ULUSLARARASI HUKUKTA SİBER SALDIRILARA KARŞI KUVVET KULLANMA*

CYBER WAR AND USE OF FORCE AGAINST CYBER ATTACKS IN INTERNATIONAL LAW

Mehmet YAYLA**

Özet: Günümüzde, siber savaş gerçektir ve siber saldırılar giderek artmaktadır. Nükleer tesislerin bilgisayar sistemlerini, elektrik şebekelerini ve hava kontrol sistemlerini kapatma kabiliyetleri siber saldırıları ulusal güvenlik için ciddi tehdit haline getirmektedir. Bazı bilim adamları siber saldırıların savaş nedeni olabileceği görüşünü ortaya atmaktadırlar. Ancak, geleneksel olarak düzenlenmiş savaş hukuku kurallarına bakıldığında, siber saldırıların çok az bir kısmı silahlı saldırı olarak kabul edilebilecek durumdadır.

Uluslararası hukuk sisteminin, bu yeni savaş alanına uyum sağlaması gerekirken, hali hazırda siber saldırılara karşı caydırıcı olacak, kalıcı ve etkin uluslararası hukuk kuralı yoktur. Bu makalede, kuvvet kullanma hakkı kapsamında, "kuvvet kullanma"ya ilişkin mevcut uluslararası hukuk kurallarının siber saldırılara nasıl uygulanabileceği incelenmektedir. Yapılan analizler, kuvvet kullanmayı yasaklayan Birleşmiş Milletler Antlaşması'nın 2(4). maddesi, VII. Bölüm güvenliğin sağlanması ve 51. maddede düzenlenen "meşru müdafaa hakkı" çerçevesinde yapılmıştır.

Anahtar Sözcükler: Siber savaş, siber saldırı, uluslararası hukuk, kuvvet kullanımı, meşru müdafaa, silahlı saldırı.

Abstract: In recent years, cyber war is real and cyber attacks have become increasingly common. Capable of shutting down nuclear systems, electrical grids and air traffic control systems, cyberattacks pose a serious threat to national security. Some scholars have suggested that cyber attacks should be treated as acts of war. Yet the attacks look little like the armed attacks that the law of war has traditionally regulated.

The international legal system should adapt to this battlegroound, altough there is currently no consistently effective internatio-

* Bu makale, TUBİTAK tarafından sağlanan destek kapsamında 2012-2013 döneminde ABD The City University of New York John Jay College'da yürütülen çalışmalar kapsamında hazırlanmıştır. Makalede yayımlanan görüş ve düşünceler tamamen yazarın kişisel fikirlerini yansıtmakta olup, çalışma gizlilik dereceli doküman kullanılmadan açık kaynaklardan yararlanılarak yapılmıştır.

** Dr., Askeri Yargıtay Başsavcı Yardımcısı (meh_yayla@yahoo.com).

nal law regime to deter these sorts of attacks. This article examines how existing international law about "use of force" may be applied to cyber attacks under the jus ad bellum. Analysis centers on the United Nations Charter's prohibition of the use of force in Article 2(4), its Chapter VII security scheme, and "right to self-defense" codified in Article 51.

Keywords: Cyber war, cyber attack, international law, use of force, self defence, armed attack.

I. GİRİŞ

İnternet ve bilgisayar modern ülkelerin hepsinde kritik öneme sahip olup ticaretin temel taşı olduğu gibi[1], stratejik devlet işleri, enerji üretimi ve dağıtımı, kritik altyapı tesislerinin yönetimi, toplu taşıma ve birçok kamu hizmeti internet ve bilgisayarlar aracılığıyla yerine getirilmektedir.[2] Bir ülke ne kadar gelişmiş ise o kadar teknolojiye, dolayısıyla internet ve bilgisayara bağımlı hale gelmiş durumdadır.[3] Network ağları ile birbirine bağlanmış olan bilgisayar sistemleri modern toplumun vazgeçilmezi olmuşlardır.[4]

Bilgisayar ve İnternet, iki tarafı keskin kılıç gibi devletlere büyük yararlar sağlarken, kritik bilgi sistemlerine saldıracak aktörlere de kapı açmaktadır.[5] Bu saldırılardan en çok etkilenecek ülkeler de teknolojisi en gelişmiş ve internet bağlantısını en çok kullananlardır.[6] Aslında, hiçbir ülke siber saldırılar karşısında güvende değildir denilebilir.

Yeni geliştirilen teknolojinin ilk kullanıldığı alanlardan biri olan, bilginin ve hızlı karar almanın önem taşıdığı askeri ortamda da bilgisayar ve iletişim teknolojileri kullanılmaktadır. Bu, her alanda olduğu

---

1 Andrew M. Colarik, *Cyber Terorism: Political and Economic Implications*, Idea Grup Publishing, 2006, s.vii-xi.

2 Colarik, s.vii-x.

3 Colarik, s.xii.

4 The White House, *The National Strategy to Secure Cyberspace,* 2003, s. vii, http://www.us-cert.gov/reading_room/cyberspace_strategy.pdf, erişim tarihi 12.1.2013.

5 Richard Garnett ve Paul Clarke, "Cyberterrorism: A New Challege for International Law", *Enforcing International Law Norms Against Terrorosim* (Editör: Bianchi, Andrea), 2004, s.465-487.

6 Clay Wilson, *Bootnets, Cybercrime, and Cyberterrorism:Vulnerabilities and Policy Issues for Congress*, 2007. s.CRS-7,CRS-8, http://www.fas.org/sgp/crs/terror/RL32114.pdf, erişim tarihi 13.1.2013.

gibi askeri alanda da bazı sorunları beraberinde getirmektedir. Her ne kadar askeri iletişim ağları, sivil kullanıma kapalı olma da bazı durumlarda sivil iletişim kaynaklarını kullanmak kaçınılmaz olmakta ve bu askeri sistemleri siber saldırılara açık hale getirmektedir.

Yaşanan olaylar göstermiştir ki siber saldırılar, ekonomik, fiziksel yıkımlara sebep olmasının yanında, yaralanmalara, ölümlere ve büyük yıkımlara sebep olabilecek kabiliyetlere ulaşmıştır. Bir yandan teknolojinin ulaştığı imkânlar göz önüne alınarak siber saldırı senaryoları üretilip, devletler bu saldırılara karşı strateji geliştirme arayışına girmekte iken diğer yandan da hukuk dünyasında ortaya çıkması muhtemel sorunlar tartışılmaktadır.

Devletlerin ya da uluslararası toplulukların siber ortamda karşı karşıya kaldığı en önemli sorunlardan biri, uluslararası hukuk kurallarının siber saldırılara uygulanıp uygulanamayacağıdır. Gerek geleneksel gerek antlaşma temelli uluslararası hukuk normları geliştirildiğinde siber teknoloji bu denli tehdit oluşturacak boyutta olmadığından mevcut hukuk kurallarının siber saldırılar için uygulanabilirliği tartışmalıdır.

Bazı yazarlar; siber savaşa gerektiğinden fazla önem verildiğini, gerçekleşecek bir siber saldırının, savaş nedeni olamayacağını, devlet kaynaklı politik bir siber saldırının, savaş kadar eski olan sabotaj, casusluk ya da tahrip amaçlı bir saldırı ile aynı sonucu doğuracağını ve konvansiyonel anlamda silahlı kuvvet kullanılmayacağını savunmaktadırlar.[7] Buna karşın, bugüne kadar yaşanan Estonya, Gürcistan ve İran'a karşı yapılan saldırılar siber savaşın ciddiyetini ortaya koymakta, uluslararası hukuk ve savaş hukuku açısından konu değerlendirilmekte, düşman devlet veya devlet güdümlü alt gruplar tarafından gerçekleştirilecek bir siber saldırı durumunda, saldırıya uğrayan devlet tarafından Birleşmiş Milletler (BM)[8] Antlaşması'nın 51. maddesindeki "meşru müdafaa hakkı"nın kullanılabileceği savunulmaktadır.

---

7 Thomas Rid, "Cyber War will not Take Place in", *Strategic Studies*, V.35, I.1, 2012, s.5-32; Ryan Singel, "White House Cyber Czar: There is no Cyber War", *Wired* (3.4.2010), http://www.wired.com/threatlevel/2010/03/schmidt-cyberwar/ erişim tarihi 10.11.2012; Ronald Deibert, . "Tracking the Emerging Arms Race in Cyberspace", *Bulletin of the Atomic Scientists,* Ocak/Şubat 2011, s.1-8.

