SİBER UZAYIN SINIRSIZ DOĞASI ÇERÇEVESİNDE ULULARARASI İLİŞKİLERDE SINIRLAR ÜZERİNE BİR ANALİZ

Doğan ARAR♣

Özet

21. yüzyılın dünyasında küreselleşme, modern ulus devlet ve sınırları karşısında "siber uzay" adı verilen teknolojik gelişme ile belki de en ciddi kartını oynamaktadır. Son yıllarda hız kazanan bilgi ve iletişim teknolojilerindeki gelişmeler neticesinde ortaya çıkan siber uzay ile devletlerin sınırları aşınma ya da yok olma riski altındadır. Sınırsız özgürlükler ve kolaylıklar sunan yapısı itibariyle siber uzay, devletlerin egemenliği açısından pek çok problem oluşturmaktadır. Bu durum son dönemde siber çatışmaların artışına neden olmuştur. Siber uzayda fâillerin tespit edilmesindeki güçlükler (anonimlik), eylemin fiziksel eylemlerden farklılığı, uluslararası hukukun uygulanmasından doğan sıkıntılar, siber uzayda ülke sınırlarının rahatlıkla geçilebilen karakteristikleri ile Westphalian ulus devlet için eşi benzeri görülmemiş bir meydan okumadır. Tüm bu noktalardan hareketle makalede, siber uzayın, uluslararası ilişkilerin kurucu fenomenlerinden biri olan sınırlar üzerinde yarattığı değişim ve dönüşümler tartışılmıştır.

Anahtar Kelimeler: Sınırlar, Siber Uzay, Uluslararası İlişkiler.

AN ANALYSIS ON BORDERS IN INTERNATIONAL RELATIONS WITHIN THE FRAMEWORK OF THE BORDERLESS NATURE OF CYBERSPACE

Abstract

In the world of the 21st century, globalization plays the most serious card, which is called cyberspace, against the modern nation state and its borders. The borders of states are at risk of erosion or extinction with the emergence of cyberspace as a result of advances in information and communication technologies that gained speed in recent years. Cyberspace creates many issues in point of the sovereignty of states due to its structure that offers unlimited freedoms and facilities. This circumstances recently led to an increase in cyber conflicts. Cyberspace is an unprecedented challenge for Westphalian nation state, with difficulties in identifying perpetrators (anonymity), the unique nature of activities separate from physical interactions, the difficulties arising from the application of international law and the easily accessible characteristics of the state and its borders. On the basis of all these points, the article discusses

♣ Yüksek Lisans Öğrencisi, Uluslararası İlişkiler Bölümü, Selçuk Üniversitesi.

the changes and transformations created by cyberspace on borders, which are one of the founding phenomena of international relations.

Keywords: Borders, Cyberspace, International Relations.

Giriş

Modern uluslararası ilişkiler, yaklaşık 370 yıl önce, Avrupa'da Otuz Yıl Savaşları'na son vermek üzere imzalanan Westphalia Barışı (1648) ile başlamıştır. Avrupalı diplomat ve prensler imzaladıkları antlaşma serisinin adıyla da anılan, modern bir uluslararası sistem (Westphalian Sistem) ve ulus devlet dizayn etmişlerdir. Bu yeni dönemde pre-Westphalian dönemin aksine, devletlerin egemen eşitliği ve birbirlerinin içişlerine karışmama (non-intervention) ilkelerine dayalı yeni bir model ön plana çıkmıştır. Westphalia modeli, modern ulus devletin egemenlik "alanının sınırlarını" çizmiştir. Sistemin ve ulus devletin en temel bileşenleri olan sınırlar (borders) ve bu sınırlar içerisinde egemen olunan alan/toprak/bölge/ülke (territoriality) ise, modern uluslararası ilişkilerin doğması ve hayatta kalmasının yegâne sebebi olmuştur. Fakat 20. yüzyılın ikinci yarısı itibariyle hız kazanan küreselleşme furyası, bu iki olgunun varlığına bir meydan okuma şeklinde algılanmıştır. Marshall McLuhan'ın tâbiriyle dünyayı küçük bir köy haline getiren küreselleşme, zamanla devlet teritoryasını (ülkesini) ve sınırlarını tehdit eder hâle gelmiştir (McLuhan, 1992). Buna ek olarak küreselleşme, devletlerin sınırlarını tam olarak ortadan kaldırmamakla birlikte aşındırmıştır. O nedenle makalenin birinci bölümünde Uluslararası İlişkiler disiplininde sınırlar ele alınmıştır.

Küreselleşmenin en önemli yapıtaşlarından birisi de, kuşkusuz bilgi ve iletişim teknolojilerindeki(BİT) gelişmeler ve bu bağlamda ortaya çıkan "siber uzay" oluşturmaktadır. Günümüzde dijital olan her şeye refere eden siber uzay kavramının tarihsel ve felsefî kökleri, kimi zaman Platon'un "Mağara Alegorisi"ne kadar götürülmektedir (Choucri, 2012: 7). Siber uzay genel anlamda, bilgi sistemleri, bilgisayar ağları, telekomünikasyon altyapılarının kesişimiyle meydana gelen ortamdır (Wingfield, 2000). Bununla birlikte kavram ilk kez bilim kurgu yazarı William Gibson tarafından 1984'te kaleme alınan *Neuromancer* adlı kitabında ifade edilmiştir (Gibson, 1984: 69). Kurucu miti "kontrol edilemezlik" olan siber uzayın, mekândan muaf, anarşik ve oldukça geniş kapsamlı doğası, Gibson'ın "karmaşa" tâbirini haklı çıkarmaktadır. İnternet kullanımının yaygınlaşmasıyla toplumsal hayatı derinden etkileyen siber uzay, 20. yüzyılın sonlarına doğru -diğer disiplinlerde olduğu gibi-

Uluslararası İlişkiler disipilininde de ağırlığını hissettirmeye başlamıştır. Siber, sınırlar ve ülkeselliğe –yani sınırlara ve egemenliğe- dayalı devlet-merkezli modern uluslararası sistemi çatırdatmıştır. Bu durum Gibson'ın "karmaşa"sının, devletlere "kötü"yü çağrıştırmasına neden olmuştur.

21. yüzyılda hayatın neredeyse her kademesine işleyen siber uzayın nimetlerinden, devletler olduğu kadar uluslararası sistemin diğer oyuncuları da faydalanmaktadır. Fiziksel ortama oranla çeşitli kolaylıklar ve imkânlar sunan yapısı, siber ortamda işlenen suçların, terörizmin ya da saldırıların önünü açmaktadır. Siber uzay, eylemi icrâ eden faillerin kimliklerinin tespit edilmesindeki güçlükler (anonimlik), eylemin fiziksel eylemlerinden çok daha farklı niteliği, ulusal ya da uluslararası hukuk normlarının uygulanabilirliğinden ileri gelen sıkıntılar, devlet ülkesinin ve sınırlarının rahatlıkla geçilebilirliği gibi özellikleri nedeniyle Westphalian ulus devlet için eşi benzeri görülmemiş bir meydan okumadır. Siber uzayın *res communis* (herkese ait olan) veya *res nullius* (hiç kimseye ait olmayan) doğası, uluslararası ilişkilerin bireyden devlete kadar tüm aktörlerine "sınırsız" özgürlükler vaat etmektedir. Bu da, hâli hazırda küreselleşmeyle sınırları aşınmış ulus devletler nezdinde Estonya, Gürcistan ve İran (Stuxnet) saldırılarında da görüldüğü gibi büyük problem yaratmaktadır. Buradan hareketle makalenin ikinci bölümünde ise siber uzay ve uluslararası sınırlar özelinde neden olduğu problemler ele alınmıştır.

Görünüşe göre siber uzay, ulus devletlere, egemenliklerinin istikrarı noktasında tam da 370 yıl önce Avrupalı diplomat ve prenslerin yaptığını yapmaktan başka çare bırakmamaktadır. Bir yanda uluslararası dijital sınırlar çizerek, bunları siber uluslararası hukuk ile korumak isteyen, yani birbirlerinin egemenliklerine saygı duydukları "Siber-Westphalia" hayâliyle yanıp tutuşan devletler vardır. Diğer yanda ne bir uluslararası sınır, ne de uluslararası hukuk tanıyan "karmaşık" bir ortam vardır. Şüphesiz bugün için pek mümkün gözükmeyen Siber-Westphalia'nın, gelecekte var olup olmayacağı hususunda bir öngörüde bulunmak kesinlikle kolay olmayacaktır. Fakat makalenin sonuç bölümünde, bu çok bilinmeyenli denklem için –zor da olsa- bir cevap aranmaya çalışılmıştır.

