International
SOCIAL SCIENCES STUDIES JOURNAL
SSSjournal (ISSN:2587-1587)

Economics and Administration, Tourism and Tourism Management, History, Culture, Religion, Psychology, Sociology, Fine Arts, Engineering, Architecture, Language, Literature, Educational Sciences, Pedagogy & Other Disciplines in Social Sciences

Vol:5, Issue:36	pp.2827-2833	2019
sssjournal.com	ISSN:2587-1587	sssjournal.info@gmail.com

Article Arrival Date (Makale Geliş Tarihi) 02/04/2019 | The Published Rel. Date (Makale Yayın Kabul Tarihi) 10/06/2019
Published Date (Makale Yayın Tarihi) 10.06.2019

SİBER UZAYDA ULUSLARARASI HUKUK MÜMKÜN MÜ?

IS INTERNATIONAL LAW POSSIBLE IN CYBER SPACE?

Şerife KARADAĞ
Selçuk Üniversitesi, Sosyal Bilimler Enstitüsü, Uluslararası İlişkiler Bölümü, Konya/ TÜRKİYE
ORCID: https://orcid.org/0000-0003-3471-8435

Article Type : Research Article/ Araştırma Makalesi
Doi Number : http://dx.doi.org/10.26449/sssj.1522
Reference : Karadağ., Ş. (2019). "Siber Uzayda Uluslararası Hukuk Mümkün Mü?", International Social Sciences Studies Journal, 5(36):2827-2833.

ÖZ

Siber uzay, çağımızın aktörlerinin en aktif rol aldığı alanlardan birisi olmuştur. Bu alanda insanlığa dair faydaların yanı sıra bir o kadar da zarar verici olaylar ve durumlar olduğu da görülmektedir. Çeşitli siber saldırılar, siber tehditler, casusluk olayları ve siber üzerinden yapılan savaşlar birçok hasara neden olan siber tehlikelerdir. Bu nedenle siber uzay artık aktörler için güvenliklerinin sarsılacağı ve tehlikeye gireceği bir alan konumundadır. Aktörler arasında özellikle büyük önem taşıyan devletler, siber güvenliklerini sağlamak uğruna birçok faaliyet ve savunma yollarına başvurmuştur. Ulusal düzeyde siber savunma ve güvenlik için hukuki yollar aramışlardır. Ancak siber gibi sınırları olmayan, fiziki dünyadan bağımsız, anarşik yapılı bir olan bu alanda yalnızca bir devlet olarak ulusal çapta yapılan savunmalar ülke açısından yetersiz kalmıştır. Bu alanda da devletler işbirliğine ve siber alanın belli kurallar çerçevesinde yönetilmesine ihtiyaç duymuştur. Peki, böylesine geniş bir yelpazede bulunan siber uzayda, uluslararası siber hukuku sağlamak mümkün müdür? Hangi devlete göre, kim tarafından bu kurallar belirlenecektir? Kurallar karşısında uymayanlara karşı nasıl bir yaptırım uygulanacaktır? Biz de bu çalışmamızda, bu sorulara yanıt arayacağız.

Anahtar Kelimeler: Siber Uzay, Siber Hukuk, Siber Güvenlik, Siber Suç

ABSTRACT

With cyber space being one of these areas where the actors of our age take the most active; in addition to the benefits to humanity in this area, there are also damaging events and situations. The actors are now jeopardized for security and emerged as an area where danger many damaging situations such as, various cyber attacks, cyber threats, spying in cyberspace, cyber warfare. The states, which are of great importance among the actors, have resorted to many defense and activity and defense ways to provide cyber security. They sought legal remedies for cyber defense and security at the national level. However, in this area, which has no borders like cyber, independent of the physical world, and which is anarchic in nature, the defenses made on a national scale as a mere state have been insufficient for the country. In this area, states need cooperation and the need to manage the cyber area within the framework of certain rules. So; is it possible to provide international cyber law in such a wide range of cyber space? By which state and who will be determined by these rules? What sanctions will be applied against those who do not comply with the rules? We will look for answers to these questions in this study.