8 Çalışmanın devamında Birleşmiş Milletler'den BM kısaltması kullanılarak bahsedilecektir.

Hukuk dünyasındaki ilerlemeler, bilimde olduğu gibi hayal etme ile birlikte gerçekleşmektedir. Bilim, evrendeki yeni buluşları tanımlamakta zorlandığında, onlarla ilgili yeni teoriler geliştirmektedir. Bu hukuk dünyasında da aynıdır. Hukukçular, günümüz teknolojisinin ve siber ortamdaki saldırıların silahlı çatışmalara ve savaş hukukuna etkisini hayal etmeli ve bu konu üzerine çalışmalıdır. Aksi takdirde hukuk, devletlere yön verme konusunda basit ve anlamsız kalacaktır.

Bu kapsamda çalışmada, kuvvet kullanma hakkı kapsamında "kuvvet kullanma"ya ilişkin mevcut uluslararası hukuk kurallarının siber saldırılara nasıl uygulanabileceği sorusuna cevap bulmak için önce BM Antlaşması'nın 2(4). maddesinden bahsedilecek, ardından kuvvet kullanma hakkının istisnalarından BM Güvenlik Konseyi kararıyla kuvvet kullanılması ve meşru müdafaa hakkının şartları ile uluslararası teamül hukukunun gereklilik ve orantılılık kuralları incelenecektir.

II. ULUSLARARASI HUKUKTA SİBER SALDIRILARA KARŞI KUVVET KULLANMA HAKKI

A. GENEL OLARAK

Uluslararası hukukta, kuvvet kullanma hakkı (jus ad bellum) ile kuvvete başvurulduğunda uyulması gereken çatışma kuralları (jus in bello) arasında bir ayrım yapılmaktadır. Buna göre, silahlı çatışma hukuku kurallarının uygulanmasının, bu hakka sahip olunup olunmadığı sorunundan tamamen bağımsız olduğu kabul edilmektedir.[9] Savaş hukuku incelenirken de, kuvvet kullanılmasının hukuka uygun olup olmadığı hususu ile silahlı kuvvet kullanılması sırasında seçilen hedef, araç ve yöntemlerin hukuka uygunluğu hususunun birbirinden ayrı düşünülmesi ve incelenmesi gerekmektedir. Siber saldırı durumunda devletlerin buna karşılık verme hakkı, kuvvete başvurma hakkına ilişkin (jus ad bellum) kuralların incelenmesini gerekli kılmaktadır.

Gelişen teknolojinin ve siber silahların imkân ve kabiliyetleri, BM Antlaşması'nın 51. maddesinde de yer alan "silahlı saldırı" kavramının değil aynı zamanda "silahlı kuvvet kullanma" kavramının da evrimleşmekte olduğunu göstermektedir. Gerçekten, BM Antlaşması'nı

9 Sadi Çaycı, *Silahlı Kuvvetlerin Kullanılması*, Genelkurmay Basımevi, Ankara,1995, s.38.

hazırlayanların, silahlı kuvvet kullanma konusunda akıllarında olan husus, hiç şüphesiz konvansiyonel nitelikte silahlarla askeri kuvvet kullanılmasıdır. Ancak, bilgi çağında artık konvansiyonel askeri kuvvet kullanma kavramı pek fazla anlam ifade etmemeye başlamıştır. Nitekim konvansiyonel silahlarla gerçekleştirilmeyen Estonya ve Gürcistan saldırılarının geride bıraktığı zarar dikkate değerdir.

Uluslararası toplumun ve devletlerin siber saldırılara karşı meşru müdafaa hakkının uygulanabilirliğini tartışması ve ABD gibi bazı devletlerin şartları gerçekleştiği takdirde siber saldırılara karşı geleneksel uluslararası hukuktan kaynaklanan meşru müdafaa hakkını kullanacağını açıklaması tartışmaları da beraberinde getirmektedir. Bir silahlı saldırının, konvansiyonel askeri kuvvet kullanılmasıyla gerçekleştirilmek zorunda olmadığının kabul edilmesi, potansiyel riskler ortaya çıkarmaktadır. Siber saldırıların, silahlı saldırı olarak kabul edilmesinin BM Antlaşması'nın 51. maddesinin uygulama alanını genişleterek uluslararası ortamı yeni karışıklıklara sürükleyeceği düşünülmektedir.

B. KUVVET KULLANMA YASAĞINA İLİŞKİN GENEL PRENSİPLER VE SİBER SALDIRILARIN HUKUKİ DURUMU

Günümüzde uluslararası hukukta kuvvet kullanmayı düzenleyen en temel kural BM Antlaşması'dır.[10] BM Antlaşması, uluslararası görüşmeler çerçevesinde BM konferanslarıyla hazırlanmıştır. Diğer uluslararası sözleşmelerde olduğu gibi BM Antlaşması, imza koyan bütün taraf devletleri bağlayıcı niteliğe haizdir. Antlaşma, uluslararası ilişkilerde kuvvet kullanılmasını ve kuvvet kullanma tehdidinde bulunulmasını açıkça yasaklamaktadır. Bu hüküm, Antlaşma'nın 2(4). maddesinde: "Teşkilatın üyeleri, milletlerarası münasebetlerinde gerek bir başka devletin toprak bütünlüğüne veya siyasi bağımsızlığına karşı, gerekse Birleşmiş Milletlerin amaçları ile telif edilemeyecek herhangi bir surette, tehdide veya kuvvet kullan*ılmasına başvurmaktan kaçınırlar*" şeklinde ifade edilmektedir. Bu, geleneksel uluslararası hukuk kuralı olan, başka devletlerin iç işlerine karışılmasının yasaklandığı "müdahale yasağı" (non-intervention) kuralı ile tamamlanmaktadır.[11]

---

10 Sertaç H. Başeren, *Uluslararası Hukukta Devletlerin Münferiden Kuvvet Kullanması*nın Sırları, Ankara Üniversitesi Basımevi, Ankara, 2003, s.46.

11 *Manila Declaration on the Peaceful Settlement of International Disputes*, G.A. Res.

BM Antlaşması'nın 2(4). maddesinde öngörülen kuvvet kullanma yasağı, sadece BM üyesi devletleri bağlamakta, üye olmayan devletlere doğrudan doğruya yükümlülük getirmemektedir. BM üyesi olmayan devletlerin BM Antlaşması'nda öngörülen kuvvet kullanma yasağına uymalarını sağlayacak şey, 2(4). maddede yer alan kuvvet kullanma yasağının evrensel bir uluslararası örf ve adet hukuk kuralı haline gelmiş olmasıdır.[12] Böylece, söz konusu yasak BM üyesi olsun ya da olmasın bütün devletleri bağlamaktadır.[13]

Ülke sınırlarını genişletme ve başka devlet hükümetlerini değiştirme amaçlarına hizmet etmemesi için BM sisteminde meşru olmayan kuvvet kullanımı, "saldırganlık" veya "yayılmacılık" olarak tanımlanmış ve yasaklanmıştır. Kuvvet kullanmaya, ancak meşru müdafaa veya Güvenlik Konseyi kararıyla ve siyasal bağımsızlık veya toprak bütünlüğünün korunması amacıyla izin verilmiştir.[14]

BM Antlaşması'nın kuvvet kullanımına ilişkin oluşturduğu sistemin iki ana özelliği vardır. Öncelikle, bütün üye devletler Antlaşma'nın

---

37/10, Annex, U.N. Doc. A/RES/37/10 (15.11.1982), http://www.un.org/documents/ga/ res/37/a37r010.htm, erişim tarihi 13.1.2013; *Declaration on Principles of International Law Concerning Friendly Relations and Co-operation Among States in Accordance with the Charter of the United Nation*, G.A. Res. 25/2625, U.N. Doc. A/RES/25/2625 (24.10.1970), http://www.unhcr.org/refworld/topic,459d17822,459d17a82,3dda1f104,0.html, erişim tarihi 13.1.2013.