Uluslararası İlişkilerde Teritoryal Sınırlar

İngiliz sosyolog Thomas B. Bottomore, modern dünyanın en önde gelen siyasal birimi olarak modern ulus devleti işaret etmiştir (Bottomore, 1987: 59). Modern ulus devleti pre-

Westphalian dönemin devletinden ayıran aslî unsur ise, şüphesiz egemenlik ve onun uzantıları olan sınırlar (borders) ve ülkeselliktir (territoriality). Avrupa'da Otuz Yıl Savaşları sonunda imzalanan Westphalia Antlaşması (1648), egemenliğin hiyerarşi yoluyla paylaşıldığı Ortaçağ düzenini lağvetmiş, yerine "sınırları" belli bir "alanda" egemen olan ulus devletleri ve sistemini getirmiştir. Ulus devletin önemli karakteristiklerinden sayılan egemenlik Westphalia'da, "içişlerine karışmama" ve "devletlerin egemen eşitliği" ilkelerinin üzerine inşa edilmiştir. Hans Max Huber'in tam da vurguladığı gibi egemenlik, devletler arası ilişkilerde bağımsızlığı ifâde etmektedir (Aufricht, 1944: 149). Bu denli önemi nedeniyle egemenlik, Uluslararası İlişkiler disiplininin de referans kavramlarından biri hâline gelmiştir. Westphalian egemenliğin temel bileşenlerinden biri olan sınırlar ise, modern uluslararası ilişkileri yaratan ve bir disiplin olarak yaşamasını sağlayan kavramdır. Diğer taraftan sınırlar da modern devletin inşasıyla hayat bulmuştur (Le Goff, 2005: 3). Westphalian teritoryalitenin (ülkesellik) ayrılmaz parçası olan sınırlar, disiplinin ilk yıllarında egemenlik çalışmalarının alt başlığı olmuştur. Sınırlar her şeyden önce zihinlerde coğrafî bir çağrışım uyandırmaktadır. Bunun için doğal olarak, 19. yüzyıla kadar kendine "Coğrafya" çalışmalarının içinde yer bulmuş, zamanla Tarih, Sosyoloji, Antropoloji, Hukuk, Siyaset Bilimi gibi disiplinlerin kapsamına girerek *interdisipliner* bir terim halini almıştır.

Malcolm Anderson'a göre sınırlar, yalnız haritalarda yer alan basit çizgiler değil, aynı zamanda politik ortamı anlamanın olmazsa olmazıdır (Anderson, 1996: 1). 1960'larla beraber dünyada yaşanan siyasî, ekonomik, teknolojik gelişmeler küreselleşme sürecinin hızlanmasına sebep olmuş, sınır ve bölge kavramları bir kez daha gündeme taşınmıştır. Küreselleşmenin "sınırsız" (borderless) mottosu, sınır çalışmalarına (limology) olan ilgiyi artırmıştır. Bu dönemde özellikle Julian Minghi ve Victor Prescott'un çalışmaları ses getirmiştir. Sınırları siyasî coğrafyanın en somut fenomeni olarak nitelendiren Minghi (Minghi, 1963: 407), 1963'te *Boundary Studies in Political Geography* adlı çalışmasını tamamlamıştır. Minghi'nin çalışmasını, Prescott'un *The Geography of Frontiers and Boundaries* (1965), *The Maritime Political Boundaries of the World* (1985) ve *Political Frontiers and Boundaries* (1987) adlı çalışmaları takip etmiştir. Bu iki ismin öncülüğünü yaptığı çalışmalar, büyük sükse yapması nedeniyle, Henk van Houtum'un da ifadesiyle ilham verici mahiyettedir (Houtum, 2005: 672). Sınırlar, bir çalışma alanı olarak, nihâyet 1990'larla birlikte Uluslararası İlişkiler disiplininin gündeminde yer almaya başlamıştır (Newman 2007: 30; Paasi, 2013: 3). 1990'lardan itibaren yapılan çalışmaların odak noktasında sınırlar olsa da, kavram "territoriality"den (ülkesellik/bölgesellik/mekansallık olarak Türkçeleştirilebilir) bağımsız olarak

değerlendirilmemiştir. En nihâyetinde sınırların oluşumu için birden fazla siyasal birimin egemen olduğu fiziksel alanların/bölgelerin varlığı şarttır. Bu nedenle konunun araştırmacıları, kavramın "territoriality" ile yekvücût olduğunun altını çizmişlerdir. Örneğin David Newman, bu iki kavramın beraber anlam ifade ettiğini savunmuş, biri olmadan ötekinin anlaşılamayacağını belirtmiştir (Newman, 2010: 774). Benzer bir yorum da Anssi Paasi'den gelmiştir. Paasi sınırların kavram olarak territoriality ile derinlemesine bağlı olduğunu vurgulamıştır (Paasi, 2005: 668). Öte yandan Friedrich Ratzel, Richard Hartshorne, Ladis Kristof and Julian Minghi gibi sınır çalışmalarının önde gelen isimleri de sınırların, alanın/bölgenin ve ulus devletlerin ortak evrimine dikkat çekmiştir (Laine, 2015: 18).

Yunanca "*synoran*/*sinoron*" kelimesinden gelen sınırlar, özü itibariyle "içeri"dekileri "dışarı"dakilerden ayıran ve esirgeyen sosyal olgudur. Sınır kavramı, deyim yerindeyse "dört başı mamur" bir tanımdan yoksun olsa da, kabaca somut ya da soyut bölme hatlarına refere etmektedir. Genellikle bitişik iki ülkeyi, iki bölgeyi, iki araziyi vb. ayıran çizgi; hat; hudut; limit olarak nitelendirilmektedir (Büyük Larousse). Bir başka tanıma göre sınırlar en genel anlamda politik, sosyal, yasal alanları birbirinden ayıran çizgilerdir (https://en.oxforddictionaries.com, 5 Aralık 2018'de erişildi). Sınırların belirlenmesinde devletler doğal ya da yapay unsurları kullanabilir. Doğal unsurlar akarsular, sıradağlar, göller, denizler gibi fizikî öğelerdir. Örneğin Güneybatı Avrupa'da yer alan Pirene Dağları Fransa-İspanya sınırını oluşturmaktadır. Yine Batı Avrupa'da Ren Nehri, Orta Avrupa'da ise Tuna Nehri pek çok bölge ülkesinin sınırını çizmesi bakımından önemlidir. Yapay unsurlar ise, enlem ve boylam çizgileri gibi sunî öğelerdir. Sınır çizen yapay unsurların en meşhur örneklerinden birisi, Kore Yarımadası'nı Kuzey Kore ve Güney Kore şeklinde ikiye bölen 38. enlem çizgisidir. Doğal ve yapay unsurların oluşturduğu sınırlara ek olarak, disiplinde son yıllarda ivme kazanan "mental sınırlar" kavramını da hatırlatmak gerekir. Mental sınırların belki de en iyi örneklerinden biri, doğal ya da yapay sınırlardan oluşmasına rağmen, ideolojik bir altyapısı olan Demir Perde (The Iron Curtain)'dir. Soğuk Savaş'ta Baltık Denizi'ndeki Stettin'den Adriyatik'teki Trieste'ye kadar, Avrupa'yı iki ideolojik kampa ayırması nedeniyle sembolik bir "sınır" işlevi olan Demir Perde, dönemin İngiltere Başbakanı Winston Churchill tarafından bu bölünmeyi belirtmek üzere kullanılmıştır. Öte yandan ister doğal, ister yapay, ister mental olsun sınırlar insanların ya da devletlerin belirlediği olgulardır. Bu bakımdan sınırlar *ahistorik* değildir. Tersine, tarih boyunca süregelen savaşlar, imzalanan antlaşmalar gibi faktörlerin etkisi yadsınamayacak kadar büyüktür.

Sınırlar, dünya askerî ve siyasî tarihinin de odak noktasını oluşturmaktadır. Savaşlar büyük ölçüde devletlerin sınırları/hudutları genişletme arzusuyla yapılmıştır. Robert Gilpin, devletlerin tarih boyunca, güvenlik, ekonomik ve diğer çıkarlarına hizmet etmek amacıyla sınırlarını genişlettiklerini belirtmiştir (Gilpin 1981: 23). Jacques Ancel ise sınırları çatışmalar, fetihler ve askeri genişlemeler sonucu sürekli değişime uğrayan çizgilerden ibaret görmüştür (Ancel, 1938). Dolayısıyla tarihsel pratiğin çıktısı olan sınırlar, zaman zaman değişime ve dönüşüme tabi olmuştur. Bugünkü anlamıyla (modern) sınırlar, uluslararası hukuk ve uluslararası sistemi şekillendiren unsur olarak, tıpkı bu iki kavram gibi Westphalia Barışı'nın ürünüdür. Modern ulus devlet öncesi hakim olan imparatorluk düşüncesinde sınır kavramının yeri sınırlıdır. Bu nedenle Anthony Giddens, sürekli genişleme idealinde olan imparatorlukların sınırlarından çok hudutları olduğunu belirtmektedir (Giddens: 2008). Hudut kavramı daha çok imparatorluklar/kültürler arasındaki sosyo-mekansal ayrışmayı ifade ederken, sınır kavramı -daha keskin olmakla birlikte- ülkeleri birbirinden ayıran çizgilere işaret etmektedir (Houtum, 2005: 672). Kısacası imparatorluğun hudutları (boundaries-lines) daha şeffaf/geçirgen çizgileri, modern ulus devletin sınırları (borders) ise katı/keskin çizgileri çağrıştırmaktadır. Nitekim Uluslararası İlişkiler disiplininde Westphalia Barışı sonrası imparatorluk hudutlarının peyderpey ulus devlet sınırlarına evrildiği görülmektedir.

