BÜYÜK GÜÇLERİN SİBER YÖNETİŞİM MÜCADELESİ

Sabri BAYRAK[♣]

Özet

Son yıllarda siber uzayla ilgili çalışmalar ciddi oranda artış göstermiştir. Bunun nedeni siberin her anlamda hayatın içine daha fazla müdahil olması ve ekonomi, sağlık eğitim ve savunma sistemlerine ve hatta bireylere kadar uzanan geniş bir yelpazede siber saldırıların ve karmaşıklığının gün geçtikçe artmasından kaynaklanmıştır**.** Anarşik yapısı ve sınırları belli olmayan siber alanda tıpkı fiziksel dünyada olduğu gibi saldırılar, ittifaklar, tehditler ve bunlara karşı önlemler bulunmaktadır. Bu durumdan Siber dünyanın bir aktörü olan devletler de etkilenmektedir. Diğer aktörlere göre bu alanda daha yeni oldukları için siber dünyada daha aktif olmak ve hatta sibere hükmetmek istemektedirler. Bu da siber güvenlik meselesini ortaya çıkarmaktadır. Fiziksel ortamda olduğu gibi siber ortamda da bir güvenlik meselesi ortaya çıkmaktadır. Bu güvenlik sorununu çözmek içinse siber yönetişim bir araç olarak ön plana çıkmaktadır. Siber yönetişim küresel yönetişimin yeni bir formu olarak siber dünyanın daha barışçıl, insan haklarına uyumlu ve daha az güvenlikçi yaklaşımlarla yönetilmesidir**.** Devletler siber dünyada bir yönetişim sağlamak yerine sibere hükmetmek ve bu alanda kendi çıkarlarını maksimize etmek istemektedirler. Bu da siber yönetişim sorununu ortaya çıkarmaktadır. Siberi kim yönetecek? Devletler mi diğer aktörler mi? Devletler yönetecekse bu hangi devlet olacak? Büyük güçler nasıl bir siber yönetişim istiyor? Bu makale temel olarak bu sorulara cevap aramak amacı ile yazılmıştır.

Anahtar Kelimeler: Siber Uzay, Siber Yönetişim, Siber Güvenlik

Cyber Governance Struggle among Great Powers

Abstract

In recent years, studies related to cyber space have increased significantly. This is due to the fact that cyberspace is more involved in life in every sense, and the seriousness and complexity of the number of cyber attacks in the economy, health education and defense systems, and even individuals, is becoming more and more problematic. In the anarchic and unclear cyber area, there are attacks, collaborations, threats and measures against them, just as in the physical world. This situation is affected by states that are an actor of the cyber world. Because they are weaker in this field than other actors, cyber worlds want to be more active and even to dominate. This raises the issue of cyber security. As in the physical environment,

♣ SÜ Uluslararası İlişkiler bölümü Yüksek Lisans Öğrencisi E mail: sabribayrak00@gmail.com

there is a security issue in the cyber environment. In order to solve this security issue, cyber governance comes to the fore as a tool. Cyber governance, as a new form of global governance, is to manage the cyber world with more peaceful, human rights-compliant and less secure approaches. Instead of providing governance in the cyber world, states want to dominate and maximize their interests in this area. This raises the problem of cyber governance. Who's going to run? States or other actors? If the States are to govern, which state will it be? What kind of cyber governance do great powers want? This article is basically written to look for answers to these questions.
Key Words: Cyberspace, Cyber Governence, Cybersecurity

Giriş

Siber uzay devletlerin devlet dışı aktörlerin ve bireylerin günlük yaşamlarını etkileyen bir olgu haline gelmiştir. Bu da siber uzayla alakalı çalışmaların artmasına sebebiyet vermiştir. Siber uzayla alakalı çalışmaların pek çoğu da siber güvenlik konusunda yapılmaktadır. Özellikle devletler sibere güvenlik açısından bakmaktadır. Yani küresel gündemde devletlerin siberle alakalı en önemli sorununu siber güvenlik oluşturmaktadır. Bunun nedeni ise ekonomi, sağlık eğitim ve savunma sistemlerine ve hatta bireylere kadar uzanan geniş bir yelpazede siber saldırıların sayısı ciddiyeti ve karmaşıklığı gün geçtikçe daha sorunlu bir hal almasından kaynaklanmaktadır. Yukarıda da belirtildiği üzere bu da siber uzayla alakalı çalışmaları arttırmaktadır. Anarşik ve sınırları belli olmayan siber alanda tıpkı fiziksel dünyada olduğu gibi saldırılar, işbirlikleri, tehditler ve bunlara karşı önlemler bulunmaktadır. Siber dünyanın bir aktörü olan devletler diğer aktörlere göre bu alanda daha zayıf oldukları için siber dünya da daha aktif olmak ve hatta sibere hükmetmek istemektedirler. Bu da siber güvenlik meselesini ortaya çıkarmaktadır. Fiziksel ortamda olduğu gibi siber ortamda da bir güvenlik meselesi ortaya çıkmaktadır.