12 Bu çerçevede örfi hukuk, sadece taraf devletler için haklar ve yükümlülükler tesis eden antlaşma esaslı hukuktan ayrılmaktadır. Uluslararası örf ve adet hukuku, hukuk olarak kabul edilen genel bir uygulamanın varlığı halinde söz konusu olmaktadır. Devletlerin bir uygulamasının örf ve adet hukuku kuralı haline gelmesi için bu uygulamayı -*opinio juris sive necessitatis*- hukuk kuralı olduğuna inanarak yapmış olmaları gerekmektedir. Günümüzde, BM Antlaşması'nın 2(4). maddesinde yer alan kuvvet kullanma yasağı, uluslararası örf ve adet hukukunun bütünleyici bir parçası haline gelmiştir. Hüseyin Pazarcı, *Uluslararası Hukuk Dersleri I. Kitap,* Turhan Kitabevi, Ankara, 1994, s. 209-218; Edip Çelik, *Milletlerarası Hukuk, Birinci Kitap,* Filiz Kitabevi, İstanbul, 1987, s. 55,157-164.

13 Yoram Dinstein, *War, Aggression And Self-Defence,* Grotius Publications Limited, Cambridge, s.91.

14 BM Antlaşması'nın düzenlediği kuvvet kullanma yasağı konusunun arkasındaki düşünceyi anlamak için hem II. Dünya Savaşını, hem de öncesinde oluşturulan girişimler ile tarihi belgelerin içeriğinin anlaşılması önemlidir. 1945 yılı, siyasi güç ve toprak kazanma amacı güden devletlerin neden olduğu ve yıkıcı sonuçların yaşandığı bir savaşın sonrasıdır. Bu acı tecrübeyi yaşayan devletler, Briand-Kellogg Paktı'nın eksikliklerini tamamlamak düşüncesiyle de San Fransisko Konferansı'nda kuvvete dayalı politikaların önlenmesi konusunda mutabık kalmışlardır. Anthony C. Arend ve Robert J. Beck, *International Law and Use of Force*, New York, Routledge, 1995, s.33,34.

2(4). maddesi gereğince uluslararası ilişkilerinde kuvvet kullanmaktan ya da kuvvet kullanma tehdidinden kaçınacaklardır. Bu koşullarda kuvvet kullanmak, hukuka aykırı bir fiil haline gelmektedir. İkinci olarak, bu yasağı ihlal eden devletlere karşı, münhasıran kuvvet kullanma yetkisiyle donatılmış merkezi bir otorite yaratılmıştır. Bu husus, Antlaşmanın VII. bölümünde, Güvenlik Konseyi'ne hukuka aykırı kuvvet kullanmaya karşı kuvvet kullanma yetkisi veren Antlaşma'nın 42. maddesinde ve takip eden maddelerde düzenlenmiştir.[15] Böylece, bir yandan devletler kuvvet kullanma yetkisini terk etmişler ve bireysel kuvvet kullanma hukuka aykırı bir fiil haline gelmiş, diğer yandan hukuka aykırı bir fiile karşı kuvvet kullanacak kolektif bir yetki oluşturularak BM'ye verilmiştir.

"Kuvvet kullanma" ve "tehdit" kriterlerini BM Antlaşması belirlemiş değildir. Antlaşma'da "savaş" terimi kullanılmaktan kaçınılmış, "savaş" terimi yerine kullanılan "tehdit" ya da "kuvvet kullanma" kavramlarının tanımı ise yapılmamıştır. Bu durum kuvvet kullanma yasağının yalnızca silahlı kuvvet kullanılmasıyla sınırlı kalıp kalmadığı yani, kimi zorlayıcı ekonomik ve diplomatik tedbirlerin de bu yasağın kapsamına girip girmediği konusunda tartışmaları gündeme getirmiştir. Zayıf devletler ve bazı bilim adamları BM Antlaşması'nın 2(4). maddesinin politik ve ekonomik zorlamaları da kapsaması gerektiği yönünde yorum yapmaktadırlar. Ancak yaygın kabul edilen görüşe göre, gerek BM Antlaşması'nın "Giriş" kısmında gerekse 41. ve 46. maddelerde "silahlı kuvvet" kavramının kullanılmış olması ve yine 1970 tarihli Dostça İlişkiler Bildirisi'nde sadece silahlı kuvvet kullanılması üzerinde durulması, bu tür siyasi ve ekonomik baskıların 2(4). madde kapsamında olmadığını teyit etmektedir.[16]

Günümüzde teknolojisi ilerlememiş, bilgisayar ve internet olanaklarını daha çok kullanan güçlü devletlerin siber saldırılara daha açık

---

15 Başeren, s.48.

16 Daniel B. Silver, "Computer Network Attack as a Use of Force Under Article 2(4) of the United Nations Charter", *Computer Network Attack and International Law*, 1999, s.80-82; Andrew B. Foltz, "Stuxnet, Schmitt Analysis, and the Cyber "Use of Force" Debate", *Joint Force Quarterly*, I.67, 4th Quarter, 2012, s.41 vd, http://www.au.af.mil/au/awc/awcgate/jfq/foltz_stuxnet_ schmitt_oct2012.pdf, erişim tarihi 18.1.2013; Matthew C. Waxman, "Cyber Attacks as "Force" Under UN Charter Article 2(4)", *International Law and the Changing Character of War*, V.87, 2011, s.44 vd; Dinstein, s.84.

hale gelmesi, bu durumun saldırıda bulunacak zayıf devletlere avantaj sağlaması nedeniyle kuvvet kullanımına ilişkin tartışmalar tersine dönmüş durumdadır. Özellikle ABD gibi güçlü devletler Antlaşma'nın 2(4). maddesinin daha geniş yorumlanmasını ve siber saldırıları da kapsayacak şekilde anlaşılması yönünde görüş bildirmektedirler.[17] Ancak 2(4). madde, halen klasik anlamda silahlı kuvvet kullanmayı yasaklamaktadır.[18]

Son on yıl içersinde özellikle Estonya, Gürcistan ve Stuxnet vakalarındaki siber saldırılar, geleneksel uluslararası hukuk normu olan "müdahale yasağı" kuralını da ihlal etmektedir. Ancak, devletler ya bu saldırıları devlet dışı aktörlere yaptırarak kendilerini gizlemekte

17 Amerika Savunma Bakanı Leon Panetta'nın 11 Ekim 2012 tarihinde New York'ta işadamları ile yaptığı toplantıda, Amerika'nın "Siber-Pearl Harbor" ihtimali ile karşı karşıya olduğunu, düşman devletlerin ya da radikal grupların siber silahları, Amerika'nın kritik altyapılarının kontrolünü ele geçirmek için kullanabileceğini, bunların enerji kaynaklarını ele geçirebileceklerini, su kanallarını kirletebileceklerini, bir treni kimyasal madde ile doldurup saldırı amaçlı yönlendirebileceklerini belirtmiş, ayrıca en kötü ihtimalin kritik altyapı sistemlerine karşı yapılacak koordineli bir saldırı olduğunu, bu saldırıda insanların hayatlarını kaybedebilecekleri gibi, halkı şok edecek fiziksel zararlar meydana gelebileceğini belirtmiştir. Bakan Panetta konuşmasında, böyle ciddi sonuçlar doğuracak bir saldırı tehdidi aldıklarında ulusun güvenliği için bu saldırılara karşılık verebileceklerini vurgulamıştır. Hemen belirtmek gerekir ki, Savunma Bakanı'nın vurguladığı husus, saldırı olduğunda değil, saldırı tehdidi doğduğunda ABD Hükümeti'nin bu saldırıyı silahlı saldırı gibi değerlendirip buna karşılık verme hakkını kendinde görmesi ve bu saldırının siber ortamda yapılacak bir karşı saldırıyı kapsadığı gibi, klasik anlamda silahlı saldırıyı da kapsamasıdır. Elisabeth Bumiller ve Thom Shanker, "Panetta Warns of Dire Threat of Cyberattack on U.S.", *The New York Times* (11 Ekim 2012), http://www.nytimes.com/2012/10/12/world/panetta-warns-of-dire-threat-of-cyberattack.html?pagewan ted=all&_r=0, erişim tarihi 3.11.2012.