Giddens'a göre ulus-devletler hudutlarını genişletmekten ziyade, sınırları içerisinde düzeni tesis etmeyi ve vatandaşlarına ahlâkî bir yaşamı cazip kılmayı amaçlamaktadır (Giddens: 1998: 24). Sınır çalışmalarının önemli ismi Victor Prescott da devletlerin sınırlarını, içeride ve dışarıda barışın/düzenin tesisi ve egemenliklerinin "sınırlarını" belirlemek üzere çizdiğini belirtmektedir (Prescott, 1987: 80). Siyasî Coğrafya'nın kurucu babası Friedrich Ratzel ise devleti aynı insan gibi doğan, gelişen, yaşlanan ve nihayet ölen bir "organizma"ya benzettiği *Politische Geographie* (1897) adlı eserinde sınırlara da değinmiştir (Günel, 1995: 458). Ratzel'e göre devletin en az merkezî bölgeleri kadar önemli kenar bölgeleri olan sınırlar, aynı zamanda devlet iktidarının bir göstergesi ve ölçüsüdür (Giddens, 1998: 49). Ayrıca en önemli işlevlerinden biri, içeridekileri dışarıdakilere karşı koruyan bariyer (Oomen, 1995; Sibley, 1995) olan sınırlar, Newman'a göre istenmeyen unsurların devlet ülkesine girişini engellemektedir. Ona göre sınırlar, bir ülkeyi dışarıdan gelebilecek işgal, uyuşturucu ticareti, göçmen işgücü, serbest piyasada rekabetin yarattığı riskler, kaçakçılık gibi tehditlerden korumaktadır (Newman, 2003: 14). Diğer taraftan devletler sınırları içerisinde farklılıklardan ziyade, benzer değerlerin paylaşıldığı bir alan yaratma çabasındadırlar. Bu nedenle Newman'a göre sınırlar, yalnız devletler ve coğrafî alanlar arasında değil aynı zamanda biz/onlar

ayrılıklarını meydana getiren çizgilerdir (Newman, 2006: 6). Bu işleviyle sınırlar, modern dünyada ulusal kimliği oluşturan ve koruyan araçlardır. Hatta ve hatta sınırlar, çevrelediği alan içerisinde tek kimliğin yükselmesiyle azınlıklar, diaspora, etnik çatışmalar gibi etkiler de yaratabilirler. Dolayısıyla yalnız askeri ve ekonomik bariyer işlevi olmayan sınırlar, aynı zamanda bir ülkenin içerisinde var olan dini, etnik, kültürel ve sosyal homojenliğin de teminatıdır. Bu minvâlde Ouali, sınırların, alanlar/bölgeler arasında önce mesafeleri daha sonra farklılıkları inşa ettiğini savunmaktadır (Ouali, 2006: 634). Böylelikle sınırlar, aynı alanı/bölgeyi paylaşan insan gruplarının birlik oluşturmasının, alan/bölge dışında kalanların "dışlanmasının" sebebi olacaktır.

Sınırlar, devletlerin hukuki egemenliklerinin belirtileri olarak da modern uluslararası hukukun mihenktaşını oluşturmaktadır. Modern uluslararası hukuk, devletlerin egemenliğinin, dolayısıyla sınırlarının korunmasını –en azından teoride- esas almaktadır. Bu denli öneme rağmen sınırlar uygulanan uluslararası hukukta kimi zaman tartışmalara neden olmaktadır. Bazı araştırmacılar, hukuksal açıdan geçerli olan sınırlar ile devletlerin ülkelerini bölen ancak hiçbir biçimde kabul etmedikleri ayrım çizgilerinin (demarcation-line) birbirinden farklı olduğunu savunmaktadırlar (Pazarcı, 2015: 237). Bu tip bir farklılığın söz konusu olduğunu savunan araştırmacılar olsa da, uygulanan uluslararası hukukta bunun pek kabul görmediği ve sınır kavramının her iki durumda da kullanıldığı görülmektedir. Pazarcı, hukuksal açıdan geçerli olan sınırlar ile hukuksal geçerliliği tartışmalı sınırlar arasında ayrım yapmanın daha doğru olacağını söylemektedir (Pazarcı, 2015: 237). Ona göre sınırların hukuksal açıdan geçerliliği taraf devletlerce (antlaşmalar yoluyla) veya uluslararası yargı/hakemlik organlarınca saptanabilir.

Sınırlar, devletlerin hem güvenlik hem dış politikaları açısından da oldukça önemli bir yere sahiptir. Özellikle II. Dünya Savaşı sonrası Soğuk Savaş'ın çetin ortamında jeopolitiğin önem kazanmasıyla, devletler sınırlarını politik hamlelerinin odağına yerleştirmişlerdir. Öyle ki devletler, egemenlik alanlarını belirleyen bu soyut çizgilere namus/onur gibi kutsiyetler atfetmişlerdir. Bu nedenle namuslarının/onurlarının muhafazası için sınır yönetişimine ihtiyaç duyan devletler, geçiş noktaları, pasaport kontrolleri, kontrol noktaları, vize, gümrük gibi uluslararası uygulamalar yoluyla sınırlarını somutlaştırmış, hatta kurumsallaştırmışlardır. Ayrıca mayınlı araziler, dikenli tel örgüler, yüksek duvarlar, radar sistemleri, askeri üsler gibi ulusal ve askerî güvenlik mekanizmalarıyla sınırlarının muhafaza edilmesini sağlamaktadırlar. Ancak sınırlar devletler tarafından yalnız çatışmalar ve anlaşmazlıklar özelinde

değerlendirilmemektedir. Prescott'un ifadesiyle devletler arası fiziksel temas hattını temsil eden sınırlar, anlaşmazlıkların olduğu kadar işbirliğinin de tetikleyicisidir (Prescott, 1987: 5). Küresel dünyada siyasi ve ekonomik bağların yani işbirliğinin artması, yine bu bağların önemini kapsayan sınır-aşan/sınır-ötesi kavramını ortaya çıkarmıştır. İronik bir biçimde, bir yandan devletlerin güvenlik kaygıları nedeniyle giderek opaklaşan sınırlar, diğer yandan siyasi, ekonomik, askeri konulardaki işbirliğinin maliyetleri azaltan dayanılmaz cazibesi neticesinde şeffaflaşmıştır.

Öte yandan küreselleşmenin etkisiyle devlet ülkeleri (territory) arasındaki mesafeler daralmakta, yavaş yavaş aşınmaya yüz tutan sınırlar sorgulanmaya başlamaktadır. Aynı zamanda küreselleşme, uluslararası politikada "aktör enflasyonu" yaratarak ulus-devletin otoritesinin sarsılmasına neden olmaktadır. Bu durum uluslararası örgütler (hükümetlerarası/hükümet-dışı), çok-uluslu şirketler, küresel terör örgütleri gibi yeni aktörlerin doğmasına ve yükselmesine zemin hazırlamıştır. Tüm bunlar alt alta toplandığında küreselleşme, Uluslararası İlişkiler'de ulus-devlet ve uzuvlarının sorgulandığı büyük tartışmalar yaratmaktadır. Tartışmaların boyutu disiplinin geleceği, hatta isminin değişmesi gerektiği tezine kadar uzamaktadır. Küreselleşmenin sınırları ortadan kaldırdığını, dolayısıyla ulus devletlerin sonu olduğunu savunan akademisyenler, "Uluslararası İlişkiler" (International Relations) yerine "Küresel İlişkiler" (Global Affairs) formülünü sunmaktadırlar (Barnett ve Sikkink, 2011).