Key Words: Cyber space, Cyber law, Cyber Security, Cyber Crime

1. GİRİŞ

İnsanlık, tarih boyunca sürekli bir gelişim içerisinde olmuştur. İlk insanlardan günümüze, yaşam şekillerini etkileyecek çok büyük keşifler, icatlar, bilimsel buluşlar gibi her alanda önemli değişimler yaşanmıştır. Bu değişimler içerisinde kuşkusuz çok önemli bir yere sahip olan internetin buluşu da yerini almaktadır. 20. ve 21. Yüzyıllarda bilgisayarların ve internetin ortaya

çıkması ve hayatın her alanın yer almaları, insanlık için çok büyük faydalar ve bir o kadar büyük zararlara sebep olmuştur.

Soğuk Savaş sonrası teknolojide, bilgi ve iletişim ağlarında yaşanan büyük gelişimler, tıpkı hava, kara, deniz ve uzay kadar gerçekliğini kabul ettiğimiz siber alanı doğurmuştur. Birçok yazar ve araştırmacı siber uzayı, dünyanın yeni bir alanı yani dünyanın 5. Alanı olarak nitelendirmektedir. Fiziki dünya ile internet dünyasını birleştiren bu alan, insan eliyle oluşturulmuş sanal bir âlemdir. Bu alan üst bir yöneticinin olmadığı anarşik, coğrafi sınırları olmayan, milyonlarca ağı birbirine bağlayan, küresel bir ortamdır.

Siber uzayı kullanan birey, devlet, kurum, kuruluş, örgüt vb. legal aktörler var olduğu gibi teröristler, casusular, ya da kötü niyetli şahıslar gibi illegal aktörler de bu alanı kullanmaktadırlar. Böylesine geniş bir kullanıcı kitlesi olan ve giriş çıkışın kolay olduğu bir ortamda, faydalı durumlar olduğu kadar zararlı durumların da olacağı tabi ki kaçınılmaz bir şeydir. Siber alana bağlı olarak ortaya çıkan siber tehdit, siber saldırı, siber casusluk ya da siber savaş gibi kavramlar bu zarar verici durumların göstergeleridir.

Ülkelerin fiziki hayattaki bankacılık ve finanstan, enerji sektörüne, su ve elektrik dağıtımından, eğitim sistemlerine, medyadan, savunma sektörüne ve bunun gibi ülkelerin en önemli sektörlerine kadar birçok şey artık sanal ortamda yapılmaktadır. Bu nedenle de ülkeler için hayati önem arz eden kritik altyapılarını, herhangi bir tehlikeye karşı korumak da günümüzde devletlerin önemli görevleri arasına girmiştir. Siber alandaki aktörler bu alanı o kadar derinden kullanmaya başlamışlardır ki, yalnızca bu işin uzmanları değil, buradan çıkar sağlayabilecek kanun dışı bankalar, dolandırıcılar, yasal olmayan ticari tüccarlar, uyuşturucu çeteleri vb. birçok kişi aktif rol almaya başlamıştır. Böylesine kompleks yapıdaki bir alanda ne devletler ne örgütler ne de bireyler bu alanın bir hukuki düzeni olmasını sağlayabilmiş değildir.

2. SİBER SUÇ

Siber suç kavramı birçok kurum ve kuruluş tarafından tanımlanmıştır. Uluslararası Telekomünikasyon Birliği siber suçu; bilgisayarların ve ağların bir araç, hedef ya da bir suç eylemi yeri olarak kullanılan ve burada yasadışı yollarla bilgileri ele geçiren, dağıtan veya bunlara benzer her türlü yasal olmayan davranış biçimi olarak tanımlar (ITU, 2012: 11). Avrupa Ekonomik topluluğuna göre de siber suç; verileri taşıyan ya da bilgilerin otomatik işleme bağlanmasını sağlayan bir sistemde, izinsiz bir şekilde, ahlak dışı olan ve kanunlara aykırı olan her türden davranış biçimidir (Altunok ve Vural, 2011: 75).

Siber suç kavramıyla ilgili daha birçok farklı tanımlamalar olsa aslında özünde tüm tanımlar siber alandaki güvenlik durumunu zedeleyen ve yasal olmayan davranışlarla işlenen suçları anlatmaktadır. Siber uzayın insanlık gelişim tarihine çok önemli katkıları olduğu gibi siber suç ve benzeri eylemlerle de birçok zararlı yönü de bulunmaktadır. Sanal ortamdaki bilgilerin gizliliği, bütünlüğü ve erişilebilirliği birçok saldırı ve tehdite maruz kalmaktadır. Yalnızca yasadışı erişim sağlanması değil, virüs ve kurtçuk gibi küçük yazılımlarla sistemlere zarar verme, DDoS saldırılarıyla hizmet engellemeleri veya organize suçlar, terör, ırkçılık, çocuk pornografisi gibi kendi içinde geleneksel suçları da barındıran suçlar işlenmektedir (Akyeşilmen, 2018: 95-96).