18 Uluslararası hukukta geleneksel anlamda "kuvvet kullanma" terimiyle, savaş dâhil her türlü silahlı zorlama yolları anlaşılmaktadır. Bu açıdan bir devletin doğrudan doğruya düzenli askeri birlikleri aracılığıyla veya bir devletin desteklediği ve yardım ettiği silahlı gruplar veya gönüllü birlikler gibi düzen dışı kuvvetlerle kuvvet kullanılması veya kuvvet kullanma tehdidinde bulunulması BM Antlaşması'nın 2(4). maddesindeki yasak kapsamında değerlendirilmektedir. Nitekim düzensiz kuvvetler aracılığıyla gerçekleştirilen bu faaliyetlerin yasak kapsamında olduğu, gerek BM Genel Kurulu'nun 2625 sayılı Dostça İlişkiler Bildirisi gerekse Uluslararası Adalet Divanı'nın 27.06.1986 tarihli Nikaragua'da Askeri ve Yarı-Askeri Faaliyetler Davasındaki kararı ile açık bir şekilde ifade edilmiştir. Ayhan Döner, "Kuvvet Kullanma Yasağı ve İnsani Müdahale Açısından II. Körfez Savaşı", *e-akademi-Hukuk, Ekonomi ve Siyasal Bilimler Aylık İnternet Dergisi*, Sayı 17. Temmuz 2003, http://e-akademi.org/incele.asp?konu='Kuvvet%20Kullanma%20Yasa%F0%FD%20ve%20%DDnsani%20M%FCdahale%20A%E7%FDs%FDndan%20II.%20K%F6rfez%20Krizi'&kimlik=-397695427&url=makaleler /adoner-1.htm, erişim tarihi 13.1.2013.

ya da teknolojik imkânlar sayesinde saldırıların kimden kaynaklandığı belirlenememektedir.[19] Aslında siber saldırıda bulunan devletler, bu hareketlerinin silahlı güç kullanma kapsamında kabul edilebileceği geleneksel uluslararası hukuk kurallarını ihlal etme endişesi ile kendilerini gizlemekte veya devlet dışı aktörlere bu saldırıları düzenlettirmektedirler.

NATO, siber tehdit konusunda en önemli hazırlıkları yapan uluslararası örgüt durumundadır. NATO Antaşması'nın 4. maddesinde, bölgesel barış, bir üye ülke ulusal güvenliği, sınır bütünlüğü ya da bağımsızlığı tehlike altına girmesi halinde üye ülkeleri istişare için bir araya geleceği kabul edilmiş ve siber saldırı durumunda bu maddede sayılan durumlarda harekete geçeceğini belirtmiştir.[20] Bu, aslında NATO'nun siber saldırıları geleneksel uluslararası hukuk kuralı olan "müdahale yasağı" kuralına aykırı bulduğunun göstergesi kabul edilmektedir. Ekim 2011'de Bakanlar tarafından belirlenen Siber Savunma Eylem Planı'na göre Siber Savunma Politikası'nda siber tehditler, yeni Stratejik Kavram doğrultusunda 5. maddede ifade edilen toplu savunma görevini yerine getirmesi için potansiyel kaynak olarak tanımlanmıştır. 2012 Chicago Zirvesi Sonuç Bildirisi'nde de sürekli gelişen ve karmaşıklaşan siber tehditlerle etkin biçimde ve işbirliği içinde mücadele edilmesi gerektiği vurgulanmıştır.

NATO, siber güvenlik konusunda önemli mesafe almış olmakla birlikte, konuyla ilgili temel sorun ortak savunma koşulunu kapsayan 5. maddenin siber saldırıları kapsayıp kapsamayacağıdır. Yani üye ülkelerden birinin silahlı saldırı yerine siber saldırıya uğraması halinde, anlaşmanın bu maddesinin geçerli olup olmayacağı, saldıran ülkenin en kısa sürede nasıl ortaya çıkarılacağı ve bu ülkeye nasıl karşılık verileceği halen belirsizliğini korumaktadır.[21]

---

19 Matthew J. Sklerov, "Solving the Dilemma of State Responses to Cyberattacks: A Justification for the Use of Active Defenses Against States Who Neglect their Duty to Prevent", *Military Law Review*, V.201, 2009, s.74,75. http://www.loc.gov/rr/frd/Military_Law/Military_Law_ Review/pdf-files/201-fall-2009.pdf, erişim tarihi 15.1.2013.

20 *EurActiv* (4.4.2008). NATO Agrees on Common Approach to Cyber Defence, http://www.euractiv.com/en/infosociety/nato-agrees-common-approachcyber-defence/article-171377 erişim tarihi 1.11.2010.

21 Washington'da 4 Nisan 1949 tarihinde imzalan NATO Anlaşması'nın 5. maddesi; "Taraflar, Avrupa veya Kuzey Amerika'daki üyelerinden biri ya da daha fazlasına karşı silahlı bir saldırıyı, anlaşma taraflarının tümüne yapılmış sayacakları

III. KUVVET KULLANMA YASAĞININ İSTİSNALARI

Günümüzde BM Antlaşması'na göre kuvvet kullanma yasağının iki istinası bulunmaktadır; BM Güvenlik Konseyi kararıyla kuvvet kullanılması ve meşru müdafaa hakkı.

A. BM GÜVENLİK KONSEYİ KARARIYLA KUVVET KULLANILMASI

BM Antlaşması, uluslararası barış ve güvenliğin başlıca sorumluluğunu 24. maddeyle Güvenlik Konseyi'ne vermiştir. Antlaşma'nın "Barışın Tehdidi, Bozulması ve Saldırı Fiili Halinde Yapılacak Hareket" başlığını taşıyan VII. Bölümündeki 39-51. maddelerinde ise, uluslararası barış ve güvenliğin korunması amacıyla, Örgüt'ün alabileceği önlemler ve bunların nasıl uygulanacağı düzenlenmiş bulunmaktadır.

BM Antlaşması'nın 39. maddesine göre Güvenlik Konseyi, barışın tehdidi veya bozulması durumlarında, bunu tespit ve gerekli tavsiyelerde bulunma ya da 41 ve 42. maddeler gereği alınacak tedbirleri kararlaştırma yetkisine sahiptir. Hangi durumlarda barışın tehdit edildiği veya bozulduğunun tespiti oldukça zordur. BM Antlaşması'nda bu konulara ilişkin açık bir düzenleme bulunmamaktadır. Konuya siber savaş veya siber saldırı kapsamında bakıldığında durum daha da zorlaşmaktadır. Siber ortamda siber silahlarla gerçekleşecek saldırıların barışı tehdidi veya bozulması olarak nitelendirilebileceği ve buna paralel olarak kollektif güvenlik tedbirlerinin alınabileceği sorunu kolay halledilebilecek bir sorun değildir.

Güvenlik Konseyi, 39. maddeyi ilgilendiren bir durum tespit ettiğinde alabileceği önlemleri geçici ve zorlayıcı önlemler olmak üzere iki gruba ayırmaktadır. BM Antlaşması'nın 40. maddesine göre geçici tedbirlerin amacı, durumun daha fazla vahimleşmesini önlemektir. Bu önlemlerin neler olduğu Antlaşma'da düzenlenmemiş olmakla birlik-

---

konusunda mutabık kalmışlar ve sonuç olarak ta böyle bir silahlı saldırı gerçekleştiği takdirde, taraf devletlerin her biri, BM Şartının 51. maddesinde belirtilen toplu veya bireysel savunma hakkının kullanılmasında saldırının muhatabı olan taraf ya da taraflara derhal karşı saldırı konumuna geçerek yardım edecek, ve diğer taraflarla iş birliği içersinde silahlı güç kullanımı, Kuzey Atlantik Bölgesinin güvenliğinin devamının sağlanması da dâhil olmak üzere gerekli görülen eylemleri düzenleyeceklerdir." şeklindedir.http://translate.google.com/translate?hl=tr&langpair=en%7Ctr&u=http://www.nato.int/docu/basics.htm&ei=I86dULifEtK80AHPoHYAw, erişim tarihi 11.11.2012.

te Güvenlik Konseyi'nin, çatışmaların durdurulması, ateşkes, silahlı kuvvetlerin geri çekilmesi, antlaşmaya varılması ve askeri malzemeye ambargo konulması gibi geçici önlemler aldığı görülmektedir.[22] Antlaşma, 41 ve 42. maddeleriyle silahlı kuvvetler kullanılmasını gerektiren ve gerektirmeyen müeyyideler olmak üzere iki çeşit zorlayıcı önlem öngörmektedir. 41. madde diplomatik, ekonomik, siyasi ilişkilerin ve hava, deniz, demiryolu ulaşımının, posta, radyo, televizyon iletişiminin kesilmesi gibi silahlı kuvvet kullanımını gerektirmeyen önlemleri kapsamaktadır. 42. madde ise, gerektiğinde hava, deniz ve kara kuvvetleri aracılığıyla kuvvet kullanılmasını öngören zorlayıcı önlemleri kapsamaktadır.[23]

Sonuç olarak bir siber savaş veya siber saldırı durumunda Güvenlik Konseyi'nin kuvvet kullanma kararı alması politik olarak zor ve ağır yürüyen bir süreç olmasına karşın, konu değerlendirilip bir sonuca varıldığında devletlerin de bu karara uyması ve bu kapsamda yapılacak siber saldırılara karşı harekat hukuka uygun olacaktır.