Ne var ki küreselleşme bilişim ve iletişim teknolojilerindeki gelişmeler, toplumlar ve kültürler arasındaki uzaklıkların azalması, hayat standardının yükselmesi gibi olumlu etkilerinin yanında, uluslararası terörizm, göç/mülteci ve sınır-aşan suçlar gibi olumsuzlukları da beraberinde getirmektedir. Bu tür tehditlerin yükselmesi, hâliyle devletlerin de "Ortaçağ burg"larını yeniden yükseltmelerine neden olmaktadır. Özellikle 11 Eylül saldırıları, Arap Baharı ve bunlara mukabil uluslararası terörizmin yarattığı travmalar vb. hadiseler ile birlikte devletin sınırlarının güvenliği, insan hak ve özgürlükleri karşısında ağır basmaktadır. Bilgi ve iletişim teknolojisinde yaşanan büyük gelişmelerle etkisini gösteren küreselleşme ise, bireye vaat ettiği uçsuz bucaksız özgürlükler ile öne geçmeye çalışmaktadır. Kısacası bir köşede internetin doğuşuyla beraber sınır ve mesafe tanımaksızın ilerleyen küreselleşme, diğer köşede tehditlerin boyut kazanmasından ötürü sınırlarına "yığınak" yapan ulus devlet oturmaktadır. Ortaya çıkan bu ikili vaziyet, Uluslararası İlişkiler disiplininde yeni bir paradoksun yaşanmasına sebep olmaktadır.

Siber Uzay: Uluslararası İlişkilerde Sınırlar Olgusunun Değişimi ve Dönüşümü

20. yüzyılın ikinci yarısı itibariyle ortaya çıkan küreselleşmenin en önemli çıktılarından biri, hiç şüphesiz bilgi ve iletişim teknolojilerinde (BİT) meydana gelen gelişmeler olmuştur. Bilgisayar teknolojisi/bilişim sistemlerinde yaşanan büyük atılımlar, internetin yaygınlaşması ve dolayısıyla dijitalleşmenin hız kazanması gibi faktörler insanlığı "siber uzay" (cyberspace) adı verilen yeni bir alanla tanıştırmıştır. Siber uzay, günümüzde pek çok kez sanal gerçeklik (virtual reality) ile bağdaşlaştırılmaktadır. Sanılanın aksine, sanal gerçeklik bilgisayar teknolojileri ile şekillendirilen soyut bir ortama refere etmekteyken, "siber uzay" genel bir biçimde fiziksel ya da sanal farketmeksizin dijital olan her şeye tekabül etmektedir. Genellenebilirliğinden de anlaşılacağı üzere, siber uzay kavramı "elle tutulur, gözle görülür" bir tanımdan yoksundur. Örneğin Lawrence Lessig siber uzayı, insanların yaşadığı ve gerçek hayatta yaşadıkları şeyleri deneyimleyebildikleri bir yer (place) olarak tanımlarken (Lessig, 1996: 1403), Wolff Heintschel von Heinegg ise gizemli özellikleri nedeniyle, siberi "beşinci boyut" (fifth dimension) olarak tanımlayabilmektedir (Heinegg, 2013: 123). Tanımlan(-ama)ması sorununun yanında, son derece kompleks ve çok boyutlu bir yapıya sahip olan siber uzay, 30 yıl öncesinin dünyasında devrim etkisi yaratmıştır. Başlangıçta teknik boyutuyla ön plana çıkan kavramın zamanla sosyal, ekonomik ve siyasal birtakım boyutları da ortaya çıkmıştır. Bu bakımdan peyderpey bireyleri, toplumları, devletleri ve nihayet uluslararası ilişkileri etkilemiştir.

Dijital her şeyin alt yapısını oluşturan siber uzay, bulut teknolojisi, nesnelerin interneti (IoTs), yapay zeka (Artificial Intelligence), büyük veri (Big Data) gibi getirileriyle günlük hayatta büyük kolaylıklar sağlamaktadır. Diğer yandan hukuk, sınır, mesafe tanımaz niteliği ve buna mukabil güvenlik tehditlerinin baş göstermesi devletlerin bu alana ilgi göstermelerinin fitilini ateşlemiştir. *Res communis* (herkese ait olan) yahut *res nullius* (hiç kimseye ait olmayan) bir yapıya sahip olan siber uzayın "kontrol edilemez" mottosu, bir yandan devletlerin karşılıklı bağımlılık ilkesine göre işbirliği yapmalarına, bir yandan da ulusal güvenliklerini sağlamaya yönelik politikalar üretmelerine sebep olmuştur. Ayrıca anarşik doğasından ötürü siber uzay, ulus devletlerin yatay yapılandığı anarşik uluslararası sistemi hatırlatmaktadır. Uluslararası İlişkilerde Realist teorisyenleri haklı çıkarır şekilde, anarşik uluslararası sistemde kendi başının çaresine bakıp *(self-help)* hayatta kalmayı *(survival)* hedefleyen –yani egemenliklerini sürdürmek isteyen- devletler bu amaçlarını siber uzaya da uyarlamışlardır. Ne var ki devletler

bu kez siber ortamın fiziksel mekandan (territory) ve sınırlardan (borders) muaf *sui generis* yapısıyla baş başa kalmıştır.

Siber uzay, ulus devletlerin egemenliğinin sürdürülebilirliği açısından oldukça karmaşık bir ortamdır. Siber uzayın devlet-merkezli değil çok-merkezli (anarşik) olması; yalnız devletler değil bireyler, uluslararası örgütler, terör örgütleri, çok-uluslu şirketler gibi aktörlere etki ve barınma imkânı sunması; uluslararası sınırları aşındırması ve bu sayede Westphalian ülkesellik ilkesini tehdit etmesi; konvansiyonel güvenlik ve savunma araçlarını etkisiz hale getirmesi; yönetişimi sorunu gibi etkenler devlet egemenliğini çıkmaza sürüklemektedir (Akyeşilmen, 2018: 180). Konuya temas eden Bellanger, devlet egemenliği ile siber uzay arasındaki ilişkiyi ele almış, devletleri "mekân/bölge/ülke"yle özdeşleştirerek egemenliğin yalnızca sınırları belli bir mekânda varlığını sürdürebileceğini belirtmiştir (Bellanger, 2011:3).

Egemenliğin varlığını oldukça katı bir kurala bağlayan Bellanger'e göre siber uzayda egemenliğin tesisi imkansızdır. Hao Yeli ise, egemenlik ile siberin ruhu arasındaki çelişkiye dikkat çekmiştir. Yeli'ye göre, devlet egemenliğinin münhasırlığı, sınırsız bağlantılara dayalı siberin ruhuna aykırıdır (Yeli, 2017: 110). Öte yandan uluslararası sistemde hâlâ başat aktör olan devletin –bireyin bile devlete meydan okuyabildiği- siber uzayda bu otoritesinin sarsıldığı açıktır. Uluslararası sistemde görece hegemonya sahibi devletler, siber uzayda güçlü ya da güçsüz diğer aktörlere tanınan manevra alanı sayesinde sınırlandırılmaktadır. Bu durum karşısında devletler egemenliklerine yönelik büyük tehditler algılamaktadır. Başka bir deyişle siber ortamın, bireyi meşru kuvvet kullanma tekeline sahip devletin kontrolünden kurtarıp, aktörler arasında denklik kurması egemenliğin ihlali olarak yorumlanmaktadır (Grosso, 2001). Geleneksel açıdan ulusal güvenlik, dışarıdan gelebilecek tehdide karşı devletin sınırlarını koruması ve tedbirler almasını öngörmektedir. 21. yüzyılın başıyla birlikte ise geleneğin sorgulanmasına yol açan gelişme, siber uzayda bilgi ve iletişim ağları arasında vuku bulan sınırsız eylemlerdir. Böylece daha önce bir devleti yine başka bir devletin tehdit edebildiği klasik güvenlik anlayışı boyut değiştirerek farklı aktörlerin zemin kazanmasına yol açmıştır (Weimann, 2006: 154). Siber, çeşitli aktörlerin modern devletin sınırlarını çiğneyebildiği ve ülke topraklarını tehdit edebilen karakteristiği nedeniyle devletler için güvensizlik ortamı yaratmıştır. Siber alanın post-modern tehditlere gebe niteliği, devletlere, egemenliklerinin ve bununla bağlantılı olarak sınırlarının/topraklarının istikrarı için spesifik ulusal güvenlik stratejeleri geliştirmelerini zorunlu kılmaktadır.

