SİBER UZAYDA AKTÖR - GÜÇ İLİŞKİSİ

Sevda KORHAN[*]

Özet

Siber alanın hızla büyümesi dünya siyasetinde önemli bir bağlamdır ve siber, gücü kendisine bağlamaktadır. Anonimlik unsuru, güvenlikte asimetrilerin varlığı, siber araçlara erişmenin maliyetinin düşük olması gibi sebepler devletdışı aktörlerin de siber alanda sert ve yumuşak bir güç sunma kapasitesine sahip olmalarını kolaylaştırmaktadır. Siberin doğasında var olan özellikler, aktörler arasındaki güç farklılıklarını önemli oranda azaltmakta ve bu durum 21. yüzyılda küresel siyaseti simgeleyen başat unsurların "gücün dağılımı" veya "gücün yayılması" gibi konular üzerinde şekillenmesine sebebiyet vermektedir. Devletlerin, özellikle büyük güçlerin kara, deniz veya hava gibi alanlarda söz sahibi oldukları gibi siber alanda da hâkimiyet kurmaları kolay değildir. Dolayısıyla devletler, siber alanda devlet-dışı aktörler tarafından güçlü bir meydan okumayla karşı karşıya kalmaktadırlar.

Anahtar Kelimeler: Siber Alan, Güç, Aktör, Devlet, Devletdışı Aktör

ACTOR - POWER RELATIONSHIP IN CYBERSPACE

Abstract

The rapid growth of the cyberspace is an important domain in world politics, and cyber is connecting its power to itself. The anonymity, the presence of safety asymmetries, and the low cost of accessing cyber tools make it easier for non-state actors to have a hard and soft power delivery capability in the cyberspace. The inherent characteristics of cyberspace considerably reduce the power disparities between actors, and this leads to the formation of dominant

[*] Master Öğrencisi, Selçuk Üniversitesi, İİBF-Uluslar arası İlişkiler Bölümü, E-mail: korhansevda@gmail.com

elements, which symbolize global politics in the 21st century, on issues such as "distribution of power" or "diffusion of power". It is not easy for the states, particularly great powers to dominate the cyberspace, as they have a say in domains such as land, sea or air. Therefore, the states are faced with a strong challenge by the non-state actors in the cyberspace.
Key Words: Cyberspace, Power, Actor, State, Non-State Actors

Giriş

Genellikle uzmanlar arasında kürselleşme süreciyle beraber uluslararası ilişkilerin temel koşullarının değiştiğinden kuşku duyulmamakta (Zacher, 1992:58) ve bilgi devrimi sıklıkla değişimin önemli bir sürücüsü olarak adlandırılmaktadır (Castells, 1996:16). Modern hayatın pek çok alanında bilginin egemen olması ve yayılması bu dönemin 'bilgi çağı' olarak adlandırılmasına neden oldu. 'Bilgi toplumu', 'siber-terörizm', 'siber-alan', 'e-ticaret' gibi terimlerin yanı sıra "bilgi devrimi", "bilgi çağı" hatta "bilgi çağı ötesi" ya da "post-information age" gibi ifadeler de bu süreçle beraber literatüre girmiş oldu. Bu konuda esas tartışma yaratan durum ise, bilgi devriminin devleti ve uluslararası sistemi nasıl etkilediği meselesi olmuştur.

Siber, küresel bir alandır. İnternet bağlantısına sahip bir bilgisayara, bir akıllı telefona veya başka herhangi bir mültimedya cihazına erişebilen herkes tarafından kullanılabilir. Dolayısıyla bu alanda farklı ihtiyaçlar, amaçlar ve niyetler taşıyan birçok aktör mevcut. Bazıları yalnız başına davranırken bazıları ise daha resmi yapılarla birlikte hareket etme eğilimindedir. Roller duruma göre değişebilir veya birbiriyle örtüşebilir. Aktörler ise zaman içinde veya mevcut hedeflerine bağlı olarak kategoriler arasında dolaşabilirler. Dolayısıyla siber uzayın meydana getirdiği yoğun ve hızlı etkileşimler, uluslararası ilişkilerin önemli iki kavramı olan "güç" ve "aktör" üzerinde ciddi değişikliklere yol açmış ve varsayımlarını zor duruma düşürmüştür.

Literatürde bu konuyla alakalı çeşitli argümanlar ileri sürülürken, yaygın olarak küresel bilgi ağının ulus ötesi mimarisinin, hayali olan sınırları tamamen ortadan kaldırdığı düşünülmüştür. Bilgi teknolojilerinin hem askeri hem de sivil alana uygulanması, siyasal, askeri ve sivil alanlar arasındaki sınırların bulanıklaşmasına yol açmış ve devlet-dışı aktörlerin de bilgi teknolojisine sahip olarak daha da güçlenmesine yol açmıştır. Dolayısıyla gücün dağılımı uluslararası sistemin bir parçası olarak yalnızca devletlerarasında değil, aynı zamanda özel işletmeler, politikacılar ve ulus ötesi kuruluşlarla birlikte giderek daha karmaşık hale gelmiştir (Papp ve Alberts, 1997:285).

Yeni bilgi ve iletişim teknolojilerinin dünya çapında uygulanmasının bireysel, ekonomik, siyasi ve kültürel tüm aktörler için uygun ortam sağladığı düşünülmekte ve her türlü bilgiye erişimin ve bilgi akışının yaygınlaştırılmasının önemini vurgulamaktadır. Aynı zamanda bu teknoloji geniş ölçüde, bu toplumsal aktörlerin devlete karşı güçlenmesine yol açmaktadır. Bu teknolojik araç uygulamalarının devlet kurumlarının etkinliğini arttırdığına ve devlet ile toplum arasında daha yakın bir işbirliği kurma potansiyeline sahip olduğuna inanılmaktadır. Bununla birlikte, bilgi toplumu kavramı ile bağlantılı olarak, birçok kuramcı ve siyasetçi bilgi çağında internetin demokratik bir etkiye sahip olduğunu iddia etmektedir (Loader, 1997:1-19).

Genel itibariyle bakıldığında esasında siber uzayda güç ve aktörün ne olduğu ve ne noktada birbiri ile ilişkili olduğu bu çalışmada tartışılacaktır. Akademik çerçevede çokça tartışılan ve derin fikir ayrılıklarına sebep olan bu konunun çalışılmaya ihtiyacı vardır. Nitekim aktörler arasında gücün dağılımı konusunda bir uzlaşmaya varılamaması ve bunun sonucunda ortaya çıkan çelişkiler de bu çalışmanın konusu olacaktır. Öte yandan, devletlerin ve devlet-dışı aktörlerin siber alanda güç sahibi olabilmek için ihtiyaç duydukları araçlar ve bunları kullanabilme kapasitelerinin önünde ortaya çıkan engeller de çalışmada analiz edilecektir. Son olarak, çalışmanın kilit noktasını oluşturan güç dağılımı üzerinde durulacaktır.

SİBER UZAYIN KAVRAMSAL ÇERÇEVESİ

"Siber" kelimesi William Gibson tarafından 1984 yılında yayınlanan *Neuromancer* adlı kitabında kullanılmıştır. Gibson siberi, insan sisteminde bilgisayarlardan soyutlanan her bir verinin grafiksel bir gösterimi olarak tanımlamaktadır. Diğer taraftan Gibson, daha soyut bir tanımlamaya giderek bu kavramı rızaya dayalı bir halüsinasyon türü veya düşünülemez karmaşıklık olarak da tanımlamıştır (Gibson, 1984:128). Günümüzde sibere kavramsal bir çerçeve kazandırmak pek de kolay bir durum olmamakla beraber, siber kavramı çeşitli şekillerde tanımlanmaya çalışılmaktadır.

Son otuz yıldır siber, 'günlük yaşamın dokusuna dokunmuştur' ve bugün modern toplumun tüm alanlarına nüfuz etmektedir. En yeni rakamlar, Haziran 2017 sonu itibariyle, 4.8 milyar insan ya da dünya nüfusunun %51'nin internet kullanıcısı olduğu yönünde(internetlvestats, 2017). 2000 yılından bu yana internet kullanıcıları sayısı hızla artmaktadır (Buchan, 2016:11). Gerçekten de teknoloji, yaşam biçimimizi büyük ölçüde değiştirdi. Bilgi çağında yaşadığımızı hissettiğimiz sınırsız araç mevcut. Kültür, ticaret, eğlence ve araştırma gibi çeşitli sektörleri de

içine alan sanal bir dünya, tüm kesimlerde devrim niteliğinde değişikliklere yol açtı. Bilgisayar ve telekomünikasyonun angaje olması ve bu teknolojilerin düşük bir maliyetle dünya çapında erişime açılması bir dönüşüm yarattı. Ancak siber alan tarafından sunulan muazzam fayda ve fırsatlara rağmen siber alanın yarattığı tehdit ve zaaflarda da artış göstermiştir. Günümüzde bilgi iletişim teknolojisinin gittikçe artan önemi konusunda fikir birliğine varılmış olmasına rağmen, bu gelişimin güvenlik ve diğer konulardaki etkisini de belirlemekte yarar var.

Siber alana olan bağımlılık pek çok yerde yaygınlaştığından, siber saldırı ve siber istihbarat gibi tehditlerin de aynı oranda artış gösterdiği gözlenmektedir. Her gün sayısız siber saldırının gerçekleşmesi önemli tehditleri önemsiz tehditlerden ayırmayı zorlaştırmaktadır (Haley, 2016). Bilgi teknolojisinin yaygınlaşmasıyla beraber, devletlerin zayıf yönlerinin sömürülmeye açık hale gelmesi, çeşitli aktörlerin ciddi yıkımlara sebep olabilecek güç ve yeteneklere daha kolay bir şekilde sahip olmasının yolu açılmıştır (Nagorski, 2010:1). Bugün sivil kuruluşların çoğunun fiziki altyapısının ve hizmetlerinin, ciddi oranda internet ve bilgi ağlarına bağımlı olduğu görülmektedir. Enerji, trafik, su, bankacılık, eğitim, sağlık, borsa, ulaşım gibi birçok hizmet internete bağımlı hale gelmiştir ve bu durum, bu alanlardan herhangi birindeki güvenlik açığının diğer bütün alanlara büyük zararlar verebileceğinin ve ülkenin kritik altyapılarını çökertebileceğinin işaretidir.

İnternetin gelişmesiyle beraber içinde yaşadığımız gezegen daha küçük bir hal alarak sınırlar arasında önemli derecede etkileşimi artırmıştır. Fakat internetin sınır-aşan özelliği sebebiyle siber uzay siber suçlular, siber saldırganlar ve organize suçlular için uygun bir ortam yaratmıştır. Bu sebeple ülkeler, etkili bir siber güç ve caydırıcılık politikasını sağlamak için çalışmalar yürütmeye başlamışlardır (Nagorski, 2010:9). Siberle ilgili faaliyetler, devletlerin sınırlarını aşarak geniş bir alana ulaşabildiklerinden dolayı, devletin geleneksel askeri şiddet unsurlarından oldukça farklıdırlar. Şimdiye kadar 140'tan fazla devlet siber silahlara sahip olmuş ve 30'dan fazla ülke ise askeri birimlerinde siber alanla ilgili birlikler ya da siber ordular kurmuşlardır (Jensen, 2012:780).