B. MEŞRU MÜDAFAA HAKKI

Kuvvet kullanma yasağının diğer istisnası ise "meşru müdafaa"dır.[24] Devletlerin kendi güvenliklerini koruma hakları, her zaman uluslararası hukukun en temel ilkelerinden birisidir[25] ve "meş-

---

22 Seha L. Meray, *Devletler Hukukuna Giriş (İkinci Cilt)*, Yeniden Gözden Geçirilmiş Dördüncü Bası, Ankara, 1975, s.444.

23 Meray, s.444.

24 Kolektif meşru müdafaa hakkı, BM Antlaşması'nın 51. maddesinin meşru müdafaa hakkını geliştirdiği yönlerden birisidir. Kolektif meşru müdafaa hakkının kullanılmasında da bireysel meşru müdafaa hakkının kullanılmasında aranan, doğrudan ya da dolaylı bir silahlı saldırının gerçekleşmiş olması, alınan meşru müdafaa tedbirlerinin BM Güvenlik Konseyi'ne bildirilmesi, Güvenlik Konseyi harekete geçinceye kadar başvurulan geçici nitelikte istisnai bir hak olması ve örfi hukuktan kaynaklanan gereklilik, aciliyet ve orantılılık kriterlerine uygun olarak gerçekleştirilmesi koşullarının hepsi aranmaktadır. Bireysel meşru müdafaa hakkından farklı olarak kolektif meşru müdafaa hakkının kullanılması için, saldırıya uğrayan devletin bunu ilan edip açıkça yardım istemesi gerekmektedir. Stanimir A. Alexandrov, *Self Defence Against the Use of Force in International Law*, Kluwer Law International, La Haye, s.95; Funda Keskin, *Uluslararası Hukukta Kuvvet Kullanma: Savaş, Karışma ve Birleşmiş Milletler*, Mülkiyeliler Birliği Vakfı Yayınları Tezler Dizisi:4, Ankara, 1998, s.56-59; Saldırıya uğrayan devletin bunu ilan edip açıkça yardım istemesi dışında diğer konulara meşru müdafaa hakkı anlatılırken değinileceğinden ayrıca siber saldırılar bakımından kolektif meşru müdafaa hakkı incelenmeyecektir.

25 Richard J. Erickson, *Legitimate Use of Force Against State-Sponsored Terrorism,* Air

ru müdafaa hakkı" ile garanti altına alınmıştır.[26] Meşru müdafaa hakkına ilişkin 51. maddenin siber saldırılar için yapılan metinsel yorumuna ilişkin mevcut doktrinsel tartışmalar Estonya, Gürcistan ve Stuxnet olayları ile zirveye tırmanmıştır.

Aslında çoğu silahlı çatışmada, karşılıklı saldırıda bulunan her iki devletin de meşru müdafaa hakkına sığınarak yaptığı eylemin hukuki olduğunu savunması durumu, sorunu çıkmaza sürüklemektedir. Ancak bu soruna takılmadan önce, asıl önemli olan siber saldırıların, silahlı saldırı olarak kabul edilip edilemeyeceğidir. Çoğu görüş siber saldırının günümüz teknolojisinde silahlı saldırı eşiğine gelebileceği yönündedir.[27]

Bir devlete, meşru müdafaa hakkı kapsamında kuvvet kullanma hakkını veren siber saldırının parametreleri konusunda, 51. madde esasındaki yanıtın gereklilik, orantılılık ve aciliyet kriterlerini değerlendirmede devletlerin derin görüş ayrılıkları içinde olmaları ve bunun bir sonucu olarak, siber saldırılar konusunda ortak analitik çerçeve geliştirilememiş olmaları çözümü zorlaştırmaktadır. Bu güçlüğe rağmen, devlet destekli siber saldırılar ve devlet dışı aktörlerin gerçekleştirdikleri siber saldırıların; hangi koşullar altında BM Antlaşması'nın 51. maddesi çerçevesinde silahlı saldırı teşkil edebileceği meselesini incelemek büyük önem arz etmektedir.

"Silahlı saldırı" terimi diğerlerinin aksine BM Antlaşması'nda dar yorumlanmaktadır.[28] Örneğin Antlaşma'nın 2(4). maddesini ihlal eden bazı tehdit veya kuvvet kullanımları, 51. madde anlamında silahlı

University Press, Washington D.C., 1989, s.100.

26 BM Antlaşması'nın 51. maddesi çerçevesinde meşru müdafaa hakkı, orijinal olarak bölgesel düzenlemelerin meşruluğunu teyit etmek için 1945'de BM Antlaşması'na eklenmiştir. Bununla birlikte, San Francisco Konferansı sonrasında meşru müdafaa hakkı, bu amacın çok ötesinde gelişmiştir. Alexandrov, s.182.

27 ABD, ülkesine karşı siber ortamdan gelecek tehditlere karşı meşru müdafaa hakkını kendinde görmekte ve bu saldırılara cevap vereceğini açıklamaktadır. The White House. (Mayıs 2011). *International Strategy for Cyberspace*. s.14. http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf, erişim tarihi 14.1.2013

28 Yoram Dinstein, "Computer Network Attack and Self-Defense", *Computer Network Attack and International Law*, V.76. *Naval War College International Law Studies*, Rhode Island, William S. Hein & Co.,Inc., 2002, s.100, https://www.usnwc.edu/getattachment/95012329-e379-4341-bd1d-a4764c84dd4c/Vol--76----Computer-Network-Attack-and-Internation.aspx, erişim tarihi 13.1.2013.

saldırı teşkil etmemektedir. Bu durumda silahlı saldırı olarak değerlendirilemeyecek olan siber saldırılar, dolayısıyla 51. madde uyarınca meşru müdafaa hakkı doğurmayacaktır.

BM Antlaşması'nın 51. maddesinde, meşru müdafaa hakkının kullanılabilmesinin ön şartı olarak "saldırının" değil bir "silahlı saldırı"nın gerçekleştirilmiş olması kabul edilmiştir. Ancak, silahlı saldırı kavramının tanımına ne bu maddede ne de diğer madde hükümlerinde yer verilmemiştir. Saldırı ve silahlı saldırı kavramları, belli ölçüde birbiriyle örtüşen kavramlar olmalarına rağmen; tam olarak aynı şey değildirler. Daha da önemlisi bunların hukuksal anlamları farklı olup pratikte farklı sonuçlar doğurmaktadırlar.

Silahlı bir saldırının aynı zamanda bir saldırı olduğu söylenebilir fakat her saldırı bir silahlı saldırı değildir. Çünkü silahlı saldırı kavramı, saldırı kavramından daha dar bir anlam ifade etmektedir. Bir silahlı saldırı, saldırının bir alt kategorisi olduğu kabul edilmektedir. Ayrıca, bu iki kavram, doğurduğu sonuçlar itibariyle de birbirinden farklıdır. Silahlı saldırı, doğurduğu sonuçlar itibariyle, kabul edilmeyecek ölçülerde olduğu için; mağdur devlete; meşru müdafaa hakkına dayanarak münferiden kuvvet kullanma yetkisi verir. Bu husus silahlı saldırının ayırt edici nitelik ve fonksiyonunu ortaya koymaktadır. Saldırı kavramına giren diğer fiillerde ise bu nitelik yoktur; kolektif güvenlik sisteminin devreye girmesini sağlayan başka fonksiyona sahiptir.

Siber saldırılara karşı kuvvet kullanmanın ön şartı; 51. madde bağlamında "silahlı saldırı" olarak kabul edilmesidir. Dolayısıyla, askeri bir harekatın meşru olabilmesi için, saldırının silahlı saldırı boyutuna ulaşmış olması zorunludur. Silahlı saldırı kavramının BM Antlaşması'nda tanımlanmamış olması nedeniyle, bilimsel olarak siber saldırının ne zaman silahlı saldırı olarak kabul edilip, silahlı meşru müdafaa hakkı doğuracağı ile ilgili üç görüş bulunmaktadır: "araç bazlı yaklaşım", "hedef bazlı yaklaşım" ve "etki bazlı yaklaşım".[29]

[29] Oona A. Hathaway & Rebecca Crootof & Philip Levitz & Haley Nix& Aileen Nowlan & William Perdue & Julia Spiegel, "The Law of Cyber Attack", *California Law Review,* V.100, 1.8.2012, s.845.