Dijital çağda bilginin ve teknolojinin son derece hızlı akışı, devletleri bu konuda sonucunu öngöremediği birtakım problemlerle karşı karşıya getirmektedir. Bunlar devletlerin kara, deniz ve hava kuvvetleri eliyle, yani konvansiyonel yöntemlerle baş edemediği türden problemlerdir. Böylesine kaotik bir ortamda, devletlerin sınırlarına ve dolayısıyla ülke bütünlüklerine kolayca kast edebilen tehditlerin, klasik tehdit unsurlarından bazı farklılıklar arz ettiği görülmektedir. Bu farklılıklardan ilki ve belki de en önemlisi, tehdidin kim tarafından gerçekleştirildiğinin tespit edil(-eme)mesidir. Siber uzay, devletlerden uluslararası örgütlere, terör örgütlerinden bireylere kadar uluslararası ilişkilerdeki tüm aktörlere "anonimlik" imkânı sunmaktadır. Daha doğru bir ifadeyle siber ortam, casusluk, terör, hırsızlık gibi eylemleri icra eden fâillerin kimliğinin belirlenmesi noktasında problem oluşturmaktadır (Placid ve Wynekoop, 2011). Çünkü siber alanın çok-merkezli yani anarşik doğası, aktörün kimliğini gizleyebilme yetisi, uluslararası ilişkilerde güçlü devletlere nazaran çok daha etkisiz olan aktörlerin önemli bir oyuncu haline gelmesine imkan tanımaktadır. Normal şartlar altında etki kapasitesi sınırlı olan bu aktörler, manipülasyon, propaganda, siber suç ve siber terör gibi yollara başvurarak siberin "nimetlerinden" yararlanmaktadır. Siber uzayın anonimlik sayesinde çeşitli suçları fâillere kolay kılan yapısı, hâli hazırda küreselleşmeyle otoritesi sarsılmış devletler için daha büyük bir meydan okumadır. Uluslararası İlişkiler'in biricik aktörü konumundaki devletlerin bile bazen çaresiz kalması tehdidin vahametini gözler önüne sermektedir. Bu sayede siber uzay, sınırlarını "gözü gibi koruyan" devletlerin çok daha kolay bir şekilde geçilmesinin önünü açmaktadır. Bu durum güçlü ya da güçsüz tüm dünya devletleri için kaygı verici olup, pratik ortam bunun örnekleriyle doludur.

Örneğin 2003 yılında Amerika Birleşik Devletleri'nde orduya yönelik yapılan "Titan Rain" adlı bir saldırı gerçekleşmiştir. ABD, saldırının arkasında kimin olduğu bilinmese de, Çin Halk Cumhuriyeti'ni suçlamıştır. Dünyanın son yıllarda en çok siber saldırıya maruz kalan ülkelerinden Ukrayna, 2017 yılında adı önce "PETYA" daha sonra "PETRWRAP" olan bir fidye yazılımdan etkilenmiştir. Saldırı, Ukrayna Merkez Bankası, devlete ait enerji dağıtım şirketi Ukrenergo, uçak üreticisi Antonov, Kiev'de bulunan Boryspil Havaalanı ve ülkede faaliyet gösteren iki posta servis sağlayacısının etkilenmesiyle sonuçlanmıştır (https://www.bbc.com/turkce, 8 Aralık 2018'de erişildi). Ukraynalı yetkililer saldırının arkasında Rusya olduğunu iddia etse de olay netliğe kavuşmamıştır. Etkisi küresel çapta hissedilen saldırıyı hisseden ülkeler arasında İngiltere, İspanya ve Danimarka da bulunmaktadır. Yine 2017 yılında yapılan büyük siber saldırılardan bir diğeri olan

"WannaCry" virüsü, Türkiye ve Rusya dahil yüzü aşkın ülkeyi etkilemesi bakımından önemlidir. Saldırının arka planında Amerikan istihbarat servislerinin olduğu iddia edilse de, kesin bir yargıya varılamamıştır. Görüldüğü üzere kimliği belirsiz (anonim) şekilde düzenlenen siber saldırılar, tek devletin sınırlarını ihlâl etmenin ötesine geçerek aynı anda birçok devletin sınırlarını çiğnemiştir.

Siber uzayda devletlerin egemenliklerini dolayısıyla sınırlarını tehdit eden bir diğer problem de, tehditlerin niteliği noktasında ortaya çıkmaktadır. Siber tehditler kara, deniz, hava ve uzay gibi fiziksel ortamların tehditlerinden bağımsız, sanal alanda da etkili olması nedeniyle epey farklılıklar arz etmektedir. Daha önce de değinildiği üzere, Realist Uluslararası İlişkiler'in geleneksel güvenlik anlayışında, bir devlet için tehdit kabul edilebilecek tek bir unsur vardır: O unsur yine başka bir devlettir. Ancak her şeyden önce bu yeni ortam, devlet dışı aktörlere geniş hareket alanı sağlaması ve bunların devletlerin güvenliği için tehdit oluşturması bakımından geleneğin dışına taşmıştır. Siber saldırıların marjinal niteliği, Uluslararası İlişkiler disiplininde çatışma ve savaş gibi güvenlikle özdeşleşen terimleri bile yapısökümüne uğratmıştır. Yaklaşık 30 yıl önce devlet bir yana, bireyleri dahi tehdit etmenin ciddi bir mali yükü bulunmaktaydı. Fakat siberin getirmiş olduğu ucuzluklar ve kolaylıklar, fâillerin devletler karşısında bile "tek bir bilgisayar"la meydan okumasının önünü açmıştır. Bazen sadece küçük bir yazılımın bazen de flash belleklerin kullanılması, geleneksel "savaş", "çatışma" ve "kuvvet kullanımı" kavramlarının içini boşaltmıştır. Ayrıca siberin cephe ve cephe gerisi gibi fizikî mekânlara gerek duymayan özelliği, bir adım öteye giderek, icrâ edilen saldırıların çoğu zaman başka yerlerden yapılıyor izlenimi vermesine imkân sağlamaktadır. Tüm bunlar alt alta toplandığında siber saldırılar, literatürde "barutsuz/silahsız/soyut savaş" olarak tanımlanmaya başlamıştır.

Siber alanın "kanlı savaşları" (https://www.timeturk.com, 8 Aralık 2018'de erişildi) olarak da adlandırılan, devletlerin sınır güvenliğini doğrudan tehdit eden saldırıların belki de en iyi üç örneği Estonya, İran ve Gürcistan saldırılarıdır. İlk örneğine 1999 yılında Kosova Savaşı'nda rastlanan bu saldırılar, 2000'lerde birbirini peşi sıra takip etmiştir. 26 Haziran 2007 akşamı, yalnızca birkaç saat içinde Estonya'nın önde gelen bankalarının, gazetelerinin, hükümetin, siyasal partilerin web sayfaları çökertilmiştir. "First Web War" olarak ifade edilen, büyük yankı uyandıran Estonya saldırısı, dünyanın en köklü askerî örgütü olan NATO'nun siber alandaki politikalarını yeniden gözden geçirmesine yol açmıştır. Saldırıların Rusya tarafından yapıldığı öne sürülse de elle tutulur bir kanıt sunulamamıştır. Benzer bir durum 7 Ağustos

2008'de başlayan Rusya ve Gürcistan arasındaki Güney Osetya Savaşı'nda da yaşanmıştır. Topların ve tüfeklerin konuştuğu bu savaşın fiziksel boyutun yanında Rusya savaşı sanal boyuta taşıyarak Gürcistan'a ait çok sayıda resmi internet sitelerini çökertmiştir. Saldırıların arkasında bulunan Rusya'nın, farklı ülkelerdeki bilgisayarları kullanarak eylemi gerçekleştirmesi, siberin devlet sınırlarını tanımaz doğasını anlamak açısından önemlidir. Bu iki örnekten biraz daha farklı olarak, Haziran 2010'da İran'daki nükleer tesisler hedef alınmıştır. STUXNET adı verilen solucan yazılım (mallware) ile birileri, flash bellek yoluyla temelde İran'ı nükleer alanda sınırlandırmayı hedeflemekteydi. İran, saldırıların Amerika Birleşik Devletleri ve İsrail tarafından tertip edildiğini iddia etmektedir. Neticede uluslararası hukukun temelini görece sağlam attığı fiziksel ortamda henüz tam olarak çözülmeyen sınırların, siber uzayın sınır tanımaz sloganı karşısında adeta eridiği söylenebilir.

Siber uzayın, Westphalian ulus devlet ve onun yapıtaşlarını oluşturan egemenlik, sınırlar ve ülkeselliği bir çırpıda silebilen özelliği karşısında, çözülmeye mahkum olan bir diğer kavram uluslararası hukuktur. Johnson ve Post, mekandan bağımsız ve sınırsız karakterinden dolayı, mevcut egemenlik ve hukuk kavramlarının siber alana uygulamasının imkansız olduğunu vurgulamışlardır (Johnson ve Post, 1996: 1367). Onlara göre devletler siber alan için farklı yasalar geliştirmelidir. Siberin devlet-merkezli değil bilâkis çok-merkezli doğası itibariyle Johnson ve Post'a hak vermemek elde değildir. Çünkü siber saldırılarda fâilin kimliğinin belirlenmesinde yaşanan güçlükler, dijital tehdidin niteliğinin fiziksel tehdidinkinden çok daha farklı olması, aktörlere sonu olmayan özgürlükler tanıması gibi etkenler meselenin hukukî boyutunda açmaza yol açmaktadır. Diğer taraftan bilgi ve teknolojiye erişimin günden güne hız kazanmasıyla siber suçlarda da akıl almaz bir biçimde artış yaşanmaktadır. Günümüzde son derece yaygın olan dijital casusluk, terör gibi faktörler göz önünde bulundurulduğunda siber ortam, bireyden devlete kadar tüm aktörler için tehdit teşkil etmektedir. Nitekim meselenin güvenlik boyutu akıllara Westphalian uluslararası hukukun, siber uzaya uyarlanıp uyarlanamayacağı sorusunu getirmektedir. Kaldı ki bu konuda devletlerin kendi sınırları çerçevesinde uyguladığı hukuk (iç hukuk) dahi yetersiz kalırken, uluslararası ölçekte fâillerin tespiti ve yargılanması noktasında çok daha fazla sorun yaşanacaktır.

