devletlerin tek başlarına siber güvenliklerini gözden geçirmeleri, siber saldırı, siber terörizm ve siber savaşlara karşı kendi alt yapılarını kurma seçenekleri mevcuttur. Devletlerin tek başına aldıkları tedbirlerden uzaklaşıp, uluslararası alanda bu eylemleri gerçekleştirmesi ile ilgili hukuki düzenlemelerde eksiklikler vardır.

Bu çalışmanın sonucuna bakıldığında, gelişen teknoloji de göz önünde tutularak siber terörizm ve siber savaşlara karşı tüm devletlerin uymaya zorunlu hale getireceği tek elden uluslararası hukuk sözleşmesi hazırlanıp, uluslararası hukuk alanındaki temel ilkelere dayandırılarak siber terörizmi, siber savaşı oluşturacak hareketleri, eylemleri tanımlayıp, hangi hallerde devletlerin kuvvet kullanma hakkına sahip olacağının, hangi eylemlerin açıkça yasaklanmış olacağının belirlenmesi, katalog halinde tanımlanması gerekmektedir. Burada çözülmesi gereken en önemli sorunlardan biri de yapılan tanımlamalarda siber saldırının, siber terörizmin ve siber savaşı başlatacak hareketin bir devlete hangi şartlarda isnat edilebileceğinin kesin sınırlarla belirlenmesi gereğidir. Her ne kadar var olan uluslararası hukuk kuralları, BM Antlaşma maddeleri, NATO uygulamaları, Tallinn El Kitabı ile bunlar sağlanmaya çalışılsa da, bunlar yeterli değildir. Uluslararası hukukta siber saldırı, siber terörizm ve siber savaş ilkelerinin tanımlamaları yapılırken, temel hak ve hürriyetlerin korunması, ölçülülük ilkesine riayet edilmesine dikkat edilmelidir. Karar alma süreçlerinde taraf devletlerin katılımının sağlanması, güvenlik kullanımı konusunda bir denge ve uyumun sağlanması, uluslararası iş birliği ile devletlerin kendi mevzuatlarını da yeni yapılacak uluslararası sözleşmeye uygun olarak düzenlemesi gerektiği göz önünde bulundurulmalıdır. Ayrıca, bu çalışmanın sonucuna göre, siber saldırı, siber terörizm ve siber savaş; hukuki, teknik, politik, ekonomik, sosyal tüm boyutlarıyla birlikte ele alınarak uygun tanımlamaların yapılması ve devletlere ait saldırıların tanımlaması yapılırken devletlere isnat sorununu ortadan kaldırmak için, devletlerin uluslararası hukuk platformunda birlikte hareket etmeleri gerekliliği vurgulanmalıdır. Devletlerin gerekli verileri iş birliği içerisinde toplaması gerektiği, yeni uluslararası sözleşme metnine eklenmelidir.

KAYNAKÇA

Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems, Aralık 2018 tarihinde https://rm.coe.int/168008160f. adresinden alınmıştır.

Agreement between the Governments of the Member States of the Shanghai Cooperation Organization on Cooperation in the Field of International Information Security, 61st Plenary Meeting, Aralık 2018 tarihinde; https://s3.amazonaws.com/ceipfiles/pdf/CyberNorms/Multilateral/ Shanghai +Cooperation+Organization+Agreement+on+Cooperation+in+the+Field+of+International+Info rmation+Security+6-16-2009.pdf adresinden alınmıştır.

ASHMORE, W. (2009), *Impact of Alleged Russian Cyber Attacks* Ocak 2019 tarihinde; https://www.bdcol.ee/files/files/documents/Research/BSDR2009/1_%20Ashmore%20-%20 Impact %20of%20Alleged%20Russian%20Cyber%20Attacks%20.pdf adresinden alınmıştır.

BESLİU, D. (2017), Cyber Terrorism-A Growing Threat in the Field of Cyber Security, *International Journal of Information Security and Cybercrime*, 6 (2), 35-39.