1. Araç Bazlı Yaklaşım

"Araç bazlı yaklaşıma" göre siber saldırılar, BM Antlaşması'nın 51. maddesi kapsamındaki silahlı saldırı kapsamında değerlendirilemez. Çünkü siber saldırılar hiçbir zaman klasik anlamda askeri silahlardan değildirler. Siber saldırılar, yalnızca siber saldırı ile birlikte ya da siber saldırı aracılığıyla klasik anlamda askeri silah kullanıyorsa silahlı saldırı olarak kabul edilebilir. Siber saldırı sonucu yönlendirilen bir bombanın bilgisayar destek merkezini veya internet kablolarını vurması ve bu silahlı saldırının "yeterli ağırlık"[30] ölçüsüne ulaşması buna örnek olarak verilebilir.[31]

Aslında BM Antlaşmasının lafzının "araç bazlı yaklaşımı" desteklediği görülmektedir. Şöyle ki, 41. madde "Güvenlik Konseyi, kararlarını yürütmek için silahlı kuvvet kullanımını içermeyen ne gibi önlemler alınması gerektiğini kararlaştırabilir ve BM üyelerini bu önlemleri uygulamaya çağırabilir. Bu önlemler, ekonomik ilişkilerin ve demiryolu, deniz, hava, posta, telgraf, radyo ve diğer iletişim ve ulaştırma araçlarının tümüyle ya da bir bölümüyle kesintiye uğratılmasını, diplomatik ilişkilerin kesilmesini içerebilir."[32] Bu düzenlemede, "telgraf, radyo ve diğer iletişim ve ulaştırma" araçlarının siber ortamdaki araçları kastettiği yorumu ile siber saldırıların Antlaşma kapsamında silahlı saldırı olarak kabul edilemeyeceği söylenebilir.

---

30 Nikaragua davasında Divan, bir devletin başka bir devletin topraklarına silahlı çeteler göndermesi halinde, bu çetelerin silahlı saldırılarının düzenli orduların saldırıları ile aynı şiddet ve ölçekte olması şartıyla, BM Antlaşması'nın 51. maddesi çerçevesinde bir "silahlı saldırı" olabileceğini kabul ederek, "silahlı saldırının" tanımlanmasında bir "ölçü ve etki" testi ortaya koymuş; "yeterli ağırlık (sufficient gravity)" koşulu getirmiştir. Divan'ın Nikaragua davasındaki kararında silahlı saldırının ve buna uygun olarak da meşru müdafaa hakkının dar bir yorumunu desteklemiş ve silahlı saldırının tanımlanmasında yüksek bir eşik tesis etmiştir. Carsten Sthan, "Nicaragua is Dead-Long Live Nicaragua-the Rigt to Self Defence Under Article 51 of UN Charter and International Terrorism", *Terrorism as a Challenge for National and International Law: Securtiy versus Liberty*, Berlin&Heidelberg, 2003, http://edoc.mpil.de/conference-on-terrorism/index.cfm, erişim tarihi 10.10.2011

31 Michael N. Schmitt, *Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework*, Research Publication 1 Information Series, 1999, s.21.22, http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA471993, erişim tarihi 10.11.2012.

32 Birleşmiş Milletler Antlaşması'nın 41. maddesi. http://www.tbmm.gov.tr/komisyon /insanhaklari/pdf01/3-30.pdf, erişim tarihi 1.2.2013.

Bu sonuca, BM Genel Kurulu'nun 14 Aralık 1974 tarih ve 29/3314 sayılı "Saldırının Tanımı" kararında yola çıkılarak da varılabilir.[33] Saldırının Tanımı kararının 3. maddesinde saldırının yedi türü sayılmış ve bunlardan hepsi klasik anlamda silah veya askeri kuvvete ilişkindir.[492] Saldırının Tanımı kararında, "kuvvet kullanma tehdidi" tanıma dâhil edilmemiştir. Tanım'da, kuvvet kullanma tehdidinin ihmal edilmiş olması, saldırının sadece fiili silahlı kuvvet kullanıldığı zaman mevcut olacağı; siyasî, ekonomik, kültürel ya da ideolojik baskı türlerinin ya da klasik anlamda silahlı kuvvet kullanılmasını içermeyen müdahalelerin "saldırı" teşkil etmeyeceği anlamına gelmektedir.[34] Saldırının Tanımı kararının önsözünde, saldırının "silahlı kuvvet kullanmak" olarak tanımlanması ve en ciddi, tehlikeli illegal kuvvet kullanma şekli olduğuna vurgu yapılması da BM Antlaşması'na aykırı herhangi kuvvet kullanmanın saldırı sayılamayacağına, Antlaşma'nın "araç bazlı yaklaşımı" desteklediği ve siber saldırıların silahlı saldırı olarak kabul edilemeyeceği değerlendirilmektedir.

"Araç bazlı yaklaşımın" en önemli özelliği uygulamanın basitliğidir. Çünkü askeri kuvvet veya geleneksel anlamda silah tanımlaması yapmak kolaydır. Buna rağmen siber saldırıların konvansiyonel anlamda silahlar kadar zararlara yol açma imkânı bulunduğundan birçok bilim adamı "araç bazlı yaklaşım"ın artık kullanamayacağı görüşündedir.

2. Hedef Bazlı Yaklaşım

Siber saldırı kabiliyetleri ve verebileceği zararlar değerlendirilerek "hedef bazlı yaklaşım" ortaya atılmıştır. "Hedef bazlı yaklaşım"da silahlı saldırı, kritik öneme sahip bir bilgisayar sisteminin siber saldırıda hedef alınması olarak kabul edilmektedir. Bu yaklaşımda, önleyici meşru müdafaa için siber saldırının, önemli ve yeter derecede muhtemel bir zararın habercisi olması gerekmektedir.[35] Hedef bazlı yak-

---

33 G.A. Res. 3314, U.N. G.A.O.R., 29th Sess., Supp. No. 31, U.N. Doc. A/9631 (1974). Türkçe metin için bkz. Aslan Gündüz, *Milletlerarası Hukuk Temel Belgeler Örnek Kararlar* (3. Baskı). Beta Yayınları, İstanbul, 1998, s.118-120.

34 Fatma Taşdemir, *Uluslararası Terörizme Karşı Devletlerin Kuvvete Başvurma Yetkisi* (1. Baskı), Siyasal Basın Yayın Dağıtım, Ankara, 2006, s.143,144.

35 Duncan B. Hollis, "Why States Need an International Law for Information Operations", *Lewis & Clark Law Review,* V.11, 1997, s.1041.

laşımın en önemli faydası, devletlere ulusal kritik alt yapıları koruma avantajı sağlaması olmasına rağmen, kuvvet kullanarak meşru müdafaa hakkı eşiğini düşürdüğünden, uluslararası ortamı yıkıcı konvansiyonel silahlı çatışmalara sürükleme riski doğurmasıdır.[36] Çünkü bu yaklaşım benimsendiği takdirde kritik alt yapı sistemlerine yapılacak siber saldırılar, fiziksel ve kinetik anlamda meşru müdafaa kapsamında karşı saldırı yapmanın önünü açacaktır.

3. Etki Bazlı Yaklaşım

"Etki bazlı yaklaşım"a göre ise siber saldırı, yaptığı etkinin ağırlığı (gravity) ölçüsüne bağlı olarak silahlı saldırı olarak kabul edilecektir. Diğer yaklaşımlarla kıyaslandığında, şu anda "etki bazlı yaklaşım" uluslararası ortamda özellikle teknolojisi gelişmiş ve ABD gibi saldırılara en çok maruz kalan devletler arasında en kabul gören yaklaşım olarak kabul edilmektedir. Meşru müdafaa hakkını doğuracak siber saldırının etkisinin ağırlığının ölçülmesi konusunda ise değişik düşünceler ortaya atılmakta ve bu en önemli sorun olarak bilim adamlarının karşısında çıkmaktadır. Örneğin, bir havaalanı kontrol sistemine düzenlenecek siber saldırı, bölgesel elektrik kesintilerine sebebiyet verecek siber saldırı, borsa veya finansal sistemi işlemez hale getirecek bir saldırı ya da 2007 yılındaki Estonya saldırısı, bunlardan hangisinin savunma amaçlı kuvvet kullanmak için yeterli ağırlık derecesine ulaşmış olduğunu tespit etmek gerekmektedir. Bu saldırılar küçük ya da büyük ölçekte zararlara yol açmakta, hatta bazıları ölümlere veya ekonomik sistemin çökmesine neden olmasına rağmen saldırının sonuçlarının ortaya konması ya da anlaşılması kolay olmamaktadır.