Egemenlik en nihâyetinde devlete, sınırları içerisinde yasal düzenlemeler yapma yetkisini de vermektedir. Devletler egemenlikleri karşısında giderek etksini daha çok hissettiren bilişim suçlarına yönelik yasal tedbirler almaktadır. Türkiye'de bilişim suçlarına yönelik en geniş

düzenlemeler 5237 sayılı Türk Ceza Kanununda yer almaktadır (http://internet.btk.gov.tr). Türk Ceza Kanununun 243, 244 ve 245. maddeleri siber kaynaklı saldırılar için düzenlenmiştir. Elbette siber saldırılardan etkilenen tek aktör devletler değildir. Bunun için, Kuzey Atlantik Paktı Örgütü (NATO), Birleşmiş Milletler (BM), Avrupa Birliği (AB) gibi bölgesel ya da küresel örgütler de siber güvenlikleri hususunda ciddi adımlar atmaktadır. Örneğin, internet ve bilgisayar ağları aracılığıyla işlenen suçlara ilişkin ilk uluslararası sözleşme 2001 yılında Budapeşte'de imzalanan Avrupa Konseyi Siber Suçlar Sözleşmesi'dir (https://www.tbmm.gov.tr, 10 Aralık 2018'de erişildi). Bunu takip eden dönemde AB, sınırları içerisinde siber güvenliğini geliştirmek için her türlü teşvik ve girişimi desteklediği platform olan Avrupa Siber Güvenlik Örgütü'nü (ESCO) kurmuştur. AB ayrıca, üye devletlerin sınırlarının güvenliğini sağlamaya yönelik oluşturduğu birim olan Avrupa Sınır ve Sahil Koruma Ajansı (FRONTEX) ile, siber kaynaklı saldırıları gündemine almaktadır.

Bir diğer örnek olan NATO, özellikle 2007 yılında Estonya ve 2008 yılında Gürcistan'a yönelik saldırılarından sonra siber alana önem vermiş, bu hususta görüşlerini şöyle belirtmiştir;

> *Siber alandaki en tehlikeli oyuncular hâlâ ulus devletlerdir. Organize suç ağlarının saldırı yetenekleri giderek artmaktadır ve bunlar gelecekte teröristler gibi devlet dışı oyuncular tarafından kullanılabilirler. Ancak siber etki alanında hayli gelişmiş casusluk ve sabotaj için hala bir ulus devletin yetenek, kararlılık ve maliyet-yarar rasyoneline ihtiyacı vardır…Daha henüz fiziksel zarar ve gerçek kinetik siber terörizm gerçekleşmedi. Ancak siber saldırılarda kullanılan teknoloji artık sadece can sıkıcı bir sorun olmaktan çıkıp bilgi güvenliğine ve hatta kritik ulusal alt yapıya yönelik ciddi bir tehdit haline gelmektedir.*(https://www.nato.int)

Bu bildiriyle siber uzaydan kaynaklanan tehditlere dikkat çeken NATO'nun, üye devletlerinin egemenliklerini korumak üzere hazırladığı "Siber Savunma Politikası", Ocak 2008'de yürürlüğe girmiştir. Örgüt ayrıca düzenli aralıklarla "Cyber Coalition", "Locked Shields" gibi adlar verdiği büyük rağbet gören güvenlik tatbikatları düzenlemektedir (https://ccdcoe.org). BM ise, internet suçlarına yönelik 1994 yılında bir el kitabı yayımlamış, 2000 yılında dijital teknolojinin kötüye kullanılmasının önlenmesi hususunda Genel Kurul kararı almış, 2011 yılı itibariyle de siber suçların ele alındığı Hükümetlerarası Uzmanlar Grubu'nu oluşturmuştur (Önok, 2013: 1239).

Siber uzayda gerçekleştirilen eylemlerin problem doğuran bir başka özelliği, daha önce de değinildiği üzere, kuvvet kullanımı (use of force) gibi geleneksel güvenlik kavramlara meydan okumasıdır. Geleneksel güvenlik anlayışı, eylemlerin (kuvvet kullanımının) kara, deniz, hava, uzay gibi fiziksel ortamlarda boy gösterebilirliğine dayanmaktadır. Geleneksel uluslararası hukuk, kuvvet kullanımı gibi eylemlerin devletlerin ikili ya da çok taraflı antlaşmalar, paktlar, sözleşmeler yoluyla yasaklanabileceğini öngörmektedir. Teoride bu şekilde ele alınan mesele tarihsel pratikte de aynı şekilde gerçekleşmiştir. Uygulanan uluslararası hukukta kuvvet kullanımı yasağının tarihsel ilk örneği 1925 yılında Almanya, İngiltere, Fransa, Belçika ve İtalya tarafından imzalanan Ren Misakı'dır (Pazarcı, 2015: 517) Ren Misakı'nı, 1928'de Türkiye dahil birçok devleti bir araya getirerek imzalanan Briand-Kellogg Paktı izlemiştir. Ancak Uluslararası İlişkilerde kuvvet kullanımının evrensel bir ilke olarak kabul edildiği ilk antlaşma BM Antlaşması'dır (Pazarcı, 2015: 517). BM Antlaşması madde 2/4'te açık bir şekilde kuvvet kullanma yasağını ilân etmektedir. "Tüm üyeler, uluslararası ilişkilerinde gerek herhangi bir başka devletin toprak bütünlüğüne ya da siyasal bağımsızlığına karşı, gerek Birleşmiş Milletler'in Amaçları ile bağdaşmayacak herhangi bir biçimde kuvvet kullanma tehdidine ya da kuvvet kullanılmasına başvurmaktan kaçınırlar". (https://www.ombudsman.gov.tr, 12 Aralık 2018'de erişildi). Ancak BM antlaşması'nın bahse konu olan maddesinde, kuvvet kullanımının kapsamına ilişkin belli başlı sorunlar ortaya çıkmaktadır. İlgili maddede, kuvvet kullanma yasağı, genelde "askeri" -silahlı kuvvetler eliyle düzenlenmiş- eylemleri kapsamaktadır. Ancak siber uzay, saldırganlara "top, tüfek ya da tanka" ihtiyaç duyulmadan, devletlerin toprak bütünlüğüne ve siyasal egemenliklerine karşı eylemler yapabilmeyi bahşetmektedir.

Öte yandan bir diğer sorun BM Antlaşması'nın 51. maddesi ile ilgili ortaya çıkmaktadır. Devletlerin kuvvet kullanımına maruz kalması durumunda "meşru müdafaa" ilkesini öne çıkaran 51. maddede, yine devletlerin kendilerini savunma haklarına ve bunun hangi koşullarda meşru kılınacağına değinilmektedir;

> *Bu Antlaşma'nın hiçbir hükmü, Birleşmiş Milletler 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. Üyelerin bu meşru savunma hakkını kullanırken aldıkları önlemler hemen Güvenlik Konseyi'ne bildirilir ve Konsey'in işbu Antlaşma gereğince uluslararası barış ve güvenliğin korunması ya da yeniden*

kurulması için gerekli göreceği biçimde her an hareket etme yetki ve görevini hiçbir biçimde etkilemez. (https://www.ombudsman.gov.tr, 12 Aralık 18'te erişildi).

51. madde, saldırının (yani kuvvet kullanımının) niteliğini silahlı unsurlara dayandırması bakımından 2/4. maddenin kapsamını da daraltmaktadır. Hâliyle bu durum, siber saldırıya maruz kalan devletlerin kullanacakları meşru müdafaa haklarının yöntemi ve ölçüsünde bilinmezliklere yol açmaktadır.

Neticede, özelde BM Antlaşması'nın bahse konu olan maddelerinin -genelde uygulanan uluslararası hukuk ilkelerinin -siber uzayda işlevsiz kaldığı görülmektedir. Ne var ki, gerek Türkiye örneğinde gerekse NATO ve BM örneğinde olduğu gibi, ulusal ve uluslararası düzeyde yasal düzenlemeler ve önlemlere rağmen, siber uzay henüz tam bir hukuksal çerçeveye bağlanamamıştır. Özetle siber uzayın eylemi icrâ eden kişi ya da grupların tespit edilemezliği (anonimlik), eylemin geleneksel güvenlik anlayışındaki eylemlerden çok daha farklı niteliği, ulusal ya da uluslararası hukukun kural/kaidelerini tanımaz karakteri, devletlerin egemenliğini ve dolayısıyla sınırlarının "geçilmesine" müsâde eden doğası, Westphalian ulus devlet için eşi benzeri görülmemiş bir meydan okumadır.