SİBER UZAYDA AKTÖRLER

Uluslararası İlişkiler disiplini içerisinde, uluslararası olarak adlandırılan geniş sahanın, aktörlerinin ve bu aktörlerin ilişki biçimlerinin tanımlanması daima önem teşkil etmiştir. Ulus-devletler, siber alanın yönetiminde, izlenmesinde ve düzenlenmesinde önemli bir rol

oynamasına rağmen devletlere karşı bağımsız olarak güçlerini kullanan devlet dışı aktörler de mevcuttur. Siber alanda farklı motivasyonlara sahip çok sayıda aktörün varlığı, anonimlik, ve kimliğini gizleme gibi yöntemlerle nedeniyle siber uzayda tam olarak ne olup bittiğini ve sorumlunun kim olduğunu belirlemeyi zorlaştırmaktadır. Bu belirsizlikler sadece siber eylemin amacını karmaşıklaştırmakla kalmaz, saldırıya uğrayanların misilleme yapma yeteneklerini de zorlaştırmaktadır. Çünkü siber alanda atıf yapmak zor olmaktadır (Grohe, 2015:9-10).

Siber uzayın, gün geçtikçe daha fazla insanı ve diğer aktörleri içine sürükleyerek kendi alanında aktör sayısını maksimize etme eğiliminde olduğu görülmektedir. Bireyler ve toplumlar ağlar aracılığıyla sınırlar dâhilinde veya sınır aşan biçimde sosyalleşmeye başlamışlardır. Van den Berg ve Boeke şu anda hangi aktörlerin farklı bir rol oynadıklarını; kavramsal olarak olayların türleri, bu aktörleri neyin yönlendirdiği ve amaçlarının neler olduğu gibi sorunları netleştirmeye yönelik yeni yöntemler geliştirmektedirler (Berg ve Boeke, 2016). Çalışmanın bu bölümünde siber uzayda etkili olan devlet ve devlet-dışı aktörlerin rolleri incelenecektir.

Devletler

Realistlere göre, uluslararası ilişkilerde devlet dışı aktörlerin pek önemi yoktur. Devlet her koşulda diğerlerinin hareket alanını belirleyen temel ya da merkez aktördür (Aydın, 2004:36-38). Edward Hallett Carr, George F. Kennan, Hans Morgenthau gibi realist yazarlar uluslararası sistemin başlıca aktörü olarak devleti görmüşlerdir (Carr, 1946; Kennan, 1966; Morgenthau, 1948). Realizmin aksine liberalizm ise birey de dâhil olmak üzere devlet dışı aktörleri siyasal ve toplumsal süreçlerin işleyişinde önemli görmektedir. Dahası liberaller, devlet tercihlerini ve davranışlarını hem ulusal hem de uluslararası sivil toplum tarafından kısıtlanmış ve etkilenmiş olarak görmektedir (Moravcsik, 1997:513). Ancak realist paradigmaya göre devletler güvenliklerini garanti altına almak ve güçlerini arttırmak için başat aktörler olarak kabul edilmiştir. Fakat ilerleyen bölümlerde değineceğimiz gibi siber alan, devletin bu başat konumuna meydan okumaya başlamıştır.

Küreselleşme süreciyle beraber Wesphalya ulus-devlet düzenine karşı kritik birtakım güçler sivrilmeye başlamıştır. Küreselleşme sürecinin ortaya çıkmasıyla beraber ulusal sınırları aşan "uluslararası toplum", "karşılıklı bağımlılık", "küresel işbirliği" gibi fikirler 20. Yüzyılın ikinci yarısından itibaren uluslararası sistemde geniş yer tutmaya başladı. Bu durum, birçok ulusal

hükümet, uluslararası kurum ve sivil toplum aktörlerinin küresel sorunlarla yüzleşmek için birlikte hareket etmeye başlamasıyla sonuçlandı.

Çevre, insan hakları, ekonomi, küresel ısınma gibi küresel bazı sorunların çözümünün küresel işbirliğiyle mümkün olabileceği gerçeği gün geçtikçe anlaşılmıştır. Küresel iletişim ağı, teknolojideki yenilikçi gelişmelere dayalı hızlı bir gelişme göstermeye devam ederken, devletin ulusal ağlarını koruma altına alma ya da güçlendirme yeteneği giderek hizmet sağlayıcıları, özel sektör, uzmanlar, ajanslar ve işbirliği yapan hükümetler arasındaki karşılıklı bağımlılığa dayanmaya başlamıştır. Dolayısıyla uluslararası işbirliği, ağ güvenliği, ağ standartlarının geliştirilmesi ve uygulanmasına yönelik bir çözüm olarak görülmüştür (Felicia ve Hensel, 2007:6). Dolayısıyla siber alandaki devletler ve devlet dışı aktörler arasında çizgilerin kısmen bulanıklaştığı söylenebilir çünkü ulus devletler, siber alanda amaçlarını gerçekleştirmek için "güçlendirme" yoluna başvurmaktadırlar. Hedeflerini yerine getirmeleri için paralı askerleri harekete geçirmektedirler. Örneğin, ABD seçimlerine Rusya'nın siber saldırı iddialarına yönelik olarak Demokratik Ulusal Komite ve Obama Yönetimi tarafından yapılan "yalnızca Rusya'nın en üst düzey yetkililerinin bu faaliyetlere izin vereceğine inanıyoruz" şeklinde yaptıkları açıklamada ABD'nin saldırıyı Rusya'nın kendi eliyle gerçekleştirmiş veya kontrol ettiği ve yönlendirdiği bazılarının olduğunu ima ettiği görülmektedir(Ackerman, 2016).

Bu işbirliği ve yönlendirmeye rağmen devletler güvenlik odaklı bir yaklaşımla bu alanda da devamlılığını sağlamaya çalışmaktadır. Birçok devlet tarafından "*beşinci muharebe alanı*" olarak adlandırılan siber uzay (diğerleri hava, kara, deniz ve uzaydır), devletlerin bu alandaki güçlerini garanti altında tutmak veya maksimize etmek için çeşitli stratejiler geliştirdikleri bir alan haline gelmiştir (Çelik, 2015:32). Siber uzayda devletlerarasında başlamış olan rekabetin doğal bir sonucu olarak devletler, gerek siber savunma stratejilerini geliştirmek için, gerekse siber saldırı kapasitelerini arttırmak için siber ordulara önemli ölçüde yatırımlar yapmaktadırlar.

Bununla beraber devletler, yalnızca rekabet etmenin rasyonel bir davranış olmadığını bilen varlıklar olarak, fiziki alanda olduğu gibi, sanal alanda da taraflarını belirleyerek, savunma ve istihbarat sistemini güçlü tutmaya çalışmakta ve bu amaçla ittifaklar kurmaktadırlar. Örneğin, Eski ABD Başkanı Barack Obama, 2016 itibariyle güvenliği arttırmak maksadıyla siber alana ayırdıkları bütçeyi %35 oranında arttırdıklarını ilan ederek, bu alana verdikleri önemi bir kez daha vurgulamıştır (Gücüyener, 2016). ABD'nin ulusal istihbarat direktörü Mike McConnell,

2010'da kaleme aldığı *Kaybettiğimiz siber savaşı nasıl kazanacağız* adlı çalışmasında, dünyanın 1950'li yıllara döndüğüne işaret ederek nükleer gücün artması için uğraşan devletlerin artık siber saldırılarla baş etmede kullanabileceği yöntemler geliştirmesi gerektiğini savunmuştur (Nagorski, 2010:1).

Geleneksel devlet-güç siyasetinin siber uzayda oynadığı rolün farklı bir biçimde işlediği görülmektedir. Siber, yalnızca uluslararası güvenlik alanlarında aynı aktörler tarafından kullanılan bir araç ya da silah olarak adlandırılabilir. Siberin yönetilemeyen alanında, devlet-iktidar politikası halen yürürlüktedir. Ancak geleneksel saldırı biçimlerinin aksine burada kurallar yoktur ve ulus devletler tarafından sıkı bir şekilde uygulanabilen kısıtlamalar mevcut değildir (The Cipher Brief, 2016). Dolayısıyla Sony, DNC veya OPM'ye karşı yürütülen saldırılar gibi büyük ölçekli saldırılar artık yalnızca ulus devletler tarafından gerçekleştirilebilecek eylemler olmayabilir (Schmitt, 2014).

Devlet-Dışı Aktörler

Devlet dışı aktörler siber alanı, bir çatışma aracı olarak kullanmaktadır. Devlet-dışı aktörlerle ilgili bu varsayımlar beş noktada özetlenebilir:

- Devlet dışı aktörler çatışmalarda siber alanı kullanır;
- Yenilgiye uğratmak, siber faaliyet alanlarındaki nihai hedefidir;
- Bu, stratejik bir anlatı yaymak ve yumuşak güç kurmak suretiyle yapılır;
- Amaçlarına ulaşmak için gerilla taktikleri kullanırlar;
- Etkinlik, organizasyonun ve kaynakların seviyesine göre belirlenir (Cathrine ve Wilhelmsen, 2014:5).

Aktör	**Motivasyon**	**Hedef**	**Yöntem**
Sıradan vatandaşlar	Hiçbiri veya zayıf	Herhangi biri	Dolaylı
Çocuklar	Merak, heyecan, ego	Bireyler, şirketler, hükümetler	Daha önce yazılmış komut dosyaları ve araçlar

Hackerlar	Siyasi veya toplumsal değişim	Karar vericiler veya masum kurbanlar	Hizmet durdurma veya DDoS saldırısı vasıtasıyla protesto gösterileri
Siyah Şapkalı Hackerlar	Ego, kişisel düşmanlık, ekonomik kazanç	Herhangi biri	Zararlı yazılımlar, virüsler, güvenlik açığı istismarları
Beyaz şapkalı hackerlar	İdealizm, yaratıcılık, yasalara saygı	Herhangi biri	Penetrasyon testi, yama
Gri şapkalı hackerlar	Belirsiz	Herhangi biri	Çeşitli
Vatansever Hackerlar	Vatanseverlik	Kendi ulus-devletinin düşmanları, dolandırıcılık, diğer kurbanlar	DDoS saldırıları, yolsuzluklar
Siber İçerikler	Finansal kazanç, intikam, şikâyet	İşveren	Sosyal mühendislik, arka kapılar, manipülasyon
Siber teröristler	Politika veya toplumsal değişim	Devletler, Ötekiler ya da diğer kurbanlar	Bilgisayar tabanlı şiddet veya imha
Kötü yazılım yazarları	Ekonomik kazanç, ego, kişisel düşmanlık	Herhangi biri	Güvenlik açığının kötüye kullanımı
Siber dolandırıcılar	Finansal kazanç	Bireyler, küçük şirketler	Sosyal mühendislik
Organize siber suçlular	Finansal kazanç	Bireyler, şirketler	Dolandırıcılık, kimlik hırsızlığı,

			şantaj için DDoS kötü amaçlı yazılım
Şirketler	Finansal kazanç	BİT tabanlı sistemler ve altyapılar (özel ya da kamu)	Saldırı veya etki operasyonları için çeşitli teknikler
Siber casusluk ajanları	Finansal ve siyasi kazanç	Bireyler, şirketler, hükümetler	Bilgi edinme teknikleri
Siber savaşçılar	Yurtseverlik, mesleki gelişme	Kendi ulus devletinin düşmanları, bireyler, şirketler	Grup yetenekleri

Tablo 1. Siber Uzayda Devlet-Dışı Aktörler (Sigholm, 2013:11).