Prof. Michael Schmitt, doktrinde bu konuda kabul görmüş "etki bazlı yaklaşım"la ilgili kriterleri en iyi belirleyen olarak kabul edilmektedir. Onun görüşüne göre siber saldırının etkileri şu altı kritere değerlendirilmelidir:[37]

1- Yıkıcılık (severity); zararın çeşidi ve boyutu,

2- Yakınlık (immediacy); saldırıdan sonra ne kadar süre içinde zararın ortaya çıktığı,

---

36 Sklerov, 56.
37 Schmitt (1999), s.18,19.

3- İlliyet bağı (directness); saldırı ile zarar arasındaki illiyet bağı,

4- İstilacılık (invasiveness); saldırının mağdur ülkenin bölgesine girme derecesi,

5- Ölçülebilirlik (measurability); saldırının meydana getirdiği zararın ölçülebilme derecesi,

6- Meşruluk beklentisi (Presumptive legitimacy); bir silahlı saldırı siber saldırı olarak değerlendirilmesinin bir kural değil istisna olması.

Yukarıdaki kriterler, karar vericiler için aydınlatıcı olsa da yeterli olmadığı değerlendirilmektedir. Diğer bir deyişle etki bazlı yaklaşıma yeni kriterler eklenebilmekte veya eleştirilmektedir.[38]

Yukarıdaki yaklaşımların hepsinde önemli olan siber saldırının politik veya ulusal güvenliği tehdit amaçlı yapılması gerekir ki siber saldırı veya siber savaş kavramından bahsedilebilsin, aksi halde siber saldırı bir asayiş olayı olmanın ötesine geçmeyecektir.

C. GEREKLİLİK VE ORANTILILIK KRİTERLERİ

Siber saldırıya karşı silahlı kuvvet kullanacak olan devletin yukarıda sayılan kuralların yanında kuvvet kullanmaya ilişkin geleneksel uluslararası hukuk kurallarından olan "gereklilik (necessity)" ve "orantılılık (proportionality)" kurallarına da uyması gerekmektedir. Günümüzde, bütün devletler, gereklilik ve orantılılık kriterlerinin, BM Antlaşması'nın 51. maddesi çerçevesinde, yasal meşru müdafaa hakkının parametrelerini oluşturduğu konusunda mutabıktır. Günümüzde bu koşullar, uluslararası örf ve adet hukukundan kaynaklanan bir sınırlama olarak meşru müdafaa hakkının kullanılmasında geçerliliklerini korumaktadırlar.[39] Bu kriterler BM Antlaşması'nın 51. maddesinde yer almamasına rağmen örfi hukukun parçası olarak devletleri bağlamaktadır. Siber saldırılara karşı devletlerin meşru müdafaa temelinde kuvvet kullanmalarında da bu ilkelere uyulması

---

38 Silver, s.89; Jason Barkham, "Information Warfare and International Law on the Use of Force", *New York University Journal of International Law & Policy,* V.34, 2001, s. 57,85,86.

39 Christine Gray, *International Law and Use of Force*. Oxford University Press, Oxford, 2000, s. 105

büyük önem taşımaktadır. Aksi takdirde siber saldırılara karşı meşru müdafaa temelindeki yanıtların hukuka aykırı zararla karşılığa dönüşme riski vardır. ABD, siber saldırılara karşı bu kriterlere başvuracağını açıklamıştır.[40]

Gerekliliğin değerlendirmesi, kuvvete başvurma konusunda kararın verildiği anda meydana gelecek ve karar verildiğinde ise gereklilik kriteri işlevini tamamlayacaktır.[41] Ancak, bir silahlı saldırı sayılacak siber saldırının meydana gelmesi meşru müdafaanın "gerekliliği" anlamına gelmemektedir. Dolayısıyla, silahlı bir saldırıya uğrayan mağdur devletin, kendisini silahla savunma dışında bir seçeneğinin olmadığını kanıtlaması gerekir.[42] Bu kapsamda, gereklilik hali, alternatif bir davranış seçeneğinin bulunmadığı "sıcak bir tehdit" durumunda söz konusu olmaktadır.[43] Olay anında verilen silahlı karşılığın, meşru müdafaa hakkı olarak uluslararası hukuka uygun sayılması için, alternatif bir davranış biçiminin, mağdur tarafın zararını telafi etme imkânının bulunmaması gerekmektedir. Şayet, saldırgan eylemle ilgili olarak taraflar arasında görüşmeler başlamışsa, olay mahallinde verilecek silahla karşılık meşru müdafaa olmaktan çıkmaktadır.[44]

Orantılılık ilkesi, savunma amaçlı tedbirlerin yol açtığı hasarın, başlangıçtaki silahlı saldırının yol açtığı maddi ve beşeri zarar ile orantılı olmasını ya da savunma tedbirlerine başvuran devletin saldırgan devletin kullandığı silahların aynısını ve aynı sayıda silahlı kuvveti kullanması gerektiği anlamına gelmemektedir.[45] Bu çerçevede söz konusu ilke, silahlı bir saldırıyı bertaraf etmek için kullanılabilecek karşı güce belli sınırlamalar getirdiği için silahlı çatışmaların tırmanmasını da önlemiş olmaktadır.[46]

Gereklilik ve orantılılık prensipleri açık olmakla birlikte sorun bu ilkelerin siber saldırılara karşı nasıl uygulanacağıdır. Bu prensiplerin

---

40 *International Strategy for Cyberspace*. (Mayıs 2011), s.14.
41 Judith Gail Gardam, "Necessity and Proportionality in Jus Ad Bellum and Jus In Bello", *International Law, The International Court of Justice and Nuclear Weapons,* Cambridge University, Cambridge, s.278.
42 Gardam, s.278.
43 Berdal Aral, *Uluslararası Hukukta Meşru Müdafaa Hakkı*, Siyasal Kitabevi, Ankara, 1999, s.26.
44 Dinstein, s.202.
45 Gardam, s.278,279.
46 Aral, s.29.

klasik silahlı saldırı durumunda bile nasıl uygulanacağı tartışılırken, siber saldırı gibi etkilerinin ya da zararlarının ölçülmesi ve hukuka uygun bir karşılık verilmesi durumu da uluslararası arenada hala çözüm bekleyen konulardan birisidir.

IV. SONUÇ

Devletler kendi sınırlarını, ulusal güvenliklerini ve barış ortamını korumak zorundadırlar. Günümüzde siber güvenlik, küçük büyük, gelişmiş ya da az gelişmiş her ülke için önemlidir ve ulusal güvenlikle eş değer tutulmaktadır. Siber alan, fiziki alan gibi sınırları olan üzerinde tek bir devletin egemenlik kurduğu bir alan değildir ve gelişen teknolojik imkânlar ve siber saldırıların sınır tanımaz yapısı, uluslararası barış ve güvenliği tehdit eden en büyük sorunlardan biri haline gelmiştir.

Günümüzde siber ortamı tamamen güvenli hale getirmek bir ütopya olarak görülmesine rağmen siber saldırıları engellemek için küresel anlamda işbirliğine ihtiyaç olduğu açıktır. Birleşmiş Milletler'e üye devletler aynı tanım, strateji veya çözüm konusunda halen uzlaşabilmiş değildirler. Devletlerin siber tehditlere karşı yaklaşımı ve stratejisi ile hukuki anlamda yorumu farklı olduğundan kolektif anlamda çözüm de zorlaşmaktadır.

Henüz siber saldırı ve siber savaş konusunda ortak bir dil oluşturamamış, hangi siber saldırının silahlı saldırı kapsamında değerlendirileceği, siber saldırılara karşı savaş hukuku kapsamında kuvvet kullanılıp kullanılamayacağı konularında ittifak edememiş uluslararası toplumun; yakın gelecekte daha karmaşık hale gelip sonuçları daha ciddi olacak siber saldırılar konusunda ortak bir çaba içine girmesi ve hukuki anlamda gerekli hazırlıkları yapmasının kaçınılmaz olduğu değerlendirilmektedir.