Özellikle 2000'li yılların başından beri siber uzay devletler arasındaki ilişkilerde daha fazla etkili olmaya başlamıştır. Ekonomik, askeri ve siyasi güçlerini maksimize etmeye çalışan devletler bunlara ilave olarak siber alanda da güçlerini maksimize etmek istemektedirler. Yani fiziksel alanda olduğu gibi siber alanda da devletler arasında mücadele ve rekabet oluşmuştur. Gelişen teknoloji ile birlikte büyük güçlerin mücadelesinde siber gücün etkili kullanımı vazgeçilmez bir hal almıştır(Nagy, 2012). Devletler siber alanda sadece mücadele etmemekte, aynı zamanda siberi kontrol etmek istemektedirler. Siberi kontrol etmek içinde siber yönetişimi bir araç olarak kullanmaktadırlar.

Siber yönetişim küresel yönetişimin yeni bir formu olarak siber dünyanın daha barışçıl, insan haklarına uyumlu ve daha az güvenlikçi yaklaşımlarla yönetilmesidir. Avrupa Konseyi Siber Yönetişim Stratejisinde siber yönetişimin amacı şu şekilde tanımlanmıştır. Siber yönetişimin amacı, devletin internetle alakalı politikalarının hukukun üstünlüğüne, demokrasiye, ve insan haklarına göre düzenlemesini sağlamaktır(CoE, 2016:8). Fakat devletlerin siber yönetişimden anladığının yukarıda bahsedilen husus olmadığını pek çok devlet faaliyetinde görebilmek mümkündür. Zira devletler siber dünyada bir yönetişim sağlamak yerine sibere hükmetmek ve bu alanda kendi çıkarlarını maksimize etmek istemektedirler. Özellikle büyük devletler bu hususta daha etkili olmaktadır. Uluslararası siber güç sahibi olan Rusya, Çin ve ABD bu konuda ön plana çıkmaktadır. ABD soğuk savaş bittikten sonra diğer alanlarda olduğu gibi siber alanda da elde ettiği siber uzaydaki görece üstünlüğünü devam ettirmek istemektedir. Diğer yandan Çin ve Rusya ise siber alandaki batının zayıflığını(ABD hariç) avantaja çevirerek etkili olmaya çalışmaktadır. Bu da siber yönetişim sorununu ortaya çıkarmaktadır. Siberi kim yönetecek? Devletler mi diğer aktörler mi? Devletler yönetecekse bu hangi devlet olacak? Büyük güçler nasıl bir siber yönetişim istiyor? Bu makale temel olarak bu sorulara cevap aramak amacı ile yazılmıştır.

Siber Yönetişim Tanımı

Son zamanlarda yönetişim ve iyi yönetişim kavramları literatür de yaygın bir şekilde kullanılmaya başlamıştır. Bu yaygın kullanımının aksine yönetişim kavramı yeni bir olgu değildir. Tarihi insanlık tarihi kadar eskidir denilse abartı olmayacaktır. Basit bir tanımlamayla yönetişim şu anlama gelmektedir: Karar alma sürecine alınan karardan olumlu ve ya olumuz olarak etkilenecek olanların bizatihi katılmasıdır(United Nations Escap, 2009). Yani Abraham Lincoln'ün demokrasi için yaptığı tanıma benzer bir tanım yönetişim içinde yapılabilir.[3]

İyi yönetişim ise yönetişimin daha ileri bir versiyonudur. İyi yönetişim temel olarak sekiz özelliğe sahip olması gerekmektedir. Bunlar, katılımcılık, fikir birliği, şeffaflık, duyarlılık, etkili ve verimli olmak, kapsayıcılık ve hukukun üstünlüğüdür. Ayrıca iyi yönetişim yolsuzluğun en aza indirilmesini hedef alır ve azınlık görüşlerini dikkate alarak toplumun