Sonuç

21. yüzyılın dünyasında küreselleşme, modern ulus devlet karşısında belki de en ciddi kozunu oynamaktadır. Yaklaşık 30 yıl önce doğan internet ve buna bağlı olarak ivme kazanan dijital teknolojiler, "siber uzay" adı verilen yeni-marjinal bir uzay yaratmıştır. Bu yeni kavram, devlet egemenliğini doğrudan hedef alan mekân/hukuk/sınır tanımayan, küreselleşmenin aşındırdığı sınırların tamamen çözülmesi misyonuyla yola çıkmıştır. Modern ulus devlet, tıpkı anarşik uluslararası sistemde olduğu gibi, "daha anarşik" siber uzayda da kendi başının çaresine bakmak zorundadır. Önce Kosova'da, daha sonra sırasıyla Estonya, Gürcistan ve İran'da siber alanda yürütülen saldırılar, devletlere sınırlarının ve vatandaşlarının güvenliği hususunda harekete geçmeleri için verilen alarmlardır. Siber uzayda her türlü resmi kaynaklarının muhafaza edilmesinden ötürü bir anlamda rahatsızlık duyan devletler, sınırlarından içeri rahatça sızabilecek potansiyel tehditlerin önüne setler inşa etmeyi amaçlamaktadır. Hali hazırda varlığını gösteren bu unsurların varlığı dolayısıyla devletler, siber uzayı politik hedeflerinin merkezine koymaktadır. Siber uzayın devletler nezdinde bu denli önemi, çok-merkezli (anarşik) doğasının devlet-merkezli uluslararası sistemi ikame ediyor olmasıdır. Bu durum doğal olarak 2000'ler öncesinin alçak politika (low politics)

alanının, yüksek politika (high politics) alanına evrilmesine yol açmıştır. Başka bir deyişle önceleri "low politics" olarak nitelendirilen siber uzayın, "high politics" olan devlet sınırlarını tehdit edebiliyor oluşu, devletlerin bugün doğal olarak siber uzayı "high politics" kategorisine sokmalarına neden olmuştur.

Günümüzde pek çok ülkede, pek çok dilde namus ve mahremiyetle bağdaşlaştırılan sınırlar, siber uzayın vermiş olduğu imkanlar vesilesiyle rahatça çiğnenebilmektedir. Bu sayede siber uzay çeşitli aktörlere, modern ulus devletin "hazine dairesi", yani en değerli şeyi olan sınırlarından içeri girme fırsatı vermektedir. Devletlerin karşısına hergün başka bir boyutla dikilen tehditler, Westphalian sınırları siber uzayda örmekten başka çare bırakmamaktadır. Siber uzayda haliyle pasaport kontrol noktası, mayınlı araziler, dikenli tel örgüler, radar sistemleri oluşturamayacak devletlerin bu hayalinin boş olduğu açıktır. Görünüşe göre devletlerin oldukça karmaşık ortama yönelik, ulusal düzeyde güvenlik strateji belgeleri hazırlamaktan ve siber uzayda kendilerini geliştirmekten, uluslararası düzeyde ise karşılıklı işbirliğine gitmekten başka çareleri yoktur.

Öte yandan siber alan, bu ortamda sınırlarını muhafaza etmek için eksik de olsa Westphalian model inşa etme idealinde olan devletlere kapılarını sımsıkı kapatmıştır. Bir kere, devletlerin arzuladığı Westphalian model, devletlerin egemen eşitliği ve birbirlerin içişlerine karışmama ilkelerine dayalı, uluslararası hukukun kurallarıyla çevrili uluslararası sistem yaratmıştır. Fakat egemenliğin, sınırların, devlet ülkesinin, normlar ve değerler temelli uluslararası hukukun, devlet-merkezli uluslararası sistemin esamesinin okunmadığı siber uzayda Westphalian model içi boş bir hayalden ibaret gözükmektedir. Daha net bir ifadeyle, devletle ilgili modern olan her şeyin –yani modern uluslararası ilişkilerin- miladı olan Westphalian modelin, siber uzayda şuan için "hiç"ten ibaret olması, ulus devleti, birey gibi aktörlerle hiyerarşik açıdan eşit konuma getirmektedir.

Pre-Westphalian dönemin "devletin devletin kurdu olduğu" güvensizlik ortamını andıran siber uzay, tıpkı 370 yıl önce olduğu gibi ulus devletlere, bu kez bilgi ve iletişim teknolojilerinde devrim yapmaktan öte çare bırakmamaktadır. Yakın gelecekte devletin ülkesini ve sınırları siber uzaya taşıyıp taşıyamayacağı muammadır. Yine de, bugün için mümkün gözükmese de, devletlerin sınırlarını çizdiği ve bu sınırların dijital bölgeler yarattığı olası "Siber-Westphalia" süreci heyecan uyandırmaktadır (Demchak ve Dombrowski, 2011: 57). "Uluslararası siber hukuk"un tamtakır uygulanabildiği, devletin egemenliğinin tesis edilip korunduğu bu ortam,

şüphesiz casusluk ve terörizmden kaynaklı saldırıların sekteye uğramasına neden olacaktır. Siber-Westphalia, adından da anlaşıldığı üzere, devletlere dijital sınırlar çizerek, bahsi geçen sınır tanımaz tehditlerin manevra alanını kısıtlayacaktır. Aynı fiziksel sınırları içerisinde yasal düzenlemeler yapabilen devlete, Siber-Westphalia'da yasa yapmak, suçluları yargılama imkanı sunacaktır. Bu sayede hem devletler, hem de bireyler, uluslararası örgütler, çok-uluslu şirketler gibi diğer aktörler için daha güvenilir ve yaşanabilir bir alan yaratılmış olacaktır.

Yukarıda bahsi geçen kehânetlerin şuan için devletler nezdinde bir "ütopya"dan ibaret olduğu açıktır. Tam tersine, bugünün dünyasında siber uzay devletlere genellikle "distopya"yı andırmaktadır. Siber uzayın sadece "kontrol edilemezlik" mottosu üzerine kurulması bile, sınırlar içerisinde kontrol etme alışkanlığına sahip devletlerin çabalarını boşa çıkarmaktadır. Bir yandan da siberin hukuksal çerçeveye sığdırılamayacak kadar geniş kapsamı, faili yargılamak bir yana, kimliğinin belirlenmesinde dahi güçlükler çıkarmaktadır. Henüz Siber-Westphalia gayesinden oldukça uzak olan ve bir aşama kaydedememiş devletler ancak işbirliğine gidebilmekte ve birtakım sınırlı tedbirler almaktadır. Devletler gerek uluslararası örgütlerde gerek ikili görüşmelerinde muhakkak siber uzaya da yer ayırmaktadır. Her defasında siber ortamın bir bütün olarak uluslararası rejimlerce yönetilmesi ve düzenlenmesi noktasında ağız birliği yapılmaktadır. Ulusal düzeyde yavaş yavaş ipleri eline almaya başlayan devletlerin, gelecekte uluslararası düzeyde kontrol mekanizmaları kurması olasıdır. Siber-Westphalia'dan ancak böyle bir ortamda söz etmek doğru olacaktır. Nitekim, belki de tarih tekerrür edecek ve 24 Ekim 1648'de Avrupalı diplomat ve prenslerin yaptığını, geleceğin devlet adamları başaracaktır.

Kaynakça

Adams, J. Albakajai, M. (2016). Cyberspace: A New Threat to the Sovereignty of the State. *Management Studies*. *4* (6). 256-265.

Agnew, J. (1994). The Territorial Trap: The Geographical Assumptions of International Relations Theory. *Review of International Political Economy*. 1. 53–80.

Akyeşilmen, N. (2018). *Disiplinlerarası Bir Yaklaşımla Siber Politika ve Siber Güvenlik*. Ankara: Orion Kitabevi.

Ancel, J. (1938). *Les Frontieres*. Paris: Armand Colin.

Anderson M. (1996). *Frontiers: Territory and State Formation in the Modern World*. Oxford: Polity Press.

Aufricht, H. (1944). On Relative Sovereignty. *Cornell Law Review*. *30* (2). 137-159.

Barnett, M. N. ve Sikkink, K. (2009). From International Relations to Global Society. Robert E. Godin (ed.).*The Oxford Handbook of Political Science*. Oxford: Oxford University Press.

border regions." Journal of Borderland Studies 15 (1): 57-83.

Borders and Boundaries - Geography - Oxford Bibliographies. 5 Aralık 2018'de erişildi. http://www.oxfordbibliographies.com/view/document/obo-9780199874002/obo-9780199874002-0056.xml

Bottomore, T. B. (1987). *Elites and Society*. London: Routledge.

Brunet-Jailly, E. (2005). Theorizing Borders: An Interdisciplinary Perspective. *Geopolitics*. 10. 633–649.