Tablo-1'den de görüldüğü üzere, devlet-dışı aktörler siber uzayda farklı motivasyon, hedef ve yöntemlerle hareket ederek bu alanda faaliyetlerini yürütmektedirler. Kimi devlet açısından kolaylıklar sağlarken kimisi ise büyük sorunlara sebep olabilmektedir. Katharina Ziolkowski, siber uzaydaki birçok devlet dışı aktörün ortaya çıkardığı kötü niyetli eylemlerin kim tarafından yapıldığının belirlenmesi ve bu doğrultuda misilleme yapılmasının zorluğuna işaret etmektedir(Pihelgas, 2013:40). East West Enstitüsü'nün (EWI) *Siber Uyuşmazlığı Yönetmek İçin Kurallar: Siber Uzayda Cenevre ve Lahey Sözleşmelerinin Oluşturulması* başlıklı çalışmasında, siber alanda devlet dışı aktörlerin sorunlarına değinildi. Raporda Rusya, ABD ve diğer ilgili taraflar, siber savaşçıların devlet dışı aktörler olabileceği gerçeğinden hareketle sözleşme ilkelerinin nasıl en iyi şekilde yürütülebileceğini değerlendireceklerdir (Rauscher, 2011). Fakat devlet dışı aktörlerin siberle olan ilişkisi hakkındaki bu değerlendirme, henüz sonuçlanmamıştır. Devlet dışı aktörlerin giderek artan önemi küreselleşme sürecinin hız kazanmasıyla beraber uluslararası ilişkilerin her alanında belirginleşmiş bir meseledir (Gady, 2011).

Sonuç olarak siber uzay, yarattığı olumlu havanın yanı sıra, aynı zamanda uzun süredir çatışmada kullanılan bir araç haline gelmiştir. Siber uzayda rekabet eden hacker çeteleri aktif olarak birbirleriyle etkileşim halindeyken, protesto grupları fikirlerini sanal vandalizm yoluyla

seslendirmekte, suç örgütleri kolay kazanç sağlamak amacıyla kötü amaçlı yazılımları yaymakta ve gizli aktörler ise yasadışı istihbarat topluluğuna hizmet etmektedir. Devlet dışı aktörlerin yaygınlaşmasında siber alan, on yıllar öncesinden başlayan bir süreci hızlandıran ve güçlendiren bir "güç çarpanı" olarak karşımıza çıkmaktadır. Bununla birlikte, devlet dışı aktörlerin belirsiz ve farklı karakterleri, bu aktörlerin hareketlerini izleme güçlüğü ve kritik altyapılar üzerinde yaratabilecekleri yıkıcı güç nedeniyle siber alanda benzersiz bir sorun teşkil etmektedir.

SİBER UZAYDA AKTÖRLER ARASINDA GÜÇ DAĞILIMI

Bu bölümde özellikle yumuşak bir güç unsuru olarak siber uzay, güç araçları, aktörlerin gücü kullanma kapasiteleri ve devletdışı aktörlerin siber uzayda güçle ilişkisi gibi konular tartışılacaktır.

Yumuşak Güç Unsuru Olarak Siber Güç

Uluslararası İlişkiler teorisyenleri 20. yüzyılın başından itibaren gücün ne olduğunu ve güç edinmenin amacını sorgulamışlardır. Özellikle realistler güç üzerinde çalışmalar yapmış ve realist teori, gücü daima maksimize edilmesi gereken nihai bir hedef olarak görmüştür. Genel anlamda güç kavramın, "başka aktör üzerindeki etki kapasitesi" olarak tanımlanır. Aslında realizmin güç tanımı, bir *hard power (sert güç)* unsuru olan askeri güç ile ilişkilendirilir ve diğer unsurlar göz ardı edilir. Realistler için uluslararası arenada güvenlik ikileminin (*security dilemma*) yarattığı çatışmayı önlemek veya çıkar maksimizasyonunu sağlamakta rol oynayan en önemli olgu güçtür (Guzzini, 2001:18). Dahası güç, Realist teori için devletin uluslararası politikada temel önceliklerini şekillendiren ve bu önceliklere ulaşmasını sağlayan ana unsurdur.

Bu bağlamda Realist teori gücü daima maksimize edilmesi gereken nihai bir amaç olarak görmekte ve genellikle bu gücü askeri güç ile bağdaştırma eğiliminde olmaktadır. Ancak 21. Yüzyılda gücün en önemli kaynağı olarak bir *Soft power* (*yumuşak güç*) unsuru olan "bilgi teknolojisi" gösterilmektedir (Nye, 2011). Bilgi teknolojisine veya siber güce sahip devletlerin, diğer devletlerden daha güçlü olduğu yönünde iddialar bulunmaktadır. 21. yy'da Joseph Nye'ın kavramsallaştırdığı *soft power*'ın varlığı önem kazanmaya başlamış, bu bağlamda "siber güç" de bir yumuşak güç unsuru olarak karşımıza çıkmıştır (Nye, 2011).

Peki, siber güç nedir? Bu kavram, klasik güç anlayışından çok da soyutlanamayacak bir tanımlamaya sahip. Siber güç; "Siber alanı, güç araçları aracılığıyla diğer aktörleri etkilemek için kullanabilme yeteneği" olarak tanımlanabilir. Realist teorinin iyi okuyamadığı küreselleşme süreciyle beraber akademisyenler, diğer konulara ek olarak gücün siber alana kayması durumuna dikkat çekmeye başlamışlardır. Çünkü ağlar üzerinden yapılan faaliyetler arttıkça devletler altyapılarını bu ağlar üzerinden sağlamaya çalışmışlardır.

Geleneksel savaş döneminin konusunu, çoğunlukla devletler arasındaki güç mücadelesi oluşturmuştur. Çatışma ve güç oyunlarının dünya siyasetine hâkim bir özelliği olduğu, realist teori tarafından sık sık vurgulanmıştır. Realist yazarlar, devlet gücünün bir indeksi olarak askeri gücün önemini vurgulamışlardır. Yumuşak gücün gerçekliği ve önemi çok tartışmalı bir konu olmakla beraber realistler doğal olarak bu kavramın en büyük eleştirmenleri arasındadır. Realistler ekonomik faktörleri, ulusal gücü yansıttıkları ya da etkiledikleri ölçüde önemli gördükleri halde, asıl gücün askeri güç olduğunu iddia etmektedirler.

Görüldüğü üzere geleneksel anlamda temel güç faktörleri olarak askeri ve ekonomik güçler görülürken şimdi ise "siber güç" de önem kazanmıştır. Bu nedenle bilgi, inanç ve düşünce üzerindeki kontrol, askeri ve ekonomi gibi somut kaynakları kontrol altına almanın bir tamamlayıcısı olarak görülmektedir. Bu düşüncenin büyük kısmını, savaş alanının sibere yayılması nedeniyle savaşın doğasında önemli bir değişikliğe gidildiğine olan inanç oluşturmaktadır (Vlahos, 1998:497-525). Bu tartışmayla ilgili en yaygın olarak kullanılan etiket, baskıdan ziyade kendine çekme yoluyla hedeflere ulaşma yeteneği olarak tanımlanan 'yumuşak güç'tür (Keohane ve Nye, 1998:81-94). Yumuşak güç; iletişim, eğlence ve fikirleri ifade eder ve güçlü bir kültürel ve psikolojik bileşeni vardır. Yumuşak güç ayrıca, başkalarını istenen davranışları üreten normlara ve kurumlara uymaya ikna ederek ya da onları kabul ettirerek hareket eder. Aslında burada dikkat çeken nokta, yumuşak güç kavramı ile yapısal gücün birbirine yakın olduğudur (Hart, 1976:294). Ancak uluslararası aktörler, daha az görünür olan bir güç biçimi olan yapısal gücü daha çok kullanmayı tercih ederler çünkü güç sahibi baskıya gerek duymaksızın hareket etme yeteneğine sahiptir (Volgy, Kanthak, Fraizer ve Ingersoll, 2004).

Öte yandan siber uzayın yarattığı güvenlik tehdidi ile birlikte realist okula bağlı güvenlik uzmanları, karar mercilerine hızlı bir şekilde siber dünyanın militarizasyonunu kabul etmeleri çağrısında bulunmuşlardır. Ayrıca devletlerin saldırgan ve savunma amaçlı siber yeteneklerini

geliştirmeleri gerektiğini savunmuşlardır. Stratejik planlamacılar tarafından yürütülen siber bir bileşenle ulusal güvenlik politikalarını geliştirme çabası birçok ülkede gerçekleştirilmiştir. Aynı şekilde, Avrupa Birliği ve NATO, ortak savunma politikaları geliştirmeye başlamışlardır (Bendiek, 2016). Bu doğrultuda devletin siber uzayda yeniden doğuşunu ve siber güç arayışı içerisinde olduğunu reddetmek zordur.

Siber Uzayda Güç Araçları

Siber alanda hizmetler, sunucular, web sayfaları vb. araçlar birbirine bağlıdır ve her bölüm farklı bir fiziksel bölgede yer alır. Ancak bu araçlar karşılıklı olarak birbirlerine bağımlı oldukları için birlikte çalışırlar. Bununla birlikte, her alanın farklı zorlukları vardır ve her alan üzerindeki hâkimiyet farklı bir teknoloji gerektirir. Siber uzayın büyük oranda fiziksel bir alan olmadığı gerçeğinden yola çıkarak siber alanda hâkimiyetin de önemli ölçüde farklı olduğu görülmektedir. Çünkü siber alanda fiziksel araçlar önemli oranda hâkimiyetini kaybeder ve yerini farklı taktik ve teknolojiye bırakır.

Siber uzay dört bileşenden oluşur. Bunlar kullanıcı, yazı, video, resim gibi paylaşılan bilgi, yazılımlar-protokoller ve fiziksel altyapıdır. Martin Libicki, siber alandaki katmanların her birine hükmetmek için gerekli olan araçları açıklamıştır. Libicki'ye göre ilk katman; fiziksel kablolardan ve anahtarlardan oluşur ve bu katman tahrip edici fiziki güç tarafından yönetilebilir. İkinci katman, bu sistemlerin kontrolünü elinde bulundurarak hâkimiyetini sağlayabilir. Üçüncü katman ise veri ile ilgilidir ve sansürleme yöntemiyle hâkimiyet kurabilir veya bilgiye erişimi kontrol edebilir. Dördüncü katmana gelindiğinde ise, bilişsel ya da pragmatik katmanın hakimiyetinin varlığı söz konusudur (Schmidt, 2016). Bu dört katman göz önüne alındığında siber alanda bilginin analiz edilmesi gerektiği ve her bilgi yeteneğinin geliştirilmesinin siber uzayda bir güç sahibi olmak için önem teşkil ettiği söylenebilir.