Sanal âlemde işlenen suçlar, fiziksel dünyada işlenen suçlardan farklı özelliklere sahiptir. Geleneksel suça uygulanan yasalar her zaman siber suçlar için geçerli değildir. Örneğin bir kişinin gerçek hayatta yaptığı hırsızlık suçu ile sanal ortamda çaldığı bilgi suçunun aynı olması beklenemez. Çünkü sanal ortamdaki suçların kovuşturulması zordur. Suçun nereden veya kim tarafından işlendiğinin tespiti, gerçek dünyada işlenen suçların tespiti kadar kolay değildir (Karla, 2017: 88-89). Ulusal düzeyde her ne kadar bu konuyla ilgili yaptırımlar belirlense de siber suçlar sınırsızdır yani suçlar ulusal sınır dışından da işlenebilir. Siber dünyada bilgileri saklamak, almak, aktarmak ve silmek daha kolaydır. Bu da suça müdahaleyi imkânsızlaştırır. Ayrıca burada suç işlemenin maliyetinin düşük olması da suçlular açısından bu ortamı daha cazip kılmaktadır.

Siber suçları işlendikleri amaç, hedef ya da araç olarak net bir şeklide kategorilere ayırmak pek mümkün olmasa da günümüzde belli sınıflandırmalar yapılmıştır. Örneğin siber suçta kimi zaman siber, bir araç olarak kullanılıp asıl hedef insan olmuştur. Eylemi gerçekleştirmek için siber alandan faydalanılmıştır. Geleneksel suçların sanal ortamda işlenmiş hali gibi düşünülebilir (Ogunlere, 2013). Siber alan bazen de direkt kendisi bir hedef olmuştur. Daha fazla bilgi ve beceriyle işlenen siber suçlar buna örnektir. DDoS saldırı, web sitelere zarar verme gibi siber uzayın yaygın kullanıldığı suçlardır (Akyeşilmen, 2018: 99). Diğer bir kategoride ise siberin bir mekân olması vardır. Bu suç türlerinde siber bir araç kullanılsa da aynı zamanda suç kaynağıdır. Fiziksel olarak işleyeceği suç için siber uzaydan kaynak sağlamaktadırlar. Örneğin birisini öldürmeyi düşünen kişinin sanal ortamda öldürme yöntemlerini araştırması gibi (Gurjar vd., 2018: 5).

2.1. Siber Suç Çeşitleri

Siber uzayın hızlı gelişimi ve değişimiyle beraber siber alanda işlenen suçlar da her geçen gün artmakta ve çeşitlenmektedir. Bu nedenle de siber suçları kalıplaşmış bir şekilde sınıflamak pek mümkündür değildir. Bazı kurum ve kişilerce sınıflamalara tabii olmuştur. Siber suçları, aldığı hedeflere göre ayıran Gurjar, bu sınıflandırmayı 3 grupta incelemiştir: (Gurjar vd., 2018: 30).

a) Bireylere karşı

i) İnsan (oltalama, spamlar, e-posta sızdırma, bilgisayar sabotajı vb.)

ii) İnsan mülkü (fikri mülkiyet suçları, siber vandalizm, bilgisayar sistemlerini heckleme vb.)

b) Örgütlere karşı

i) Hükümet (heckleme, şifre çalma, siber terörizm vb.)

ii) Firma şirket grubu, bireyler grubu (DoS saldırıları, virüs saldırıları vb.)

c) Genel olarak topluma karşı

(kaçakçılık, sahtecilik, mali suçlar, kritik altyapılara yönelik siber saldırılar vb.)

ITU ise siber suçları 4 ana başlık altında toplamıştır: (ITU, 2012: 12).