[3] Abraham Lincoln demokrasiyi halkın halk tarafından halk için yönetilmesi olarak tanımlamıştır. Yönetişim kavramı da buna benzer şekilde karar alma sürecine karardan etkilenenlerin katılmasını ifade etmektedir. Böylece daha katılımcı, daha şeffaf ve daha fazla hukukun üstünlüğüne dayanan bir yönetim şekli oluşturulması hedeflenmektedir.

içindeki en zayıf halkanın karar alma sürecine katılmasına olanak sağlar(United Nations Escap, 2009). Bütün bunların yapılabilmesi içinde yönetilenlerin yönetim sürecine katılabilmesi için kamuya açık objektif verilerle bilgi sağlanması gerekmektedir(Rotberg, 2014). Bunun için 1996 yılında dünya çapında iki yüzden fazla ülkenin yönetişim kalitesini ölçmek için dünya bankası tarafından finanse edilen yönetişim göstergeleri programı kurulmuştur(Kaufmann & Kraay, 2002). Bu gösterge, hangi ülkenin iyi yönetişim ilkelerine sahip olup olmadığını incelme fırsatı sunmaktadır.

Yönetişim kavramı tek bir olgudan ibaret değildir ve çeşitleri mevcuttur. Örneğin ulusal yönetişim, uluslararası yönetişim, yerel yönetişim ve şirket yönetişimi. Gelişen teknoloji ile birlikte bunlara bir de siber yönetişim eklenmiştir.

Siber yönetişim, siber uzayı yönetmek için düzenleyici ve prosedürsel kuralların oluşturulmasıdır. Siber yönetişim daha çok internet yönetişimi olarak isimlendirilmiştir. Ve iyi bir siber yönetişim için tıpkı iyi yönetişim için olduğu gibi belli başlı özelliklere ihtiyaç vardır. İyi siber yönetişim insan hakları normlarına dayanmalı, şeffaf olmalı, katılımcı ve hesap verilebilirlik özelliklerine sahip olmalıdır. Bütün bunlar iyi siber yönetişimin oluşturulması için temel özelliklerdir ve aşağıda iyi bir siber yönetişim için olmazsa olmaz üç ilke daha detaylı şekilde açıklanmıştır.

Şeffaflık

Siber yönetişimin sağlanabilmesi için karar verme süreçleri şeffaf olmalı ve karar vericiler kararlarından dolayı sorumlu tutulabilmelidir. Ayrıca yönetişim içinde yer alan hiçbir paydaşın resmi ve ya gayri resmi veto hakkına sahip olmaması gerekmektedir.

Katılımcılık

Siber yönetişim mekanizmaları oluşturulurken katılımcılık hususu dikkate alınmalıdır. Siber yönetişimin daha fazla katılımcıyı içermesi yönetişimin daha kolay sağlanmasına olanak sağlamış olacaktır.

İnsan Hakları

Fiziksel alanda olduğu gibi siber alanda da insan hakları normlarının olması siber yönetişim için gerekli olan özelliklerden biridir. Siber dünyanın belirsizliklerle dolu olması ve tehditlerin her geçen gün artması devletleri zayıflatmaktadır. Bu da insan haklarını korumakla

görevli devletlerin bu görevini yerine getirememesine neden olmaktadır. Siber alanda insan hakları ve hukukunun daha etkin hale gelmesi hem siber dünyada yönetişim kolaylığı sağlarken hem de devletlerin zayıflamasını engellemiş olacaktır(Marcus, 2015).

Yukarıda bahsedilen bu özellikler iyi siber yönetişimi sağladığı gibi diğer yandan insan haklarının gelişimine katkı sağlamaktadır(Mihr, 2014). Bütün bu özellikleri içinde barındıran siber yönetişim siber uzayın daha normatif daha katılımcı ve daha şeffaf olmasına katkı sağlamaktadır.

Siber Yönetişim Sorunu

Siber yönetişim uluslararası politikayı etkileyen en önemli sorunlardan biridir. Fiziksel alanda küresel iyi yönetişimin zorluklarını siber yönetişim konusunda da görmek mümkündür. Zira önceki sayfalarda da bahsedildiği üzere siber yönetişim küresel iyi yönetişimin ayrılmaz bir parçasıdır. Uluslararası ilişkilerin anarşik olması, mevcut uluslararası hukukun yetersizliği, insan hakları ve demokrasinin göz ardı edilmesi gibi küresel yönetişimin mevcut eksiklikleri iyi siber yönetişimin de önüne geçmektedir. Fakat siber yönetişimin tek sorunu bunlar değildir. Zira kendine has bir yapısı olan siber uzayı fiziksel alanda kullanılan kurallar ve kavramlarla yönetmeye çalışmak daha başka sorunlara neden olabilir. İyi bir siber yönetişim için devlet ve devlet dışı aktörleri içinde barındıran resmi ve gayri resmi mekanizmalar ve kurallar oluşturulmalıdır(Almeida, 2016). Siber yönetişim konusunda literatürde üzerinde durulan iki temel mekanizma vardır.