Brunet-Jailly, E. (2005). Understanding Borders: A Model of Border Studies. *Geopolitics*. *10* (4). 633-649.

Choucri, N. (2012). *Cyberpolitics in International Relations*. Cambridge: The MIT Press.

Cox, L. (2004). Border Lines: Globalisation, De-territorialisation and the Reconfiguring of National Boundaries. In M. Fine, N. Smith, & A. Wise (Eds.) Mobile Boundaries/Rigid Worlds: Proceedings of the 2nd Annual Conference of the Centre for Research on Social Inclusion Sydney: Centre for Research on Social Inclusion, Macquarie University.

Czosseck, C. ve Geers, K. (2009). *The Virtual Battlefield: Perspectives on Cyber Warfare*. Amsterdam: IOS Press BV.

David, N. ve Paasi, A. (1998). Fences and Neighbours in the Postmodern World: Boundary Narratives in Political Geography. *Progress in Human Geography*. 22. 186-207.

Delanty, G. ve Rumford, C. (2005). *Rethinking Europe: Social Theory and the Implications of Europeanization*. New York: Routledge.

Demchak, C. C. ve Dombrowski, P. (2011). Rise of a Cybered Westphalian Age, *Strategic Studies Quarterly*. 32-61.

Finklea, K. M. (2013). The Interplay of Borders, Turf, Cyberspace, and Jurisdiction: Issues Confronting U.S. Law Enforcement. *Congressional Research Service*. 1-27.

Gibson, W. (1984). *Neuromancer*. New York: Ace Books.

Gibson, W. (1987). *Burning Chrome*. New York: Ace Books.

Giddens, A. (1987). *A Contemporary Critique of Historical Materialism: The Nation-State and Violence*, Berkeley: University of California Press.

Giddens, A. (1998). *The Consequences of Modernity*. Cambridge: Polity Press.

Gilpin, R. (1981). *War and Change in World Politics*. Cambridge: Cambridge University Press.

Günel, K. (1995). Siyasal Coğrafyada Yeni Yaklaşımlar. *Türk Coğrafya Dergisi*. *30*. 457-461.

Heinegg, W. H. (2013). Territorial Sovereignty and Neutrality in Cyberspace. *International Law Studies*. *89* (1). 123-156.

Houtum, H. (2000). An Overview of European Geographical Research on Borders And Border Regions." *Journal of Borderland Studies*. *15* (1): 57-83.

Houtum, H. (2005). The Geopolitics of Borders and Boundaries. *Geopolitics*. *10* (4). 672-679

Johnson, D. R. ve Post, D. (1996). Law and Borders - The Rise of Law in Cyberspace. *First Monday*. *1* (1). 1367-1402.

Kalir, E. ve Maxwell, E. E. (2002). *Rethinking Boundaries in Cyberspace: A Report of the Aspen Institute Internet Policy Project*. Washington DC: The Aspen Institute.

Kearney, M. (1991). Borders and Boundaries of State and Self at the End of Empire. *Journal of Historical Sociology*. *4* (1). 52-74.

Laine J. (2015). A historical View on the Study of Borders. Sergey Sevastianov, Jussi Laine, Anton Kireev (ed.). *Introduction to Border Studies*. Vladivostok: Dalnauka. 14-32.

Le Goff, J. (2005). *The Birth of Europe*, Oxon: Blackwell.

Lessig, L. (1996). The Zones of Cyberspace. *Stanford Law Review*, *48* (5). 1403-1411.

Linklater, A. (1998). *The Transformation of Political Community: Ethical Foundations of the Post-Westphalian Era*. Cambridge: Polity.

Loader, B. D. (1997). *The Governance of Cyberspace Politics, Technology and Global Restructuring*. Newyork: Routledge.

McLuhan, M. (1992). *The Global Village: Transformations in World Life and Media in the 21st Century*. Oxford: Oxford University Press.

Mezzapelle, D. ve Zarrilli, L. (2009). Border and Cyberspace: Some Reflectıons of Political Geography, *Romanian Review on Political Geography*, 133-139.

Migdal, J. S. (2004). Boundaries and Belonging: States and Societies in the Struggle to Shape Identities and Local Practices. Cambridge: Cambridge University Press.

Minghi, J. V. (1963), Boundary Studies in Political Geography, *Annals of the Association of American Geographers*. *53* (3). 407-428.

Moraczewska, A. (2010). The Changing Interpretation of Border Functions in International Relations. *Revista Română de Geografie Politică*. 329-340.

Newman D. ve Paasi A. (1998). Fences and Neighbours in the Postmodern World: Boundary Narratives in Political Geography. *Progress in Human Geography*. *22* (2). 186-207.

Newman, D. (2003). On Borders and Power: A Theoretical Framework, *Journal of Borderland Studies*. *18* (1). 13-25.

Newman, D. (2006). The Lines that Continue to Separate Us: Borders in Our `Borderless' World. *Progress in Human Geography*, *30* (2). 143-161.

Newman, D. (2010). Territory, Compartments and Borders: Avoiding the Trap of the Territorial Trap. *Geopolitics*. *15* (4). 773-778.

Oomen, T. (1995). Contested Boundaries and Emerging Pluralism" *International Sociology*. 10. 251-268.

Ouali, A. (2006). Territorial Integrity: Rethinking the Territorial Sovereign Right of the Existence of the States. *Geopolitics*, *11* (4). 630-650.

Önok, M. (2013). Avupa Siber Suçlar Sözleşmesi Işığında Siber Suçlarla Mücadelede Uluslararası Adli İşbirliği. *Marmara Üniversitesi Hukuk Fakültesi Hukuk Arşatırmaları Dergisi*. *19* (2), 1229-1269.

Paasi, A. (2003). Boundaries in a Globalizing World. Kay Anderson, Mona Domosh, Steve Pile and Thrift Nigel (ed.)*Handbook of Cultural Geography*. London: Sage. 462-472.

Paasi, A. (1999). Boundaries as Social Practice and Discourse: The Finnish-Russian Border. *Regional Studies*. *33* (7). 669-680.

Paasi, A. (2005). Generations and the 'Development' of Border Studies, *Geopolitics*, *10* (4). 663-671.

Paasi, A. (2013). Borders and Border-Crossings, Johsnon Nuala, Schein Richard, Jamie Winders (ed.).*A New Companion to Cultural Geography*. London: Wiley-Blackwell. 478-493.

Pazarcı, H. (2015). *Uluslararası Hukuk*. Ankara: Turhan Kitabevi.

Placid, R. ve Wynekoop, J. (2011). Tracking down anonymous Internet abusers: Who is John Doe?. *Florida Bar Journal*. *85* (9), 38-40.

Prescott, J. R. V. (1965). *The Geography of Frontiers and Boundaries*. Chicago: Aldine.

Prescott, J. R. V. (1987). *Political Frontiers and Boundaries*. London: Allen and Unwin,

Ratzel, F. (1897). *Politische Geographie*. Munich/Leipzig: Oldenbourg.

Reveron, D. S. (2012). *Cyberspace and National Security: Threats, Opportunities, and Power in a Virtual World*. Georgetown: Georgetown University Press.

Sibley, D. (1995). *Geographies of Exclusion: Society and Difference in the West*. London: Routledge.

Starr, H. ve Most, B. A. (1976). The Substance and Study of Borders in International Relations Research. *Wiley*, *20* (4). 581-620.

Svantesson, D. J. B. (2006). Borders on, or Border Around - the Future of the Internet. *Law Faculty Publications*. 343-381.

Swanda, G. (2016). The Deficiencies of a Westphalian Model for Cyberspace: A Case Study of South Korean Cyber Security. *International Journal of Korean Unification Studies 25* (2). 1-28.

Tekin, F. (2014). *Sınırın Sosyolojisi: Ulus, Devlet ve Sınır İnsanları*, İstanbul: Açılım Kitap.

theory. Review of International Political Economy 1: 53-80.

Van Houtum, Henk. 2000. "An overview of European geographical research on borders and

Vaughan-Williams, N. (2009). *Border Politics: The Limits of Sovereign Power*. Edinbugh: Edinburgh University Press.

Weimann, G. (2006). Cyberterrorism: The Sum of All Fears?", *Studies in Conflict & Terrorism*. 28. 129-149.

Williams, J. (2003). Territorial Borders, International Ethics and Geography: Do Good Fences Still Make Good Neighbours?. *Geopolitics*. *8* (2), 25-46.

Wilson T. M. ve Donnan, H. (1998). *Border Identities: Nation and State at International Frontiers*. Cambridge: Cambridge University Press.

Wingfield, T. C. (2000), *The Law Of Information Conflict: National Security Law In Cyberspace*, Falls Church, VA: Aeges Research Cooperation.

Yeli, H. (2017). A Three-Perspective Theory of Cyber Sovereignty. *Prism*. *7* (2). 109-115.