1) **Bilgisayardaki veri ve sistemlerin gizliliğine, bütünlüğüne ve kullanılabilirliğine karşı işlenen suçlar** (yasadışı erişim, veri çalma, veriye müdahale vb.)
2) **Bilgisayar ile ilgili suçlar** (online kumar, kimlik hırsızlığı, ücret sahteciliği vb.)
3) **İçerikle ilgili suçlar** (ırkçılık, nefret söylemi, şiddeti övme, yanlış bilgi vb.)
4) **Telif hakkıyla ilgili suçlar** (telif ve fikri mülkiyet haklarına saldırı)

3. SİBER HUKUK İHTİYACI

Günümüz dünyasının yeni tehditlerini oluşturan, bilişim ve teknolojik ağlar içerisinde hukuk dışı çerçevede gerçekleşen siber tehlikeler, bütün dünya ülkeleri tarafından önemli olduğu kabul edilmiş ve ulusal güvenlik unsurları arasında sayılmıştır. Bu amaçla da birçok devlet siber güvenliği sağlamak maksadıyla ulusal çapta önlemler almaya çalışmış ve bu uğurda stratejiler üretmişlerdir. Ancak yalnız başına ulusal çapta uygulanan bu güvenlik tedbirleri ne kadar etkili olabilmiştir? Siber uzay coğrafi sınırları olmayan, diğer alanlardan bağımsız ve anarşik yapılı sanal bir âlemdir (Lıbıckı, 2009: 12). Böylesi geniş bir alanda tek başına bir ülke olarak gerçekleştirilen siber güvenlik faaliyetleri ve hukuki adımlar yeterince etkin olmamaktadır. Siberin hızına ve gücüne yetişebilmek için uluslararası işbirliği büyük önem taşımaktadır.

Gerçekleşen siber suç oranlarına baktığımızda aslında bu konunun hiç de göz ardı edilemeyecek kadar önemli olduğunu da görmekteyiz. 2018 yılında işlenen siber suçların küresel düzeyde 1,5 Trilyon doları aşacağı belirtilmektedir (Nohe, 2018). Siber suçlarda, güvenlik açıklığına sebep olan kişilerin, yoğun olarak kurum içi çalışanlar olduğu gözlemlenmiştir. Bir gün içerisinde

yapılan siber saldırı sayısı giderek artarken, web sitesi hecklemeleri 50 binin üzerine çıkmıştır. İnternet kullanıcı sayısının 2022 yılında yaklaşık 6 milyarı aşacağı tahminleri de, siber suçlarda çeşitlerin ve sayıların artacağının belirtisidir (Akyeşilmen, 2018: 78).

Siber uzayda yaşanan siber saldırı, siber suç ya da siber güvenlik gibi terimler birbirinden bağımsız değildir. Siber saldırı ya da siber suç ortak noktada siber güvenliği etkileyen ve ona zarar veren olaylardır (Akyeşilmen, 2018: 86). Siber saldırı gerçeği, zaman içerisinde bu alana müdahaleyi zorunlu kılmıştır ve siber hukuk konusunun tıpkı diğer hukuk dalları gibi bir ihtiyaç olduğunu ortaya koymuştur.

Ulusal düzeyde devletler kendi hukuk kurallarına, sibere ilişkin kanun hükümlerini koysa dahi henüz uluslararası geçerli bir siber hukuk sistemi bulunmamaktadır. Çünkü her ülkenin kendine özgü hukuk kültürü, teknolojisi ya da savunma ve tehdit algılama şekli vardır. Ülkelerdeki farklı algılayışlar küresel bir siber hukuk kuralları altında birleşmeyi zorlaştırmaktadır. Bir ülkeye yapılan saldırı başka bir devlet tarafından mı yoksa bir birey ya da bir terör örgütü tarafından mı yapılıyor bunu öğrenmek kolay değildir. Siber alandaki saldırıların kaynaklarının tespiti zordur. Coğrafi sınırları belli olmayan ve kesin kimlik tespiti yapılamayan bu saldırılar karşısında ülkelerin nasıl bir ortak noktada buluşacağı, bir sorundur. Kime göre ve neye göre siber saldırı kabul edilecek? Ayrıca bazı devletler yerel yasalarını, uluslararası hukukun getireceği yasalara karşı üstün tutmaktadır. Bir devletin iç hukuku veya anayasa hukuku, uluslararası anlaşmanın gerektirdiği bir eylemi reddedebilir. Bu da uluslararası hukukun üstünlüğünün ihlaline neden olmaktadır (Schmitt and Vihul, 2014: 12). Her ülkenin tehdit anlayışı ya da tehditler karşısında gösterdiği davranışlardaki farklılıklar bu işbirliğini zora sokan başka nedenlerdendir. Siber gibi soyut bir alanda geleneksel olan hukuk kurallarını koymak ve düzenlemek kolay değildir.