Siber alanda devletler, saldırılara karşı güvenliklerini koruyabilmek için çeşitli güç araçlarına ihtiyaç duymaktadırlar. Tüm devletlerin, anarşik, rasyonel ve güç mücadelesi içerisindeki birimler olduğunu kabul ettiğimizde siber uzay, uluslararası ilişkilerin bu temel oyuncularına yeni bir rekabet alanı sunmaktadır (Valeriano, 2016:142). Teknik açıdan bu yeni 'ortamın' gerçek dünyadan bağımsız olduğu düşünülse de siber uzayda yaşananlar, gerçek dünyadaki güç ilişkilerinin bir devamıdır. Tıpkı klasik anlamdaki ulusal güvenlik ve güç anlayışındaki gibi

devletler, siber alanda da güvenliklerini arttırmaya ve güçlerini maksimize etmeye çalışmakta ve bu bağlamda da etkili stratejiler geliştirmektedirler.

Devletler bu doğrultuda ilk adım olarak siber ordular kurmaktadırlar. Bugün dünya üzerinde resmi ve gayri resmi olarak faaliyet gösteren bir sürü siber ordu mevcut ancak ABD, Rusya, Almanya, Çin, İsrail, İran ve Kuzey Kore'nin siber ordularının olduğu bilinmekte. Onun dışında devletler eylem planlarıyla ya da caydırıcılık stratejileriyle savunma pozisyonu almakta ve bu durum daha çok güvenlik odaklı bir yaklaşımı temsil etmektedir. Diğer yandan devletler, *hard* ya da *soft power* araçlarıyla saldırıya geçmekte ya da etki alanlarını genişletmeye çabalamaktadırlar. Bu da daha çok güç odaklı bir yaklaşımı temsil etmektedir.

Devletler sert güç unsurlarını daha çok sistemleri çökertecek ya da fikri mülkiyet haklarını çiğneyebilecek şekilde kullanmakta ve hükümetler bunu genellikle ekonomik kaynaklarını artırmanın veya siyasi üstünlük sağlamanın bir yolu olarak yapmaktadır. Örneğin Çin, bu tür faaliyetlerde bir numaralı ülke olarak gösterilmektedir. Çin'in özellikle Batılı şirketlerin ticari sırlarını ele geçirdiği, ayrıca büyük çaplı savunma ve silah projelerinin gizli bilgilerine ulaşmaya çalıştığı iddia edilmektedir. Yumuşak güç uygulamasında ise genellikle siber bilgiler, başka bir ülkedeki vatandaşları cezbetmek veya bir ideolojiyi yaymak amacıyla kullanılabilmektedir. Bu durum bir çeşit "siber kamu diplomasisi" olarak da adlandırılabilir.

Devletlerin siber alanda yaptığı bir diğer faaliyet, siber uzmanlığı arttırmak ve bu alanda hacker yetiştirmektir. Ancak derin bilgisayar uzmanlığı bir avantaj olmasına rağmen siber alanda stratejik etki üretmek için çok yetersiz bir yol olarak görülmektedir. Bu konuda Col Stephen Korns'ın işaret ettiği gibi, birçok siber "silah" artık metod haline getirildi ve kişisel bir bilgisayara indirilebilen yazılımlar var. Estonya ve Gürcistan saldırılarında kanıtlanmıştır ki, çoğunluğu programlama veya bilgisayar bilimi olmayan uzman bireyler bile hazır programlarla saldırı düzenleyebilmektedir. Bu nedenle uzmanlaşmayı bir güç kıstası olarak almak yanlış olacaktır ve gücün buna göre ölçülmesi de eksik kalacaktır (Sheldon, 2011:97).

Aynı şekilde gücü ölçen bir diğer araç, Booze Allen Hamilton tarafından geliştirilen Cyber Power Indeks (CPI) aracıdır. CPI siber saldırılara dayanma ve güvenli bir ekonomi için gerekli olan dijital altyapıyı dağıtma becerisi olarak devletin siber gücünü ölçmek için kullanılan bir araçtır. Bu amaçla, bir devletin siber gücüne katkıda bulunan dört genel bileşen önerilmektedir. Bunlar; mevcut hukuki ve düzenleyici çerçeveler, ekonomik ve sosyal bağlam, teknoloji

altyapısı ve endüstri uygulaması bileşenlerinden oluşur. CPI, bir devletin savunma ve saldırı gücünü açıkça ölçmeye çalışır. CPI tarafından sağlanan bu ölçme işlemi aracılığıyla güce atıfta bulunmak cazip gelebilir fakat bu da misilleme söz konusu olduğunda güç ölçümü için yetersiz kalmaktadır. Çünkü bir devlet, misilleme sonucu oluşabilecek önemli bir hasarın farkındaysa, siber gücünü eksiksiz bir şekilde kullanmak istemeyebilir. Dolayısıyla bu durum CPI'e güçsüzlük olarak yansıyacaktır ve bu da sonuçların tutarsızlığını doğuracaktır (Gomez, 2013:3).

Yine bir güce atıfta bulunmak için geliştirilmiş bir diğer yöntem teori geliştirmek olmuştur. Zaten uluslararası ilişkiler öğrencileri için teori üretmeden yapılan bir güç tanımı eksik kalacaktır. Bir kavramın teorisini oluşturmak, kavramı anlamak açısından fayda sağlayacaktır. Biz de siber gücü bir teori olarak değerlendirmeye kalktığımızda "Bu teori pratikte nasıl kullanılabilir?" sorusu gündeme gelecektir. Böyle bir teori oluşturulduğunda nasıl bir etki yaratabilir ya da bu teori ne gibi görünmelidir? Bu konuda Harold Winston, siber alana uygulanabilen veya en azından herhangi bir girişimde bulunabilecek bir siber güç teorisinin oluşturulması için gerekli beş kriter ortaya koymuştur. Bunlar; (Winston, 2011:19-35).

- ***Alanı tanımlamak:*** Bu kriter, siber alan ve siber gücün ne olduklarıyla ilgili bilgi verir. Siber güç stratejik uygulaması araştırmaları, bu alanın olgunlaşmadığını kanıtlayan en az 14 siber uzay tanımı ortaya koydu. Dolayısıyla siber uzay ve siber güç tanımları konusunda bir fikir birliğine varmak, makul bir teori oluşmasına katkı sağlayacaktır.
- ***Seçilen parçaları kategorize etmek:*** Bu konuda Winston bir benzetmeye başvurarak şöyle bir öneride bulunuyor: "Siber gücü turuncu bir meyve olarak düşünün, dilimler halinde kesip, her birini inceleyin ve ardından bütünü yeniden oluşturmak için onları bir araya getirin." Winston'a göre bu şekilde siber gücü oluşturan parçalar veya araçlar daha kolay tanımlanabilir.
- ***Açıklamak:*** Burada siber gücün stratejik ortamda bozulma, aldatma, reddetme gibi istenen etkileri nasıl sağladığını açıklamak gerekir. Dahası bir teori, siber güçlerin en etkili olacağı koşulları belirlemeye çalışmalıdır.
- ***Diğer alanlara bağlamak:*** Bir teori, siber gücü daha geniş bir evrene bağlayabilmelidir, çünkü siber gücün hangi yönlerde diğer alanlarla etkileşime girdiğinin analiz edilmesi önemlidir. Örneğin siber güç; sürtüşmelerden, kültürler arası farklılıklardan, ekonomi gibi alanlardan ne yönde ve ne kadar etkilenir? Buna yönelik ayrıntılı bir açıklama olmalıdır.
- ***Tahmin etmek:*** İyi bir teori, siber gücün toplumu ve teknoloji üzerinde yaratacağı muhtemel etkileri tanımlamalıdır. Ancak burada beklenti ve tahminin aynı olmadığı

unutulmamakla beraber siber gücün gelecekte ölçülebilir olan daha büyük etkilerini belirlemek mümkündür.

Güç Kullanma Kapasitesi

Dünya, devletlerin siber saldırı, sömürü ve casusluk yeteneklerini arttırmaya çalıştıkları bir siber "silahlanma yarışının" yanı sıra, aynı işlemlere karşı savunma için siber güvenlik önlemlerini arttırmaya çalıştığına da tanıklık etmektedir. Siber uzay kavramı NATO tarafından da kara, deniz, hava ve uzay'dan sonra muharebenin beşinci boyutu olarak kabul edildi (Yüksel, 2017). Enformasyon devrimi ve yukarıda aktarılan pek çok noktada literatürün çoğunun ortak bir özelliği, "bilgi çağında" bilginin iktidarın ana kaynağı haline geldiğine olan inançtır. Örneğin, 'yumuşak güç' kavramı, 'gücün sermaye zenginden bilgi zenginine geçtiği' tartışmalarına dayanır. Sonuç olarak bu, enformasyon devrimine en iyi şekilde liderlik edebilecek bir ülkenin, diğerlerinden daha güçlü olacağı anlamına gelir. Ancak, bu durum birçok ülke için asimetrik bir etki yaratabilir. Çünkü altyapılarını siber teknolojiye bağımlı hale getiren ülkeler, siber saldırılara karşı daha açık bir konuma gelmiştir. Bu durum devletlerin gücü edinme ve kullanma kapasitelerini kısıtlayan bir durum olsa da devletler güçten ve güçlü olmaktan vazgeçmemektedir.

İçinde bulunduğumuz dönem itibariyle en ileri siber savaş kapasitesine sahip olduğu düşünülen ülkeler ABD, Rusya, Çin, İngiltere ve İsrail olarak görülmektedir. Devletler siber savaş kapasitelerini arttırabilmek için siber savunmaya belli bir bütçe ayırmaktadırlar. Bugün siber alanda savunma harcamaları için ABD 19 Milyar Dolar, Rusya 11 Milyar Dolar, İsrail 6 Milyar Dolar ve İngiltere 860 Milyon Pound ayırmaktadır (Yüksel, 2017). NATO, Mükemmeliyet Merkezi (Cooperative Cyber Defence Center of Excellence) adlı siber savunma sistemini kurarak siber kapasitesini arttırmaya yönelik önemli bir adım atmıştır. NATO'nun yanı sıra Avrupa Birliği de siber alana yönelik önemli girişimlerde bulunmuştur. Bilhassa 2010'da Avrupa Konseyi (Council of Europe) bünyesinde imzalanan Siber Suçlar Sözleşmesi, uluslararası işbirliği yolunda önemli girişimler arasında yer almaktadır (Yüksel, 2017).

ABD ise bu alanda maliyet önlemi yoluyla saldırganları caydırmaya çalışmaktadır. Bu önlemler, ABD aleyhinde siber saldırı veya diğer kötü niyetli siber faaliyetlerde bulunmayı seçen düşmanlara karşı cezalandırma ve maliyeti arttırma amacıyla eylemler gerçekleştirmek üzere tasarlanmıştır. Bu önlemler, ABD Hükümetinin geçerli uluslararası yasalara uygun ve

uyumlu olan tüm gerekli vasıtalarla siber saldırılara cevap verme kabiliyetini ve istekliliğini kullanmaktadır. Bu tür tedbirler, kanun uygulama önlemlerini almak, kötü niyetli siber aktörleri cezalandırmak, saldırgan ve savunma amaçlı siber operasyonlar yürütmek, hava, kara, deniz ve uzay yoluyla güç sunmak ve mevcut tüm seçeneklerin tükenmesinden sonra askeri güç kullanmak gibi görevleri içermektedir (Federal News, 2015). "Caydırıcılık" terimi, ABD politika belgelerinde de merkezi ve belirleyici bir rol oynamaktadır. Örneğin, Birleşik Devletler Doğu Batı Enstitüsü ve Rusya Bilişim Güvenliği Enstitüsü 2011 yılında siber ve bilgi güvenliği için kritik şartları tanımlayan ortak bir Rus-Amerikan raporu yayınladı. Bu rapor belirli şartlar için kabul edilmiş tanımları içermektedir. Rapor, Rusya ve ABD tarafından hükümet düzeyinde siber meselelerde olası işbirliğine iyi bir örnektir. Raporun bir diğer amacı, her iki tarafın siber alanla ilgili belirli terimlere ilişkin anlayışını açıklamasıdır (Lin, 2017).