Bunlardan ilki Joseph Nye tarafından oluşturulan rejim komplexi teorisidir. Joseph Nye bu teoride siber yönetişim için daha önce uluslararası ilişkilerde devlet davranışlarını açıklamak için kullandığı karmaşık karşılıklı bağımlılık teorisinden yararlanarak siberin karşılıklı bağımlılık teorisinde olduğu gibi kurumsal ve gücün eşit olarak dağıldığı ve prosedürleri olan bir sistem kurularak yapılabileceğini savunmaktadır. Fakat Nye sadece geleneksel kurallar ile siberin kontrol edilemeyeceğini de eklemiştir. Nye'a göre siber yönetişim için gerekli olan rejim, siberin hem teknolojik hem de siyasi yönünü birlikte ele almalı ve insan haklarını göz önünde bulunduran bir yaklaşım olmalıdır(Nye, 2014). Nye siber yönetişim için böyle bir rejim önerse de siberin fiziksel alandan farklı olduğunu ve her an her şeyin değiştiğini belirterek siberi yönetmek için kalıcı ve kesin çözüm getiren kuralların hiçbir zaman

oluşturulamayacağını da vurgulamıştır. Siber yönetişimi sağlamak için literatürde en çok üzerinde durulan ikinci mekanizma Birleşmiş Milletler İnternet Yönetişim Formudur.

Bu forum 2006 yılında Birleşmiş Milletler tarafından oluşturulmuştur. Bir tartışma platformu olarak İnternet Yönetişim Formu(IGF) çeşitli kişileri ve paydaş gurupları internet ve teknoloji ile ilgili iyi politikaları uygulamak be bilgi alışverişinde bulunmak için aynı masada bir araya getirmektedir. İnternet fırsatlarının nasıl en üst düzeye çıkarılabileceğini ve onların nasıl ele alınacağına dair ortak bir anlayış geliştirmiştir(IGF, 2018).

IGF ayrıca, gelişmekte olan ülkeler de dahil olmak üzere tüm ülkelerden paydaşlara internet yönetişimiyle ilgili tartışmalara katılma fırsatı vermekte ve kapasite oluşturulmasına katkıda bulunmakta, bu paydaşların mevcut İnternet yönetişim kurumlarına ve düzenlemelerine katılımlarını kolaylaştıracak bilgi ve beceriler geliştirmelerine olanak tanımaktadır(IGF, 2018).

Bu kurallar ve mekanizmalar dışında siber yönetişim sorununu aşmak için iki farklı yaklaşım ileri sürülmektedir. Bunlardan birincisi teknik ve dar yaklaşımdır. Bu yaklaşım siber yönetişimin teknik bir mesele olduğunu ve siber yönetişimle alakalı soruların teknik uzmanlar tarafından teknik yollarla çözülmesi gerektiğini savunmaktadır(Kurbalija, 2014). Bu yaklaşımı savunanlar siber yönetişimi daha çok ICANN, TCP, DNS gibi internet protokollerinin denetimine bırakarak siberi siyasetin zararlı etkilerinden korumak istemektedirler(Akyeşilmen, 2018).

İkinci yaklaşım siyasi ve geniş yaklaşımdır. Bu yaklaşım siber yönetişimi teknik bir konu olmasının yanı sıra siyasi ve sosyal yönü bulunan kapsamlı bir alan olarak görmektedir. Bu yaklaşıma göre iyi bir siber yönetişimin oluşturulabilmesi için devlet merkezci bakış açısının terk edilerek uluslararası ilişkilerin diğer aktörlerini(Sivil toplum kuruluşları ve çok uluslu şirketler gibi) de kapsayacak şekilde kurallar ve mekanizmalar oluşturulmalıdır.