Özellikle teknolojik açıdan çok fazla gelişmiş olan ülkeler siberi uzayı daha fazla kullandığı için bu alana olan bağımlılıkları da daha fazladır. Dolayısıyla gelişmemiş ülkelere oranla siber tehditlere daha açık konumdadır. Bu yüzden de gelişmiş ülkeler tek başlarına savunmada yeterli olamayacaklarını bildikleri için uluslararası işbirliği konusunda daha fazla adım atmaya çalışmaktadır. Bu ülkelere en iyi örnek Amerika Birleşik Devletleridir. İnternete ve iletişim sistemlerine en bağımlı olan ve bu sistemlere ayırdığı serveti çok fazla olan ABD'nin siber saldırılardan en büyük payı alması kaçınılmazdır. ABD hükümetinin bu konuyla ilgili uluslararası müzakerelere girme baskısı, kritik altyapılarını ve diğer dijital varlıklarını uluslararası işbirliği olmadan yeterince koruyamayacağını anlayarak birçok ulusal ve uluslararası girişimde bulunmuştur (Goldsmith, 2011: 2).

Siber hukuk, esasen siber alan ve siber alan yönetişiminin düzeni ile ilgilidir ve kendi içinde alt konuları barındırır. Alt konuları siber suç, elektronik ve dijital imza ve fikri mülkiyet hakları ile veri koruma ve mahremiyet alanları olan siber hukuk, henüz yeni bir hukuk dalıdır (Jahankhani ve Diğerleri, 2014:153-155; Gurjar ve Diğerleri,2018:7). Siber hukuk devletlerin ulusal çapta tam anlamıyla yeterli olmasa bile yine de etkinlik sağlayabildiği fakat uluslararası düzeyde etkinliği olmayan bir hukuk dalıdır.

4. SİBER HUKUKA FARKLI YAKLAŞIMLAR

Sağlıklı bir Siber Hukuk kanunlarının oluşturulması için temel alınan yaklaşımları Lunker şöyle anlatmıştır:

- Ülkeler yeni yasalarını oluşturulmalı veya mevcut durumdaki yasalarını değiştirmeli, böylece internetin üzerinde etkili olduğu tüm eylemleri düzenleme olanağı sağlar
- Ülkeler, internette özellikle uygulanabilir yeni ve tek tip kurallar oluşturmak için çok taraflı uluslararası anlaşmalara girebilirler.
- Yeni kurallar ve bu kuralları uygulamak için yeni yollar oluşturabilecek tamamen yeni bir uluslararası kuruluş oluşturulabilir

- Kurallar, DNS (alan adları sistemi) ve IP adresi kaydı gibi bireysel kararlardan ve kime hükmedeceklerine karar veren web siteleri ve kullanıcılar tarafından doğal olarak ortaya çıkabilir (Lunker, 2018).

Bu yaklaşımlara göre siber hukukun nasıl olması gerektiğine dair birçok farklı yaklaşım olduğunu görmekteyiz. Kimi anlayışa göre siber alandaki sağlanmak istenen düzen ulusal bir hukuk düzenlemesiyle sağlanabilecekken başka bir yaklaşıma göre uluslararası işbirliği şarttır. Bir diğer yaklaşıma göre siber alan yönetişimi için tamamen bunlardan bağımsız yepyeni bir küresel örgüt kurulmalıdır. Bütün bunların dışında bir de siber alana müdahale edilmeyip kuralların kendiliğinden oluşabileceğini söyleyen bir anlayış da vardır.

5. KÜRESEL SİBER HUKUK ÇALIŞMALARI

1960'lı yıllarda doğan internet dünyasına ancak 1990'lı yılların sonunda düzenlemeye yönelik çalışmalar yapılmaya başlanmıştır. İnternet kullanıcı sayısındaki artış ve hızlı yükseliş ve uygun bir yasal çerçevenin bulunmamasıyla siber hukuk alanındaki kaygılar artmıştır (Lunker, 2018). Yıllarca süren tartışmalara ve her tür sınır aşan sanal çatışmalara rağmen, dünya ülkeleri, ulusal sınırlar dışındaki İnternet zararlarını engellemek ve hukuki açıdan düzenleme yapabilmek için tek bir anlaşma yapmayı başarmıştır, o da Avrupa Konseyi Siber Suçlar Sözleşmesi'dir.