Bradley Manning ve Edward Snowden ABD'nin siber gücü ile ilgili bazı açıklamalarda bulunmuşlar ve ABD'nin siber yeteneklerini şöyle özetlemişlerdir: "ABD dünyada başkalarının yapabileceği her şeyi yapabilir ancak yapabileceği her şeye karşı bir savunma sistemi geliştiremez."(Carafano, 2013). Çünkü siber yeteneklerini ve gücünü arttırmaya çalıştıkça saldırıya maruz kalma riskini de doğru orantılı olarak arttırmaktadır. ABD bu yüzden siber alanda davranışlarını kısıtlamak zorunda olan bir ülke haline gelmiştir. ABD'nin teknolojik altyapısı ne kadar güçlüyse, siber saldırılara karşı da o denli savunmasızdır. Çünkü Rusya ve Çin gibi ciddi rakiplerine oranla sivil ve askeri altyapısını büyük oranda siber alana angaje etmiştir. Dolayısıyla ABD, siber alanda hem savunmacı hem de saldırgan pozisyonu itibariyle en üst düzeyde olan devlet konumunda görünmektedir (Marmon, 2011). 2016 ABD seçimlerine Rusya tarafından bir müdahale gerçekleştiği yönünde iddialar bulunmaktadır. Obama yönetimi, seçimlere müdahale etmesi nedeniyle Rusya'ya yönelik bir dizi yaptırım uygulayacağını açıklamıştır. Bu yaptırım ve tehditlerin ileride olabilecek herhangi bir Rus saldırısına karşı caydırıcılık unsurunu devreye sokacağı düşüncesi söz konusudur (Rojansky, 2016).

Ulusal Güvenlik Ajansı (NSA) gözetim merkezleri ise, siber alana yönelik politikalarının gerekçesi olarak; "birisinin bunu yapması gerektiği" ve "bunu başka herhangi birinden daha iyi yapabileceğimiz" fikrini öne sürmüşlerdir (The Guardian, 2014). Eski NSA Çalışanı Edward Snowden, ABD'nin "İstihbaratın Beş Gözü" adı verilen bir yapı kurduğunu açıkladı. Devletlerarasında siber istihbarat ve veri paylaşımında bulunan bu yapıya üye olan ülkeler; ABD, İngiltere, Kanada, Yeni Zelanda ve Avusturya'dır. Bu devletler dünyanın çeşitli yerlerinden edindikleri bilgileri ekonomik, askeri ve istihbari stratejilere dönüştüreceklerdir.

Ayrıca bu devletler rakiplerinin güvenlik açıklıklarını tespit etme veya onları dinleme gibi faaliyetleri de yerel taşeron örgütlere yaptırmaktadırlar (Yüksel, 2016).

Siber tehdit ciddi bir ulusal güvenlik meselesidir, çünkü orada saldırmayı bekleyen online düşmanlar mevcuttur. Ancak Choney'e göre burada da düşmanlar eşit olarak yaratılmamıştır. Özellikle Amerikan bir bakış açısıyla yaklaşan Choney, ABD'nin karşısındaki en büyük rakipler olarak Çin ve Rusya'yı görmektedir. Ancak bu durum, diğer devletlerin bir tehlike oluşturmadığı anlamına gelmemektedir. Zira K.Kore, Suriye ve İran gibi ülkeleri de azımsamamak gerekir. Örneğin ABD eski başkanı Obama Suriye'ye yönelik yaptırım kararı aldığında, Suriye Siber Ordusu'nun New York Times, Twitter ve ABD Deniz Piyadeleri web sitelerine başarıyla saldırdığını gösteren medya raporları ortaya çıkmıştır (Choney, 2013).

Suriye gibi siber yetenekleri sınırlı olan bir ülkenin bile siber silahlanma yarışında yer alması, bütün devletlerin gelecekte bu yarışa katılacağı yönündeki beklentileri arttırmaktadır (Grohe, 2015:15). Sosyal medyadaki haber kuruluşları ve videoların yanı sıra, siber bölgedeki iç savaşı etkileyen en önemli aktör Suriye Siber Ordusu Syrian Electronic Army (SEA) olarak adlandırılan bir gruptur.

SEA, halka açık alanlardan yıkıcı siber saldırı ve sömürüye kadar uzanan ve siber casusluğa işaret eden bazı kanıtlarla faaliyet gösteren bir rejim yanlısı hack grubudur. Mayıs 2011'in başından itibaren SEA, Suriye Bilgisayar Topluluğuna ait çeşitli kurucu üyelerle birlikte Beşar Esad'a yakın bir ilişki içinde ve bilgi teknolojisi alanını Suriye toplumuna dâhil etmekle yükümlüdür (Perlroth, 2013). Suriye kadar siber altyapısı zayıf olan bir ülke bile, sosyal medya ve haber kuruluşlarının raporlarını genişletebilir, arttırabilir veya aşabilir. Haber kuruluşları bir olayı işleme ve sunma kapasitesini kaybettiğinde, sosyal medya bu boşluğu doldurabilir. Suriye'deki çatışmanın tarafları, olaylara ilişkin görüşlerini yaymak için sosyal medyanın gücünden faydalandılar. SEA'nın Beşar Esad rejimiyle dolaylı ilişkilerine rağmen, grubun rejim adına siber operasyonlar gerçekleştiren fiili bir ulusal siber güç olduğu açıkça görülmektedir (Grohe, 2015:9).

Estonya da küçük ülkeler arasında yer almasına rağmen siber alanda ilerleme kaydeden ülkeler arasında yer almaktadır. Estonya'nın post-Sovyetler Birliği'nden hızlı bir şekilde kopması dünyanın önde gelen bilgi devletlerinden biri haline gelmesini ve güvenliğe de daha hızlı ulaşmasını sağlamıştır. Estonya, dijital kimlik kartları ve veri tabanları oluşturmada oldukça

başarılı bir ülke olarak görülmektedir. Estonya ayrıca, yurtdışındaki büyükelçilik konutlarının yanı sıra, ulusal verilerini yedekledikleri güvenli bölgelerde "veri elçilikleri" de kurarak bölgede sanal bir ülke olarak yeniden yapılandırmasını sağlamaktadır (Khanna, 2015).

Estonya şimdi NATO'nun Siber Savunma Birimine ev sahipliği yapmaktadır. 2015 yılının başında da Microsoft Windows gibi işletim sistemleri aracılığıyla saldırılara karşı koruma amaçlı bir "eğitim kilidi" olan "Locked Shield" operasyonu için bir düzine NATO müttefikleriyle toplanmıştır. (NATO Cooperative Cyber Defence Centre of Excellence, 2017). Temmuz 2015'te Estonya; içerisinde İngiltere, Güney Kore, İsrail ve Yeni Zelanda'nın bulunduğu dünyanın önde gelen resmi siber ittifakının kurucu üyesi olmuş ve bu ittifaka göre birbirinden farklı ancak gelişmiş ülkeler birbirlerinin sunucularını güvenli bir şekilde barındırmayı kabul etmiştir. "Digital Five" olarak adlandırılan bu ittifak bir yer veya coğrafya adını almaksızın siber bir ittifak olarak kurulmuştur (Ramishvili, 2016).

Siber uzayla ilgili bilinmesi gereken bir diğer mesele, tüm tehditlerin devlet destekli olmadığıdır. Bazı devlet-dışı aktörlerin gücü kullanma kapasitesi devletlerden daha etkili olabilmektedir. Bazı ülkeler, siber alanlarında kötü aktörlere karşı korkunç bir mücadele vermektedir. Örneğin Pakistan, bir siber suç merkezi haline geldi. Pak Cyber Pyrates (PCP), belki de en çok aktif olan Pakistan hacker topluluğudur ve yüzlerce Hindistan karşıtı saldırıda bulunmaktadır. PCP, 9 Ekim 2011 tarihli bir yazı ile Keşmir ve Filistin gibi devletler için yaptığı "Özgür Filistin, Özgür Keşmir" sloganında esas amacını bildirmiştir (Ahmad, 2012).

Görüldüğü üzere bütün bu stratejilere ve güç kullanımına rağmen özellikle büyük güçlerin siber alanda karşı karşıya kaldığı ciddi bir sorun var. O da şu ki; büyük ülkelerin altyapılarının siber alana aşırı derecede bağımlı hale gelmiş olması, bu ülkeler için dış veya iç güçler tarafından kolayca istismar edilebilir zayıflıklar yaratmaktadır. Bu da temel güvenlik açıklarının onlar için daha büyük bir sorun haline gelmesine sebep olmaktadır. Bunun yanında, siber alanda etki yaratmanın maliyeti oldukça düşük olduğundan küçük devletler siber alanda önemli bir etki yaratabilmekte ve bu durumda ABD, Rusya, Çin gibi büyük ve zaten güçlü olan devletlerin siber alanda istedikleri gibi hâkimiyetlerini sürdürmeleri pek de mümkün olmamaktadır (Nagy, 2012:15). Bunun sonucu olarak siber alanda güvenli bir ağ oluşturmak fazlasıyla zor olduğundan, iletişim daha az korumalı bir hal almaktadır. Dolayısıyla güvenlik açığından kaynaklı olabilecek herhangi bir saldırının niteliği çok daha kötü sonuçlar doğurabilecektir. Bu nedenle siber alanda ihtiyaç duyulan şey, düşmanın siber ayak izlerinin "görselleştirilmesini"

sağlayan bir yazılım, toplanan verilerin belirlenmesine yardımcı olan analitik araçlar ve bilgiyi yorumlama ve aktarmada yetenekli kişilerdir (Carafano, 2013).

Güç Kullanmanın Önünde Ortaya Çıkan Engeller

Siber alanda gücün sağlanabilmesi yalnızca devletlerin kapasitelerine ve becerilerine bağlı bir durum olarak algılanmamalıdır. Çünkü siber uzayda bir güç olarak sivrilebilme veya saldırıları caydırabilme noktasında bütün bu saydığımız nedenlerin dışında siber alanın doğası gereği de ortaya çıkan bazı engeller mevcuttur. Her şeyden önce siber uzayda düşmanı silahsızlandırmak ya da yok etmek ya da etkili bir şekilde karşı-kuvvet stratejileri kullanma yeteneği sınırlıdır. Dolayısıyla siber alanda caydırıcılık mümkündür ancak bir saldırı kaynağının atfedilmesi sorunları nedeniyle zorluklar meydana getirir. Bir devletin siber alanda gücünü arttırması veya saldırıları caydırabilmesinin önünde engel olarak beliren üç faktör vardır. Bunlar; asimetri, gizlilik ve süper güçlendirme unsurlarıdır. Ortaya çıkan bu engel ve zorlukları bir siber güç gösterisi örneği olan 2007'de Rusya'nın Estonya'ya saldırısı üzerinden değerlendirmek daha açıklayıcı ve anlaşılır olacaktır (Guzman, 2017).