Bunun yanında hukukçuların, devlet güvenliğine, ulusal ve uluslararası barışa karşı tehdit oluşturan siber savaş ve siber saldırıların hukuk dünyasına etkileri, mevcut kuralların uygulanabilirliği ve ihtiyaç duyulan düzenlemeler konusunda çalışmalarının uygun olacağı düşünülmektedir.

KAYNAKLAR

Andrew M. Colarik, *Cyber Terorism: Political and Economic Implications*, Idea Grup Publishing, 2006.

Andrew B. Foltz, "Stuxnet, Schmitt Analysis, and the Cyber "Use of Force" Debate", *Joint Force Quarterly*, I.67, 4th Quarter, 2012, s.40-48, http://www.au.af.mil/au/awc/awcgate/jfq/foltz_stuxnet_ schmitt_oct2012.pdf, erişim tarihi 18.1.2013.

Anthony C. Arend ve Robert J. Beck, *International Law and Use of Force*, New York, Routledge, 1995.

Aslan Gündüz, *Milletlerarası Hukuk Temel Belgeler Örnek Kararlar* (3. Baskı). Beta Yayınları, İstanbul, 1998.

Ayhan Döner, "Kuvvet Kullanma Yasağı ve İnsani Müdahale Açısından II. Körfez Savaşı", *e-akademi-Hukuk, Ekonomi ve Siyasal Bilimler Aylık İnternet Dergisi*, Sayı 17, Temmuz 2003, http://e-akademi.org/incele.asp?konu='Kuvvet%20Kullanma%20Yasa%F0%FD%20ve%20%DDnsani%20M%FCdahale%20A%E7%FDs%FDndan%20II.%20K%F6rfez%20Krizi'&kimlik=-397695427&url=makaleler /adoner-1.htm, erişim tarihi 13.1.2013.

Berdal Aral, *Uluslararası Hukukta Meşru Müdafaa Hakkı*, Siyasal Kitabevi, Ankara, 1999.

Carsten Sthan, "Nicaragua is Dead-Long Live Nicaragua-the Rigt to Self Defence Under Article 51 of UN Charter and International Terrorism", *Terrorism as a Challenge for National and International Law: Securtiy versus Liberty*, Berlin&Heidelberg, 2003, http://edoc.mpil.de/conference-on-terrorism/index.cfm, erişim tarihi 10.10.2011

Christine Gray, *International Law and Use of Force*, Oxford University Press, Oxford, 2000.

Clay Wilson, *Bootnets, Cybercrime, and Cyberterrorism:Vulnerabilities and Policy Issues for Congress*, 2007, http://www.fas.org/sgp/crs/terror/RL32114.pdf, erişim tarihi 13.1.2013.

Daniel B. Silver, "Computer Network Attack as a Use of Force Under Article 2(4) of the United Nations Charter", *Computer Network Attack and International Law*, 1999, s.73-98.

Declaration on Principles of International Law Concerning Friendly Relations and Cooperation Among States in Accordance with the Charter of the United Nation, G.A. Res. 25/2625, U.N. Doc. A/RES/25/2625 (24.10.1970), http://www.unhcr.org/refworld/topic,459d17822,459d17a82,3dda 1f104,0.html, erişim tarihi 13.1.2013.

Duncan B. Hollis, "Why States Need an International Law for Information Operations", *Lewis & Clark Law Review,* V.11, 1997, s.1023-1061.

Elisabeth Bumiller ve Thom Shanker, "Panetta Warns of Dire Threat of Cyberattack on U.S.", *The New York Times* (11 Ekim 2012), http://www.nytimes.com/2012/10/12/world/panetta-warns-of-dire-threat-of-cyberattack.html?pagewan ted=all&_r=0, erişim tarihi 3.11.2012.

EurActiv (4.4.2008). NATO Agrees on Common Approach to Cyber Defence, http://www.euractiv.com/en/infosociety/nato-agrees-common-approachcyber-defence/article-171377, erişim tarihi 1.11.2010.

Fatma Taşdemir, *Uluslararası Terörizme Karşı Devletlerin Kuvvete Başvurma Yetkisi* (1. Baskı), Siyasal Basın Yayın Dağıtım, Ankara, 2006.

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

Hüseyin Pazarcı, *Uluslararası Hukuk Dersleri I. Kitap,* Turhan Kitabevi, Ankara, 1994, s. 209-218; Edip Çelik, *Milletlerarası Hukuk, Birinci Kitap,* Filiz Kitabevi, İstanbul, 1987.

Jason Barkham, "Information Warfare and International Law on the Use of Force", *New York University Journal of International Law & Policy,* V.34, 2001, s. 57-113.

Judith Gail Gardam, "Necessity and Proportionality in Jus Ad Bellum and Jus In Bello", *International Law, The International Court of Justice and Nuclear Weapons,* Cambridge University, Cambridge, s.275-292.

Michael N. Schmitt, *Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework*, Research Publication 1 Information Series, 1999, http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA471993, erişim tarihi 10.11.2012.

Manila Declaration on the Peaceful Settlement of International Disputes, G.A. Res. 37/10, Annex, U.N. Doc. A/RES/37/10 (15.11.1982), http://www.un.org/documents/ga/ res/37/a37r010.htm, erişim tarihi 13.1.2013.

Matthew C. Waxman, "Cyber Attacks as "Force" Under UN Charter Article 2(4)", *International Law and the Changing Character of War*, V.87, 2011, s.43-57.

Matthew J. Sklerov, "Solving the Dilemma of State Responses to Cyberattacks: A Justification for the Use of Active Defenses Against States Who Neglect their Duty to Prevent", *Military Law Review*, V.201, 2009, s.1-85, http://www.loc.gov/rr/frd/Military_Law/Military_Law_ Review/pdf-files/201-fall-2009.pdf, erişim tarihi 15.1.2013.

Oona A. Hathaway & Rebecca Crootof & Philip Levitz & Haley Nix& Aileen Nowlan & William Perdue & Julia Spiegel, "The Law of Cyber Attack", *California Law Review,* V.100, 1.8.2012, s.817-886.

Richard J. Erickson, *Legitimate Use of Force Against State-Sponsored Terrorism,* Air University Press, Washington D.C., 1989.

Richard Garnett ve Paul Clarke, "Cyberterrorism: A New Challege for International Law", *Enforcing International Law Norms Against Terrorosim* (Editör: Bianchi, Andrea), 2004, s.465-487.

Ronald Deibert, . "Tracking the Emerging Arms Race in Cyberspace", *Bulletin of the Atomic Scientists,* Ocak/Şubat 2011, s.1-8.

Ryan Singel, "White House Cyber Czar: There is no Cyber War", *Wired* (3.4.2010), http://www.wired.com/threatlevel/2010/03/schmidt-cyberwar/ erişim tarihi 10.11.2012;

Sadi Çaycı, *Silahlı Kuvvetlerin Kullanılması*, Genelkurmay Basımevi, Ankara,1995.

Seha L. Meray, *Devletler Hukukuna Giriş (İkinci Cilt)*, Yeniden Gözden Geçirilmiş Dördüncü Bası, Ankara, 1975.

Stanimir A. Alexandrov, *Self Defence Against the Use of Force in International Law*, Kluwer Law International, La Haye, 1996.

Sertaç H. Başeren, *Uluslararası Hukukta Devletlerin Münferiden Kuvvet Kullanması*nın Sırları, Ankara Üniversitesi Basımevi, Ankara, 2003.

The White House, *The National Strategy to Secure Cyberspace,* 2003, http://www.us-cert.gov/reading_room/cyberspace_strategy.pdf, erişim tarihi 12.1.2013.

The White House (Mayıs 2011), *International Strategy for Cyberspace,* http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf, erişim tarihi 14.1.2013.

Thomas Rid, "Cyber War will not Take Place in", *Strategic Studies*, V.35, I.1, 2012, s.5-32.

Yoram Dinstein, "Computer Network Attack and Self-Defense", *Computer Network Attack and International Law*, V.76. *Naval War College International Law Studies*, Rhode Island, William S. Hein & Co.,Inc., 2002, s.99.120, https://www.usnwc.edu/getattachment/95012329-e379-4341-bd1d-a4764c84dd4c/Vol--76----Computer-Network-Attack-and-Internation.aspx, erişim tarihi 13.1.2013.

Yoram Dinstein, *War, Aggression And Self-Defence,* Grotius Publications Limited, Cambridge, 2001.