Avrupa Konseyi'nin hazırladığı Siber Suçlar Sözleşmesi, siber suçlara karşı hukuki açıdan karar alınmasını sağlayan ve taraf olan devletler içinde kararların bağlayıcı olması açısından bugüne kadar bölgesel çaptaki en önemli adımdır. Avrupa Konseyi 47 ülkeden oluşmaktadır. 2001 senesinde imzalanan ve 2004 senesinde yürürlüğe giren sözleşmeyi, 45 devlet onaylamıştır (Akpek, 2015: 17-19). Bu sözleşmede amaç "toplumun siber suçlara karşı korunmasına yönelik ortak bir ceza politikası" oluşturulmaktadır. Üye ülkelerin mevzuatlarını bilişim suçlarıyla ilgili hükümlere uyumlu hale getirmeyi hedeflemişlerdir (Aliusta ve Benzer, 2018: 38). Yasadışı erişim ve müdahale, veri ve sistem müdahalesi, cihazların kötüye kullanılması, sahtecilik, sahtekârlık dâhil olmak üzere çeşitli bilgisayar suçlarını yasaklayan yasaların kabul edilmesini gerektiren bir anlaşmadır. Yalnızca kendi üyeleri için değil diğer devletler için de siber suçlarla mücadelede iyi bir rol model olmuştur. Yine NATO'nun bu yöndeki düzenlemeleri ile Şangay benzeri birkaç bölgesel çalışmalar haricinde pek fazla bağlayıcı düzeyde küresel bir anlaşma yapılmamıştır (Akyeşilmen, 2018: 93).

Dünyadaki en büyük örgütlerden birisi olan Birleşmiş Milletler (BM), yaptığı anlaşmalarla üye ülkelerini bağlayıcı kararlar alma gücüne sahiptir. Siber alandaki tehditlere karşı ilk olarak, 1990 yılında gerçekleştirdiği 8. Suçların Önlenmesi ve Suçlulara Muamele Kongresi'nde hazırlanan raporla, BM Genel Kurulunca siber alanı düzenleme konusuyla ilgili kararlara yer verilmiştir (Eight United., 1990). İlerleyen yıllarda ceza ve usul hukukuna bilgisayar ile işlenen suçların engellenmesi ve bu konuda işbirliği yapılmasına dair BM Bilgisayar Bağlantılı Suçların Önlenmesi ve Kontrol Altına Alınması Rehberi eklenmiştir. BM Genel Kurul'u 2001 senesinde yine uluslararası alanda işbirliğini sağlamak ve bu teşvik etmek, siber suçlarla mücadele de yetkililere eğitim vermek gibi amaçlarla "Bilgi Teknolojilerinin Kötüye Kullanılması ile Mücadele" adlı kararı almıştır (UN GAOR, 2001). 2005 yılında BM siber alana yönelik siber suçlarla mücadele kapsamında sözleşme için tartışmalara başvursa da. Örgüt bu kapsamda sözleşme yapmak yerine ülkelere destek vermenin daha verimli olacağını düşünmüştür. Devletlerin çıkarlarındaki farklılıkları ve farklı yaklaşımları, bu alanda gerçekleşecek işbirliğine engel olmuştur (Akyeşilmen, 2018: 92).

Ekonomik Kalkınma ve İşbirliği Örgütü (OECD), siber suçlarla mücadelede ulusal ve uluslararası hukuki durumların uyumlaşması için öncülük etmiş örgütlerdendir. Zaman içerisinde bu konuyla ilişkili kararlar almaya çalışmıştır. Bunlardan bir tanesi de 1992 yılında aldığı "Bilgi Güvenliği Sistemleri için Rehber ile İlgili Kurul Tavsiyesi" kararıdır. Bu karar yıllar geçtikçe yeni dönemlere göre uyarlanmıştır. Bu karar ülkeler açısından bağlayıcı nitelikte değil, bir tavsiye niteliğinde olmuştur (OECD, 2012: 34). Siber hukuk yolunda yine 2008 yılında OECD tarafından Online Kimlik Hırsızlığı Rehberi yayınlanmıştır.