- ***Anonimlik (Atıf Sorunu):*** Anonimlik, savunmacı için oldukça büyük bir engel olarak karşımıza çıkmaktadır. Patrick Morgan'ın altını çizdiği kimlik ve motivasyon unsurlarının bilinmezliği, verilecek mesajın doğruluğu konusunda da engel teşkil etmektedir. Yani siber uzayda saldırıyı kimin gerçekleştirdiğini öğrenmek için birine atıf yapmak veya saldırganın niyetini tespit etmek oldukça zordur (Graham, 2010:104). Ancak saldırının niteliği ve buna verilecek tepki önemli bir aşama olduğu için istihbarat kapasitesi ve kaynakları olan ulus devletler bile kendilerine yönelik bir saldırıya doğrudan atıfta bulunmak için doğrudan doğruya yetki sahibi olamazlar (Schmitt, 2011:570). Estonya örneğine baktığımızda saldırının hala Rusya tarafından yapılıp yapılmadığı şaibeli bir durumdur. Bu yüzden anonimlik faktörü burada önemli rol oynamıştır (Nye, 2010:10).
- ***Asimetri:*** Zayıf tarafın daha güçlü tarafa karşı onun zayıf taraflarından da istifade ederek farklı taktik veya rastgele yöntemlerle yürüttüğü mücadele olarak adlandırılabilir. Örneğimiz bağlamında baktığımız zaman; uzmanlara göre Rusya Estonya'ya karşı siber bir saldırı gerçekleştirmiş olsa bile bu alanda Estonya için meydan okuyabileceği bir alan bırakmayabilir. Bu durumda Estonya, Rusya'ya herhangi bir saldırı gerçekleştirmek istese bile Rusya Estonya için bu saldırıyı gerçekleştirebileceği ortamı ortadan kaldırmış olabilir. Bu da siber alanın asimetrisini ortaya çıkarır (Betz, 2012:695).

- ***Süper Güçlendirme:*** Estonya saldırıları, internet üzerinde var olan süper yetkili aktörlerin nasıl oluştuğunu göstermektedir. Her ne kadar Estonya, bu saldırının Rusya tarafından gerçekleştiğinden emin olsa da bu konuda yalnızca Rus kökenli bir Estonyalı hüküm giymiştir. Bu da, yalnızca bir kişinin (bireyin) devlet kapasitesinde bir saldırı gerçekleştirerek siber alanda nasıl güç sahibi olabileceğini göstermiştir. Bu durum, hem devletin gücünün sarsılması konusunda hem de rakiplerin caydırılması konusunda büyük sorunlar yaratmaktadır (Reinbold, 2010). Zira bir devleti caydırmak veya bir devletle rekabet etmek bu denli zor iken, "bireylerle" baş etmek imkânsız görünmektedir (Goodman, 2010:113).

Estonya'nın arkasında ABD ve Avrupa ülkeleri olduğundan, Rusya'nın saldırısından en az zararla çıkabilmeyi başardı. Ancak siber saldırılar yalnızca Estonya gibi sınırlı alanlara yayılabilen küçük ülkelerle sınırlı kalmamakta ya da bu şekilde geçici zararlar vermemektedir. Aksine büyük güçler siber saldırılara karşı daha savunmasız durumdadırlar. Dolayısıyla büyük güçlerin uğradığı saldırıların neticesi çok daha büyük hasarlarla sonuçlanabilir. Asya ve Avrupa gibi bölgeler bilgi ağlarına güvenirken, ağlarında oluşabilecek hasarlara karşı oldukça savunmasız görünmektedirler. Dolayısıyla siber saldırı için kullanılan araçların artması siber uzayda kötü niyetli aktörlerin de teknik kapasitesini arttırmakta ve bu durum siber alanda savunmasızlıkların yükselmesine neden olmaktadır.

Devlet – Devlet-dışı Aktör Arasında Güç Dağılımı Tartışması

Uluslararası ilişkilerde realist paradigma devletler arasında itici bir güç olarak gücün dağılımına odaklanır. Realistler, dünya siyasetini anarşi koşulları altında devletlerarasındaki mücadeleler olarak nitelendirerek devletlerin güvenliklerini en üst düzeye çıkararak hayatta kalmayı garanti altına aldıklarını savunmaktadırlar. Devletler kendilerini korumak için daha yüksek bir otoriteye güvenemediğinden, nihai olarak diğer devletlerin saldırılarından kendilerini korumak için *self-help* denen kendi çabalarıyla hayatta kalma stratejisine bağlıdırlar. Realizm, uluslararası davranışları belirlemekte devlet dışı aktörlerin rolünü kabul ederken, bu aktörlerin devletlerin ve devlet çıkarlarının uluslararası siyasette önceliğine halel getirmediğini vurgulamaktadır (Walt, 1997:931).

Bir devletin egemenliğini askeri güç kullanarak kontrol etme yetkisi, konvansiyonel (askeri) araçları inşa etme ve onları kullanabilme yetkisine sahip olmak demektir. Bu yetenek genellikle

devletlere aittir ve bireyler bu tür özel araç ve ekipmanları tasarlayıp üretme konusunda bilgi ve kapasiteye sahip değildir. Fakat söz konusu siber alan olduğunda bir birey siber altyapıyı oluşturan bazı sistem ağlarını kullanarak bir bölgeyi kontrol etme konusunda bilgi ve yeteneğe sahip olabilir. Dolayısıyla bu durum doğrudan bireyleri, dolaylı olarak da devlet dışı aktörleri güçlendirir. Ancak bunlar yalnızca devlet-dışı aktörleri değil, bizatihi devletin kendisini de güçlendirebilir. Bunun kanıtı olarak devletlerin bugüne kadar hiçbir izole siber saldırıya atfedilmemiş olması gösterilebilir. Böyle bir durumda uluslararası hukuk, bir devletin durdurulması veya caydırılması için yararlı olmayacaktır (Schmidt, 2016:36). Bu durumda herhangi bir siber saldırı eyleminde bulunmayı planlayan devletler kimliğin ortaya çıkarılması sorunundan yararlanacaklardır. Ancak bu devlet güçlenmesinin arka planında da bir çelişki söz konusu olabilmektedir. Çünkü saldırıda gizlilikten, bilinmezlikten yararlanan devlet, bir operasyonu gizli bir şekilde yürütmek istediğinde operasyonun gerçekleşmesi safhasında bir devlet dışı aktörle işbirliği yapabilir veya direkt olarak saldırıyı ona yüleyebilir. Bu da devletin devlet dışı aktörleri kendi eliyle güçlendirmesi anlamına gelecektir.

Siber alan konusunda temel argümanlardan biri, teknolojik gelişmenin, devletten daha etkili olabilecek aktörlerin çeşitlendirilmesine ve bununla bağlantılı olarak güç yapılarında bir değişime yol açtığıdır. Bu iki merkezi ve birbirine bağlı gelişme, siber uzayla beraber uluslararası sistemde var olan güç ve gücün yeniden dağılımındaki değişimin doğasını ortaya koymaktadır. Niteliğin değişen doğası, bilgi teknolojilerinin giderek artan öneminin bir sonucu olarak görülmektedir. Eğer bir devlet siber bilgiye sahipse, onu yürütmek için geliştirmek, icat etmek veya ortaya çıkarmak zorunda değildir. Çünkü siber gücü kullanma maliyeti sıfıra yakındır. Bu durumda siber gücü edinmek veya geliştirmek, geleneksel bir askeri gücü geliştirmekten ve üretmekten daha ucuza mal olacaktır. Fakat burada devletler açısından bazı problemler ortaya çıkacaktır. Bu problemlerden en önemlisi, bu siber gücün devlet dışı aktörlerin de elinde olabileceği gerçeğidir. Bu nedenle, geleneksel olmayan şiddet yöntemleriyle daha az masraflı saldırıların devlet-dışı aktörler tarafından gerçekleştirilmesi kaçınılmaz bir hal almaktadır. Üstelik siber alanın saldırı kaynağında yarattığı atıf istismarı göz önüne alındığında bu ihtimalin tırmanması daha kolay hale gelmektedir (Choucri, 2012:4). Bunun dışında siber alanda uzaklığın olmaması, kapsadığı alan bakımından bir sınırlama olmaması, hedeflerin fiziksel alana ihtiyaç duyulmadan gerçekleştirilebilmesi ve geleneksel zaman kavramının yerini anlık zamanlara bırakması sebebiyle aktörlere daha rahat olabilecekleri bir ortam sağlar (Libicki, 2007:276).

Schmidt ve Cohen gibi yazarlar siber uzayı, devlet dışı grupları devlete karşı güçlendiren bir araç olarak tanımlamaktadır. Schmidt ve Cohen siber alanda, potansiyel kazananlar ve kaybedenler arasında yapılan bir yarışmanın varlığından söz etmektedirler. Bu durumda, küçük ve otokratik rejimler, rejim istikrarı için uğramış oldukları tehdidi azaltmaya çalışmaktadır. Fakat öte yandan, siber teknolojinin mevcut yapılandırmasında en çok fayda sağlayacak olan tarafın, Batı'nın büyük ve demokratik devletleri olduğunu savunmaktadırlar (Schmidt ve Cohen, 2010:75-86). Murphy ise, "erdemsiz" kimlik tabanlı ulus-ötesi grupların kamusal alanda olabilecek etkisini şöyle değerlendirmektedir: Daha "erdemli" sivil toplum grupları gibi, erdemsiz gruplar da siber teknoloji tarafından güçlendirilmektedir."(Murphy, 2009:138-139). Drezner ise birçok yazarın aksine devlet otoritesinin azalmadığını ve uluslararası siber yönetişimdeki sonuçların sistemdeki en güçlü ülkelerin çıkarları tarafından belirlendiğini savunmaktadır (Drenzner, 2004:480).

Bu konudaki en uç bakış açısı, "küresel köyler"in ve devlet-dışı aktörlerin ulus devleti tamamen ortadan kaldıracağı fikridir. John Perry Barlow'un 1996'da yayınladığı bağımsız bir siber uzayın manifestosu, yeni bilgi ve iletişim teknolojilerinin (BİT) özgür pazarının hükümet müdahalesi olmadan gelişmesine izin verdiği ve hükümetlerin halk üzerinde herhangi bir güce sahip olmadığı ütopik bir dünyayı imgeleştirmektedir (Barlow, 1996). Ayrıca burada coğrafi konum yerine ortak inanç ve değerler önem taşımaktadır. Burada seçilmiş bir hükümetten, otoriteden ve yaptırımdan bağımsız bir alanda konuşlanmış olan bir topluluktan söz edilmektedir (Kreiss, 2010). Barlow gibi düşünürler bilgi devrimini, kaçınılmaz ve geri döndürülemez biçimde yaşamın her alanını dönüştüren teknolojik bir sıçrama olarak görmektedir (Toffler, 1993). Bazı tahminlere göre gelecekte artan ölçüde, devlet dışı aktörlerin kendilerini devlet kontrolünden kurtarmaları ve bağımsız bir rol oynamaları beklenmektedir. Aynı zamanda bağımsız bir rol oynamakla kalmayıp daha fazla güç kullanma kapasitesine sahip olabileceklerdir. Örneğin; kendi yasalarını yapacak, kendi adalet sistemlerini geliştirecek, kendi vergilerini alacak ve hatta kendi paralarını basmaya başlayacaklardır (Joey, 2014).