Birleşmiş Milletler Antlaşması, Aralık 2018 tarihinde; https://www.tbmm.gov.tr/komisyon /insanhaklari/pdf01/3-30.pdf adresinden alınmıştır.

BRENT, L. (2019), NATO'nun Siber Uzaydaki Rolü, Nisan 2019 tarihinde; https://www.nato.int/docu/review/2019/Also-in-2019/natos-role-in-cyberspace-alliance-defence /TR/index.htm adresinden alınmıştır.

BUCHAN, R. (2012), Cyber Attacks: Unlawful Uses of Force or Prohibited Interventions, *Journal of Conflict and Security Law*, 17(2), 211-228.

BUCHAN, R., TSAGOURİAS, N. (2012), Cyber War and International Law, *Journal of Conflict and Security Law*, 17(2), 183-186.

BURKADZE, K. (2018), A Shift in NATO's Article 5 in the Cyber Era?, *The Fletcher Forum of World Affairs*, 42(2), 215- 226.

COLLIN, B. (1996), The Future of CyberTerrorism, *Proceedings of 11th Annual International Symposium on Criminal Justice Issues*, Nisan 2019 tarihinde; http://www.crime-research.org/library/Cyberter.htm adresinden alınmıştır.

CONWAY, M. (2002), Reality bytes: Cyberterrorism and terrorist 'use' of the Internet, *First Monday*, 7(11).

ÇELİK, Ş. (2013), Stuxnet Saldırısı ve Abd'nin Siber Savaş Stratejisi: Uluslararası Hukukta Kuvvet Kullanmaktan Kaçınma İlkesi Çerçevesinde Bir Değerlendirme, *Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi*, 15(1), 137-175.

DİNSTEİN, Y. (2013), Cyber War and International Law: Concluding Remarks at the 2012 Naval War College International Law Conference, *International Law Studies Series*, 89, [i]-287.

FİDLER, D., PREGENT, R., ve VANDURME, A. (2013), NATO, Cyber Defense, and International Law, *St. John's Journal of International & Comparative Law*, 4(1), 1-25.

GENÇTÜRK, T. (2012), *Terör Kavramı ve Uluslararası Terörizme Farklı Yaklaşımlar*, Aralık 2018 tarihinde http://sam.baskent.edu.tr/makaleler/tgencturk/TerorUluslararasi.pdf adresinden alınmıştır.

GRAHAM, D. (2010), Cyber Threats and the Law of War, *Journal of National Security Law & Policy*, 4(1), 87-102.

GRANGE, M. (2014), Cyber Warfare and the Law of Armed Conflict, Nisan 2019 tarihinde https://core.ac.uk/download/pdf/41339676.pdf adresinden alınmıştır.

GÜNDÜZ, A. (2018), *Milletlerarası Hukuk*, 9. Baskı, Ankara: Savaş Yayınları.

Güvenlik Konseyi'nin 28 Eylül 2001 günü 4385 inci oturumunda kabul edilen (2001) 1373 sayılı Kararı, http://www.masak.gov.tr/media/portals/masak2/files/mevzuat/terorun_finansmani/uluslararasi_mevzuat/BirlesmisMilletler/BM_1373_Karar.htm adresinden Aralık 2018 tarihinde alınmıştır.

HATHAWAY, O., CROOTOF, R., LEVİTZ, P., ve NİX, H. (2012) The Law of Cyber-Attack, *California Law Review*, 100 (4), 817-886.

KARADAĞ, U. (2016), Birleşmiş Milletler Antlaşması'na Göre Meşru Müdafaa Hakkı, *İnönü Üniversitesi Hukuk Fakültesi Dergisi*, 7(2), 171- 186.

KOLASİ, K. (2017), Savaşın Değişen Niteliği ve Jus ad bellum ve Jus in bello'ya Etkisi, *İnsan Hakları Yıllığı*, 35, 1-29.