Dünyanın en gelişmiş endüstrilerine sahip olan 8 ülkenin bir araya gelerek oluşturduğu G8, siber alanda da güvenliklerini sağlamayı istedikleri için çeşitli girişimlerde bulunmuştur. 1997 yılında siber suçlara karşı, suçluların yargılanması ve cezalandırılması amacıyla Denver Zirvesi'nde bir bildiri yayınlamıştır ve 40. Maddesinde bu isteğini açıklamıştır (G8, 1997). Günümüze kadar da bu yöndeki istekleri doğrultusunda faaliyetler göstermeye çabalamıştır. Siber alanda daha güvenlikli bir şekilde hareket etmeyi hedeflemiş, bu amaçla da G8 üyelerine, bu konulardaki tavsiyelere uymalarını ayrıca Avrupa Konseyi'nin siber alan için yayınladığı sözleşmeye katılmalarını tavsiye etmiştir.

Siber alandaki suçlarla mücadelede hukuki açıdan aktif olmaya çalışan bir diğer örgüt ise Avrupa Birliği'dir. 2013 yılında siber uzayda karşılaşılabilecek sorunlar ve her türlü sibere dair Birliğin sorunlarında çözüm olabilmesi adına AB Siber Güvenlik Strateji Belgesi yayınlanmıştır (Akpek, 2015: 16). Yine bu kapsamda siber suçları engellemek için kendi bünyesindeki Avrupa Komisyonu tarafından Avrupa Siber Merkezi kurulmuştur. 2001'de "Dolandırıcılık ve Parada Sahtecilik Suçları ile Mücadele için Çerçeve Kararı", 2002'de "E-Gizlilik Direktifi(2002/22/EC)" yayınlanmıştır. 2013 yılında "Bilgi sistemlerine yönelik saldırılara ilişkin Avrupa Birliği Direktifi" düzenlemesi yapılmıştır.

Siber saldırıları dolaylı olarak düzenleyen uluslararası yasal rejimler arasında Uluslararası Telekomünikasyon Kanunu, Havacılık Kanunu, Uzay Kanunu ve Deniz Kanunu yer almaktadır. Bu rejimler, siber saldırılarda kullanılabilecek siber alanın bölümlerini düzenlemektedirler (Wrenn, 2012: 156). Kısacası bölgesel ve küresel örgütler güvenliklerini sağlamak ve siber suçlardan arınmak için, uluslararası işbirliği ve uluslararası hukukun uygulanabilmesi için girişimlerde bulunmuşlardır. Ancak her şeye rağmen istenilen uluslararası bir siber düzen sağlanamamıştır.

6. SONUÇ

Dünyada her alanda suç işlenebildiği gibi siber alanda da, siberin kendine has özellikleri itibariyle suç işlenmesi kaçınılmaz bir durumdur. Anarşik bir yapıda ve anonim olan bu alan suçlular için çok ideal bir âlemdir. Burada suç işlemenin maliyeti oldukça düşükken, işledikleri suçun karşılığı olan kazançları ise çok daha fazladır. Bu yüzden de siber âlem suçları gün geçtikçe artmakta ve siber suç piyasası artık trilyon dolarla yürümektedir. Bu suçlar karşısında da doğal olarak güvenliğini sağlamak isten aktörler daha fazla güvenlik için çalışmaktadır. Böylece güvenliği sağlamanın da maliyetleri giderek artmaktadır.

Siber güvenliklerini sağlamak için uğraşan aktörlerden en önemli yeri alan devletler de bu yönde birçok faaliyet gerçekleştirmektedir. Bunlardan biri de hukuki açıdan güvenliği sağlamaktır. Birçok ulus hukuki çerçevelerine siber alan düzenlemelerini eklemiştir. Ulusal normlarla güvenliklerini sağlamayı hedeflemişlerdir. Ancak bu normlar belli bir noktaya kadar fayda sağlasa da siber suçların coğrafi bir sınırının olmaması, saldırıların kim tarafından yapıldığının tespitinin zor olması, kendi hukuki normlarıyla başka uluslara karşı bunu kullanamaması gibi sebepler dolayısıyla ulusal çaptaki hukuki müdahale yetersiz kalmıştır. Uluslararası boyutta bir siber hukuka ihtiyaç vardır.

Uluslararası siber güvenliğin oluşturulması ve uygulanması için bazı örgütler veya aktörler bu kapsamda çeşitli adımlar atsa da şuan ki mevcut durumda böyle bir hukuki düzenleme henüz bulunmamaktadır. Çünkü ülkelerin kendi hukuki anlayışları, suç algılayışları ve buna benzer birçok farklılıkları uluslararası alanda ortak bir hukuki sistemi oluşturmayı zora sokmaktadır.