Bu tür radikal fikirler kısa vadede uygulanabilir olmasa da, devletin uluslararası meselelerde merkezi aktör olarak öncelikli konumuna rakip olarak çıkabilmektedir. Siber, devletin ana görevlerinden ikisi olan güvenliği ve ekonomik refahı sağlama rolünü tehlikeye atarak devleti bu rollerinden vazgeçmeye zorlamaktadır. Örneğin devletler, siber savaş ve siber terörizm tehditlerine karşı güvenliği sağlamakta zorluk çektiğinden ve ekonomik faaliyetler giderek devletlerin sınırlarını aşmaya başladığından, devletlerin onları güvence altına alıp kontrol etme

yetenekleri de azalmaya başlamıştır. Siber nedeniyle, çok uluslu şirketler (ÇUŞ) ve bazı sivil toplum örgütleri (STK) gibi bir coğrafya tarafından sınırlandırılmayan uluslararası aktörler, devletlerin taleplerini dikkate almaksızın uluslararası alanda istedikleri gibi hareket edebilmektedirler.

Bu gibi radikal görüşlerin yanı sıra daha şüpheci gözlemciler, bilgi teknolojilerinin sınırlı ekonomik ve sosyal etkisine işaret etmekte ve değişim sürecinin evrimsel niteliğini vurgulamaktadırlar. Bu gözlemciler ayrıca toplumun ve siyasetin değişen doğasına teknolojik olarak deterministik bir yaklaşım getirmektedirler (Kitchin, 1998; Keohane, 1998). Örneğin Dunn'a göre siber alan BİT'i devlet dışı aktörlerin eline geçirse de, çoğunlukla bilgi avantajına sahip olan devlettir. Çünkü stratejik bilgi yaygın değildir ve devlet-dışı aktörler çoğunlukla bilgileri toplamak ve düzenlemek için gerekli olan yetenekler ve kaynaklardan yoksundurlar (Dunn, 2012:59).

Devlet ve siber uzaydaki kötü aktörlerin ilişkisine baktığımız zaman ise, Paul Rosenzweig, devletin kötü aktörlerle olan siber işbirliğinin her zaman kötü bir fikir olduğunu belirtmektedir. Ancak Rosenzweig'in aksine bu konuda Lin şöyle diyor: "Kötü aktörlerle işbirliği yapmak hep kötü bir fikir olsaydı, düşmanlarla asla anlaşma yapmazdık." Lin bu sözünü ise düşmanlarla yapılan anlaşmalarla örnekleyerek desteklemiştir. Lin'e göre böyle bir durumda silahlı çatışma yasalarında herhangi bir anlaşma, silah kontrol anlaşmaları veya deniz kanunları olmayacaktı (Lin, 2017).

Görüldüğü üzere siber alana ilişkin üç ana tema üzerinde durulmaktadır. Bunlar; atıf-kaynak ya da saldırıyı yapanı belirleme sorunu, devlet-iktidar siyasetinin rolü ve hem hükümet hem de özel sektörün sorumluluklarındaki değişimdir (Kostadinov, 2013). İki temel çatışma, gücün yeniden dağılımı üzerinde tartışmalara yol açmaktadır. Birincisi, bilgi devriminin, STK'lar ve aktivistler gibi uluslararası aktörlerin yeni biçimlerini güçlendirdiği ve dolayısıyla devletin uluslararası sistemdeki en büyük aktör olması fikridir. İkincisi ise, küresel bir elektronik pazarın ortaya çıkmasının kaçınılmaz olarak, şirketlerin ekonomik sınırlarını yok ettiğini ve bununla birlikte devletin ekonomi direğinin çöküşünün gerçekleşmiş olduğu iddiasıdır (Rothkopf, 1998:211). Geleneksel olarak, özel sektör ulusal güvenlik araçlarını geliştirir ve hükümet bu araçları kullanarak çalışır. Fakat şu anda özel şirketler, ülkeleri bir başka ulus devletin eylemlerine maruz kaldıklarında ulusal güvenlik giderleri konusunda sorumluluk sahibi olmaya başlamıştır. Bu zaten olması gereken bir durumdur çünkü siber alanda ayakta kalabilmek için

kamu-özel arasında istihbarat ve bilgi alışverişi olmalıdır. Çünkü bu durum, hükümetin daha gizli bir bağlamda çalışmasını ve şirketlerin daha fazla paylaşımda bulunmasını gerektirir. Bugün az sayıda şirket, Devlet Güvenliği Departmanı ile veri paylaştığından dolayı bazı uzmanlara göre bu durum ele alınması gereken ciddi bir konu olarak görülmektedir (The Cipher Brief, 2017).

Sonuç

Bilgi devrimi, mevcut geleneksel askeri yeteneklerin yanı sıra stratejik dünyadaki bilgilerin önemini önemli ölçüde artırdı ve bilgi, savaşta kilit unsur olmaya başladı. Edward Snowden, siber-politiğin uluslararası ilişkilerin incelenmesinde "yüksek politika" konusu haline geldiği hususunda bir fikir birliğinin bulunduğunu iddia etmektedir (Ralston, 2014:2). Nazli Choucri ise siberi 'düşük politika' ile 'yüksek politika' arasındaki ilişkinin bir meselesi olarak görmektedir. Yani Choucri siberi; siber- politik ve siber güvenlik ile uluslararası politika ve ulusal güvenlik arasındaki kritik bir nokta olarak görmektedir (Choucri, 2012:3). Gerçekten de internet, fiziksel bir çerçevede mantıksal yapı taşları ve etkileşim aracılığıyla “katmanların" her biri için gerçek siyasi sonuçlar doğurmaktadır.

Bu doğrultuda siberin yeni çatışma biçimlerine yol açtığı görülmektedir. Siber alanda savaş kayıplarına maruz kalma olasılığının düşük olması, çatışmaya girme maliyetinin düşük olması ve fiili savaşçıların kimliklerini gizleyebilme becerisi nedeniyle savaş açmak ya da saldırıda bulunmak çok daha kolay hale geldi. Savaş alanının insan algısını ve sanal alanı kapsayacak şekilde genişlemesi, çatışmalarda devlet-dışı aktörlerin daha fazla yer almasına sebep oldu. Dolayısıyla devletler yumuşak gücün eşit olmayan dağılımının bir sonucu olarak ortaya çıkacak olası güvenlik tehditlerine işaret etmek zorunda kalacaklardır.

Hâlihazırda ekonomik sıkıntı çeken ve siyasi ve kültürel yabancılaşmaya maruz kalan ülkeler, bölgeler ve çeşitli grupların, siber alanın faydalarını kolayca hissetmeleri pek muhtemel değildir. Fakat gelişmiş ülkeler, bilgi teknolojisi tarafından kendilerine tanınan fırsatlardan istifade ederken; altyapılarını bu teknolojiye angaje ettikleri durumda rakiplerinin saldırı ve tehditlerine daha açık bir konuma geldiklerini de göz önünde bulundurmak zorundadırlar. Zira bilgi teknolojisine en fazla sahip olan devletler, saldırıya en açık olan devletlerdir. Bu nedenle özellikle bu alanda daha güçlü olan devletlerin güvenlik risklerini minimize etmek için çabalaması gerekmektedir. Ancak güvenlik risklerinin azaltılması, yalnızca çok taraflı

işbirliğinin artırılmasını değil, aynı zamanda bilgi sistemine sahip olan devlet dışı aktörlerle, özel sektördeki kişilerle, marjinal gruplarla, devletlerle ve bölgelerle olan ilişkinin arttırılmasını gerektirmektedir (Dunn, Hensel ve Mauer, 2007:12).

Esas olarak siber, ülkeleri birbirine yakınlaştırmıştır. Çünkü askeri güce dayalı geleneksel fetih anlayışı, çevre, ordu, sermaye gibi faktörler sanal devlet için değersizdir. Bu fikrin en dikkat çekici yönü, nihai olarak bu devletlerin bilgi kaynakları için rekabet edeceği fikridir. Bugünün gelişmiş devletlerinin artık siyasal hâkimiyet için mücadele etmek yerine, küresel bilgiye ulaşmak için mücadele edeceği gibi görüşler de mevcuttur. Bu görüşe göre siber alan özellikle toprak faktörünü ortadan kaldırdığı için devletler ek topraklara ihtiyaç duymamakta ya da bunu arzulamamaktadır.

KAYNAKÇA

Ackerman, S. and S. Thielman. (2016). US Officially Accuses Russia of Hacking DNC and Interfering with Election. https://www.theguardian.com/technology/2016/oct/07/us-russia-dnc-hack-interfering-presidential-election (Erişim Tarihi: 21.08.2017).

Ahmad T. (2012). Pakistani Cyber Armies Hacking Indian Websites, Using Twitter, Facebook and YouTube to Cause Ethnic Conflicts in India. http://cjlab.memri.org/uncategorized/pakistani-cyber-armies-hacking-indian-websites-using-twitter-facebook-and-youtube-to-cause-ethnic-conflicts-in-india/ (Erişim Tarihi: 18.08.2017).

Aydın, M. (2004). Uluslararası İlişkilerin 'Gerçekçi' Teorisi: Kökeni, Kapsamı, Kritiği. *Uluslararası İlişkiler Dergisi*. Cilt 1. Sayı 1.

Bendiek, A. (2016). Making States Responsible for Their Activities in Cyberspace: The Role of the European Union. https://www.cfr.org/blog/making-states-responsible-their-activities-cyberspace-role-european-union (Erişim Tarihi: 30.08.2017).

Betz, D. (2012). Cyberpower in Strategic Affairs: Neither Unthinkable nor Blessed. *The Journal of Strategic Studies*. Vol 35, No 5.

Boeke, S. (2016). Who Determines the Cyber Security Agenda?. *Journal of Security and Global Affairs*. No 1.

Buchan, R. (2016). Special Issue: Non-State Actors and Responsibility in Cyberspace: State Responsibility, Individual Criminal Responsibility and Issues of Evidence. *Journal of Conflict and Security Law*. Vol 21, No 3.

Carafano, J. J. (2013). Fighting on the Cyber Battlefield: Weak States and Nonstate Actors pose Threats. http://www.heritage.org/defense/commentary/fighting-the-cyber-battlefield-weak-states-and-nonstate-actors-pose-threats (Erişim Tarihi: 18.09.2017).

Carr, E. H. (1946). The Twenty Years' Crisis, 1919–1939: An Introduction to the Study of International Relations. Oxford University Press.

Castells. M. (1996). *The Rise of the Network Society*. Oxford: Blackwell Publishers. ,

Choney, S. (2013). New York Times Hacked, Syrian Electronic Army Suspected. https://www.nbcnews.com/technology/new-york-times-hacked-syrian-electronic-army-suspected-8c11016739 (Erişim Tarihi: 04.10.2017).

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

Craig, A. and B. Valeriano. (2016). Conceptualising Cyber Arms Races. *8th International Conference on Cyber Conflict: Cyber Power*.

Çelik, M. (2015). Siber Ordu Kurmak İçin Devletler Özel Sektör ile Çalışıyor. *TMMOB Bilgisayar Mühendisleri Odası Dergisi*. Sayı 5.