KUMAWAT, M. (2016), E-commerce, Cyber Crime and Indian Cyber Law, *International Journal of Law*, 2(1), 45-48.

LİN, H. (2012), Cyber Conflict and International Humanitarian law, *International Review of the Red Cross*, 94(886), 515-532.

LOTRIONTE, C. (2012), State Sovereignity and Self Defence in Cyberspace: A Normative Framework for Balancing Legal Righs, *Emory International Law Review*, 26.

MAKARİM, E. (2010), Cyber Terrorism Prevention and Eradication in Indonesia and Role and Functions of Media, *Indonesian Journal of International Law*, 7(3), 542-561.

MARCEL, I. (2013), The Components of Cyber-Terrorism, *International Journal of Information Security and Cybercrime*, 2(1), 49-58.

MİHAİ, I. (2012), Study on Cyber Attacks over Time and Cybercrime Evolution in Romania, *International Journal of Information Security and Cybercrime*, 1(1), 68-79.

MURPHY, J. (2013), Cyber War and International Law: Does the International Legal Process Constitute a Threat to U.S. Vital Interests, *International Law Studies Series*, 89, [i]-340.

NYE, J. (2014), The Regime Complex for Managing Global Cyber Activities, *The Centre for International Governence; Global Commission on Internet Governance: Paper Series*, 1.

O'CONNELL, M. (2012), Cyber Security without Cyber War, *Journal of Conflict and Security Law*, 17 (2),187-210.

PAZARCI, H. (2007), *Uluslararası Hukuk*, Ankara: Turhan kitabevi.

PETKİS, S. (2016), Rethinking Proportionality in the Cyber Context, *Georgetown Journal of International Law*, 47 (4),1431-1458.

POOL, P. (2013), War of the Cyber World: The Law of Cyber Warfare, *International Lawyer*, 47(2), 299-324.

ROBERTSON, Jr. H. (2002), Self-Defense Against Computer Network Attack Under International Law, *International Law Studies*, 76, 121-145.

SARAÇLI, M. (2007), Uluslararası Hukukta Terörizm, *Gazi Üniversitesi Hukuk Fakültesi Dergisi,* 9 (1-2), 1049- 1078.

SCHMİTT, M. (2011), Cyber Operations and the Jus in Bello: Key Issues, *International Law Studies Series*, 87, 89-112.

Responsibility of States for Internationally Wrongful Acts, Ocak 2019 tarihinde; http://legal.un.org/ilc/texts/instruments/english/draft_articles/9_6_2001.pdf adresinden alınmıştır.

SCHMİTT, M. N. (Ed.). (2013), *Tallinn Manual on the International Law Applicable to Cyber Warfare*, Cambridge: Cambridge University Press.

SCHMİTT, M. N. (Ed.). (2017), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, Cambridge: Cambridge University Press.

SECAREANU, M. (2014), The New Scientific Revolution - Types of Cyber Attacks Police Taken into Consideration on a European and International Level, *Public Security Studies / Studii de Securitate Publica*, 3(2), 215-220.

SHACKELFORD, S. (2009), From Nuclear War to Net War: Analogizing Cyber Attacks in International Law, *Berkeley Journal of International Law*, 27(1),192-252.

STAHN, C. (2006), *'Jus ad bellum', 'jus in bello' . . . 'jus post bellum'?* -Rethinking the Conception of the Law of Armed Force, *European Journal of International Law*,17(5), 921-943.

SUR, M. (2018), *Uluslararası Hukukun Esasları,* İstanbul: Beta.

YILMAZ, Ö. (2006), İspanya Terörle Mücadele Tecrübesi: Medeniyetler İttifakı Olabilir mi?, *Terörizm: Terör, Terörizm ve Küresel Terörle Mücadelede Ulusal ve Bölgesel Deneyimler*, Ankara: Uluslararası Stratejik Araştırmalar Kurumu Yayını.