KAYNAKÇA

Akpek, N. O. (2015). "Siber Suçlar Sözleşmesinin Getirdikleri ve İç Hukuk Açısından Konuya Yaklaşım", Yüksek Lisans Tezi, İstanbul Üniversitesi, Sosyal Bilimler Enstitüsü, İstanbul.

Akyeşilmen, N. (2018b). Disiplinlerarası Bir Yaklaşımla Siber Politika & Siber Güvenlik, Orion Kitapevi, Ankara.

Aliusta, C. & Benzer, R. (2018). "Avrupa Siber Suçlar Sözleşmesi ve Türkiye'nin Dahil Olma Süreci", Uluslararası Bilgi Güvenliği Mühendisliği Dergisi, 4(2), 35-42.

Altunok, E. & Vural, A.F. (2011). "Bilişim Suçları", http://dergipark.gov.tr/download/article-file/208853, Erişim Tarihi: 27.02.2019.

Eight United Nations Congress on the Prevention of Crime and the Treatment of Offenders, (1990), A/RES/45/121, UN GAOR, https://www.un.org/en/ga/search/view_doc.asp?symbol=A/RES/45/121, Erişim Tarihi: 24.02.2019.

G8 (1997). Denver Summit of the Eight: Communiqué. http://www.g8.utoronto.ca/summit/1997denver/g8final.htm, Erişim Tarihi: 24.02.2019.

Goldsmith, J. (2011). Cybersecurity Treaties A Skeptical View. (edited by Peter Berkowitz) in Future Challenges in National Security and Law. http://www.futurechallengesessays.com, Erişim Tarihi: 19.02.2019.

Gurjar, L.R. ve Diğerleri (2018). Cyber Crime, http://assets.vmou.ac.in/PGDCL04.pdf, Erişim Tarihi: 27.02.2019.

ITU (2012). Understandıng Cybercrıme:Phenomena, Challenges and Legal Responses, http://www.itu.int/ITU-D/cyb/cybersecurity/docs/Cybercrime%20legislation%20EV6.pdf, Erişim Tarihi: 27.02.2019.

Jahankhani, H.; Al- Nemrat, A.; Far, A.H. (2014). "Cybercrime classification and characteristics". (Ed. Babak Akhar, Andrew Staniforth Francesca Bosco), Cyber Crime and Cyber Terrorism Investigator's Handbook, ss. 149-164, https://www.sciencedirect.com/book/9780128007433/cyber-crime-and-cyber-terrorism-investigators-handbook, Erişim Tarihi: 27.02.2019.

Kalra, K. (2017). "Emergence of Cyber Crimes: A Challange for he New Millennium", Bharati Law Review, 86-103.

Libicki, M.C. (2009). Cyberdeterrence and Cyberwar, RAND Corporation, U.S.A.

Lunker, M. (2018). Cyber Laws: A Global Perspective, http://unpan1.un.org/intradoc/groups/public/documents/apcity/unpan005846.pdf, Erişim Tarihi: 22.02.2019.

Nohe, P. (2018). 2018 Cybercrime Statistics: A closer look at the "Web of Profit",

https://www.thesslstore.com/blog/2018-cybercrime-statistics/, Erişim tarihi: 27.02.2019.

OECD (2012). "Review of the 2002 Security Guidelines". http://www.oecd.org/sti/ieconomy/Security%20guidelines%20review.pdf, Erişim Tarihi: 24.02.2019.9

Ogunlere, S. (2013). "Cyber Crimes and Cyber Laws in Nigeria", The International Journal Of Engineering And Science, 2(4): 19-25.

Schmitt, M. N. and Vihul, L. (2014). "The Nature Of Internatıonal Law Cyber Norms", Tallinn Paper No. 5, Tallinn.

UN GAOR (2001). Combatting the Criminal Misuse of Information Technologies, A/RES/55/63, Agenda Item 105. http://www.itu.int/ITU-D/cyb/cybersecurity/docs/UN_resolution_55_63.pdf, Erişim Tarihi: 24.02.2019.

Wrenn, C. F. (2012). "Strategıc Cyber Deterrence". Doctoral Thesis, The Fletcher School of Law and Diplomacy, Medford.