Drezner, D. W. (2004). The Global Governance of the Internet: Bringing the State Back In. *Political Science Quarterly*. Vol 199, No 3.

Dunn, M. (2012). *Information Age Conflicts Myriam Dunn A Study of the Information Revolution and a Changing Operating Environment*, Zurich: Zürcher Beiträge. http://www.css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/ZB_64.pdf (Erişim Tarihi: 21.08.2017).

Dunn, M., S. F. Krishna-Hensel and V. Mauer. (2007). *Power And Securıty In The Informatıon Age: Investigating the Role of the State in Cyberspace.* Ashgate Publishing.

Gady, F. (2011). From the Middle Ages to the Cyber Age: Non-State Actors. http://www.huffingtonpost.com/franzstefan-gady/from-the-middle-ages-to-t_b_818650.html (Erişim Tarihi: 28.08.2017).

Gibson, W. (1984). *Neuromancer*. Ace Books.

Gomez, M. A. (2010). Identifying Cyber Strategies vis-a-vis Cyber Power. http://cybersummit.info/sites/cybersummit.info/files/Identifying%20Cyber%20Strategies%20vis-a-vis%20Cyber%20Power.pdf_Miguel%20Gomez.pdf (Erişim Tarihi: 07.09.2017).

Graham, D. E. (2010). Cyber Threats and the Law of War. *Journal of National Security Law and Policy*. Vol 87. No 4.

Grohe, E. (2015). The Cyber Dımensıons of the Syrıan Cıvıl War: Implications for Future Conflict. *The Johns Hopkıns Unıversıty Applıed Physıcs Laboratory.* Vol 14. No 7.

Guzman, G. (2017). Cyberpower – the Great Equalizer: Estonian Cyberpower Development. https://www.iapss.org/shop/budapest/uploads/2512_guzman_g_cyberpower_the_great_equalizer_03_2017_politikon_ela.pdf (Erişim Tarihi: 15.10.2017).

Guzzini, S. (2001). The Enduring Dilemmas of Realism in International Relations. *Copenhagen Peace Research İnstitute*.

Gücüyener, A. (2016). 21. Yüzyılda "Siber" Rekabet: Yeni Hedef Kritik Altyapılar mı?. https://www.linkedin.com/pulse/21-y%C3%BCzy%C4%B1lda-siber-rekabet-yeni-hedef-kritik-m%C4%B1-ayhan-gucuyener (Erişim Tarihi: 19.08.2017).

Haley, C. (2016). A Theory of Cyber Deterrence. http://journal.georgetown.edu/a-theory-of-cyber-deterrence-christopher-haley/ (Erişim Tarihi: 01.09.2017).

Hart, J. (1976). Three Approaches to the Measurement of Power in International Relations. *International Organization*. Vol 30. No 2.

Hensel, S. F. Krishna. (2007). Cybersecurity: Perspectives on the Challenges of the Information Revolution. Myriam Dunn Cavelty, Victor Mauer, *Power and Security in the Information Age Investigating the Role of the State in Cyberspace.* Ashgate Publishing.

Jensen, E. T. (2012). Cyber Deterrence. *Emory International Law Review*. No 26.

Joey, S. (2016). The Role of Non-state Actors in International Relations. http://www.academia.edu/5124220/The_Role_of_Non-state_Actors_in_International_Relations (Erişim Tarihi: 05.09.2017).

Kennan, G. F. (1966). *Realities of American Foreign Policy*. New York: The Norton Library.

Keohane, R. O. and J. S. Nye. (1998). Power and Interdependence in the Information Age. *Foreign Affairs*. Vol 77. No 5.

Kitchin, R. (1998). Cyberspace: *The World in the Wires.* Chichester: Wiley-Blackwell.

Kostadinov, D. (2013). The Attribution Problem in Cyber Attacks. http://resources.infosecinstitute.com/attribution-problem-in-cyber-attacks/#gref (Erişim Tarihi: 11.08.2017).

Kreiss, D. (2010). A Vision of and for the Networked World: John Perry Barlow's A Declaration of the Independence of Cyberspace at Twenty. https://danielkreiss.files.wordpress.com/2010/05/kreiss_barlow202.pdf (Erişim Tarihi: 18.10.2017).

Libicki, M. (2007). *Conquest in Cyberspace National Security and Information Warfare*. Cambridge.

Lin, H. (2017). On Cooperating with Bad Actors in Cyberspace. https://www.lawfareblog.com/cooperating-bad-actors-cyberspace (Erişim Tarihi: 17.09.2017).

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

Marmon, W. (2011). Main Cyber Threats Now Coming From Governments As "State Actors". https://www.europeaninstitute.org/index.php/136-european-affairs/ea-november-2011/1464-main-cyber-threats-now-coming-from-governments-as-state-actors (Erişim Tarihi: 03.10.2017).

Moravcsik, A. (1997). Taking Preferences Seriously: A Liberal Theory of International Politics. *International Organization.* Vol 51. No 4.

Morgenthau, H. J (1948). *Politics Among Nations: The Struggle for Power and Peace*. New York: Mc Graw Hill.

Murphy, E. C. (2009). Theorizing ICTs in the Arab World: Informational Capitalism and the Public Sphere. *International Studies Quarterly*. Vol 53. No 4.

Nagorski, A. (2010). Global Cyber Deterrence: Views From China, The U.S., Russia, India, and Norway. *East- West Institute*.

Nagy, V. (2012). The Geostrategic Struggle in Cyberspace between the United States, China, and Russia. *AARMS*. Vol 11. No 1.

Nye, J. S. (2010). Cyber Power. *Harvard Kennedy School,Belfer Center for Science and International Affairs*. No 18.

Nye, J. S. (2011). The Future of Power. *Los Angeles World Affairs Council*. http://www.lawac.org/speech-archive/pdf/1596.pdf (Erişim Tarihi: 10.10.2017).

Papp, D. S. and D. Alberts. (1997). The Impacts of the Information Age on International Actors and the International System. Papp and Alberts (eds). *The Information Age: An Anthology of its Impacts and Consequences*. CCRP Publication Series.

Parag, K. (2015). How Small States Prepare for Cyber-War. http://edition.cnn.com/2015/09/02/opinions/estonia-cyber-war/index.html (Erişim Tarihi: 05.10.2017).

Perlroth, N. (2013). Hunting for Syrian Hackers Chain of Command. New York Times.

Pihelgas, M. (2013). Back-Tracing and Anonymity in Cyberspace. Katharina Ziolkowski (ed.) *Peacetime Regime for State Activities in Cyberspace*. Tallinn: NATO CCD COE Publication.

Ralston, R. J. (2014). *Ontological Security: State Identity and Self-Image in the Digital Age.* Master of Arts in Political Science. Virginia Polytechnic Institute and State University.

Ramishvili T. (2016). Estonia's D5 Presidency. https://www.fpri.org/2016/01/estonias-d5-presidency/ (Erişim Tarihi: 09.10.2017).

Rauscher, K. F. (2011). First Joint Russian-U.S. report on Cyber Conflict. https://www.eastwest.ngo/idea/towards-rules-governing-cyber-conflict-0 (25.08.2017).

Reinbold, M. (2010). Superempowerment, Networked Tribes and the End to Business as We Know It. http://igniteshow.com/videos/super-empowerment-networked-tribes-and-end-world-we- know-it (Erişim Tarihi: 16.10.2017).

Rojansky, M. (2016). Russia and America's Cyber Deterrence Dilemma. http://nationalinterest.org/feature/russia-americas-cyber-deterrence-dilemma-18900 (Erişim Tarihi: 20.10.2017).

Rothkopf, D. J. (1998). Cyberpolitik: The Changing Nature of Power in the Information Age. *Journal of International Affairs*. Vol 51. No 2.

Schmidt, E. and J. Cohen. (2010). The Digital Disruption: Connectivity and the Power of Diffusion. *Foreign Affairs* Vol 89. No 6.

Schmidt, N. (2016). Super-empowering of Non-State Actors in Cyberspace. http://www.academia.edu/10088487/Super-empowering_of_Non-State_Actors_in_Cyberspace (Erişim Tarihi: 02.09.2017).

Schmitt, M. (2014). International Law and Cyber Attacks: Sony v. North Korea. https://www.justsecurity.org/18460/international-humanitarian-law-cyber-attacks-sony-v-north-korea/ (Erişim Tarihi: 24.08.2017).

Schmitt, M. N. (2011). Cyber Operations and the Jus Ad Bellum Revisited. *Villanova Law Review*. Vol 56.

Sheldon, J. B. (2011). Deciphering Cyberpower: Strategic Purpose in Peace and War. *Strategic Studies Quarterly*. No 18.

Sigholm, J. (2013). Non-State Actors in Cyberspace Operations. *Journal of Military Studies,* Vol 4. No 1.

Toffler, A. and H. Toffler. (1993). *War and Anti–War*: *Survival at the Dawn of the 21st Century.* New York.

Vandenberg, J. (2013). From Information Security to Cyber Warfare: Security to Cyber Warfare: Some Paradigm Shifts and Research Callenges. http://www.w-i-c.org/MWM2013/VanDenBerg_paradigmshifts.pdf (Erişim Tarihi: 15.08.2017).

Vlahos, M. (1998). Entering the Infosphere. *Journal of International Affairs*.

Volgy, T. J., K. Kanthak, D. Frazier, and R. S. Ingersoll. (2004). Structural Versus Relational Strength: The Cohesion of the G7 and the Development of the Post-Cold War International System. *Fifth Annual Pan European International Relations Conference*.

Walt, S. M. (1997). The Progressive Power of Realism. *The American Political Science Review*. Vol 91. No 4. 1997.

Wilhelmsen, V. C. R. (2014). *Soft War in Cyberspace: How Syrian Non-state Actors Use Hacking to Influence the Conflict's Battle of Narratives*. Master's Thesis - Political Science, Universıty of Oslo.

Winston, H. R. (2011). On the Nature of Military Theory. Charles Lutes (ed.). *Toward a Theory of Spacepower: Selected Essays*. Washington: NDU Press.

Yüksel, M. (2016). 3. Dünya Savaşı Öncesi Siber Güç Testinde Zayiat Büyük. http://www.yenisoz.com.tr/3-dunya-savasi-oncesi-siber-guc-testinde-zayiat-buyuk-makale-16757 (Erişim Tarihi: 01.10.2017).

Yüksel, M. (2017). Siber Savaş Oyunları. http://www.yenisoz.com.tr/siber-savas-oyunlari-makale-22631 (Erişim Tarihi: 09.09.2017).

Zacher, M. W. (1992). The Decaying Pillars of the Westphalian Temple: Implications for International Order and Governance. James N. Rosenau and Ernst-Otto Czempiel (eds). *Governance Without Government*: *Order and Change in World Politics*. Cambridge University Press.

ULUSAL SİBER GÜVENLİK STRATEJİ BELGELERİNDE İNSAN HAKLARI

Gül Nazik ÜNVER[*]

Özet

Bu çalışmada, siber alanda ABD, Türkiye, İngiltere, Almanya ve Hollanda'nın ulusal siber güvenlik strateji belgelerinde insan haklarının nasıl işlendiği, uluslararası insan hakları koruma

[*] Doktora Öğrencisi, Selçuk Üniversitesi, İİBF-Uluslar arası İlişkiler Bölümü, E-mail: gulunver@outlook.com