Büyük Güçler ve Siber Yönetişim

2000'li yılların başından beri siber uzay devletler arasındaki ilişkilerde oldukça etkili olmaktadır. Ekonomik, askeri ve siyasi güçlerini maksimize etmeye çalışan devletler bunlara ilave olarak siber alanda da güçlerini maksimize etmek istemektedirler. Yani fiziksel alanda

olduğu gibi siber alanda da devletler arasında mücadele ve rekabet oluşmuştur. Gelişen teknoloji ile birlikte büyük güçlerin mücadelesinde siber gücün etkili kullanımı vazgeçilmez bir hal almıştır(Nagy, 2012). Özellikle uluslararası siber güç sahibi olan Rusya, Çin ve ABD bu konuda ön plana çıkmaktadır. ABD soğuk savaş bittikten sonra diğer alanlarda olduğu gibi siber alanda da elde ettiği siber uzaydaki görece üstünlüğünü devam ettirmek istemektedir. Diğer yandan Çin ve Rusya ise siber alandaki batının zayıflığını(ABD hariç) avantaja çevirerek etkili olmaya çalışmaktadır.

Büyük güçler siber alanda mücadele ederken diğer yandan siberin kullarının ve yönetim ilkelerinin olması gerektiğini dile getirmekteler. Siber uzayı daha normatif hale getirmek için siber yönetişimi savunurken ironik olarak siberde bir yönetişim platformu oluşturmaktan ziyade her bir gücün sibere hükmetmek istediği görülmektedir. Aşağıda ABD, Rusya ve Çin'in siber yönetişime bakışı ve siber alandaki faaliyetleri tek tek ülke bazında incelenmiştir.

ABD

Modern dünyada internetin gelişimi ve ABD'nin süper güç haline gelmesi arasında bir paralellik vardır. Soğuk Savaşın bitmesiyle süper güç olan ABD internet ve siberin gelişimine katkı sağlarken aynı zamanda bu gelişmelerden de çıkar elde etmiştir. Son yirmi beş yılda siber uzay ile alakalı bütün gelişmeler ABD'nin uluslararası politikadaki etkinliğinin temelini oluşturmuştur. Yani siber uzaydaki gelişmeler Amerika'nın ekonomik, sosyal ve siyasi meselelerinin ayrılmaz bir parçası olmuştur(The White House, 2018). Dünya çapında ABD, özellikle siber güvenlik politikası ve stratejisini geliştirmenin öncüsü olmuştur(Layne & Lee, 2001). Amerika Birleşik Devletleri internet yönetişimi konusunda çok taraflı yönetişim modeli olarak isimlendirilen bir modeli ön plana çıkarmaktadır. ICANN[4] bu modelin bir örneğidir. Bu modele göre internet hakkında karar alma ve uygulama sürecine hükümetlerin yanı sıra özel sektör ve sivil toplum kuruluşları gibi devlet dışı aktörlerinde katılması savunulmaktadır(Wallace, 2014). Fakat ICANN siber konularda yaptırım ve düzenleme yetkisi bulunmayan bir platformdur ve bu açıdan eksiktir. Örneğin ABD'deki herhangi bir mahkeme ve ya ABD yasaları ABD'nin kamusal çıkarlarını gerekçe göstererek ICANN'a politikalarını değiştirme konusunda baskı uygulayabilmektedir(Singh, 2016). Bu da ABD'nin ICANN gibi kuruluşları kullanarak siber alanda istediği politikaları yapma fırsatı elde

[4] ICANN dünyanın dört bir yanından internet paydaşlarının katılımı ile oluşturulan çok paydaşlı bir internet yönetişim organizasyonudur. Uluslararası internet yönetim organı olarak sorumluluğunu etkin ve verimli bir şekilde yürütebilmek için dünya çapında farklı internet paydaşları ile iş birliği yapmaktadır(ICANN).

etmesine neden olmaktadır. Bu durum ABD karşıtı Çin ve Rusya tarafından eleştirilmektedir. Diğer yandan ABD'nin uluslararası müzakerelere karşı duyarlılığı konusundaki artan ilgisi, yerel siber güvenliğin sağlanmasına yönelik çabaların yetersiz olduğunu göstermekte ve ABD bir kenarda oturmak yerine kendine zarar verdiğini düşündüğü siber sorunları müzakere yolu ile çözmeye çalışmaktadır. Zira bir siber saldırının - bilgisayara, iletişime, ulaşıma ve enerji ağlarına saldıran bilgisayar gücünün kullanılması - ekonomiyi bozabileceği, kritik altyapıları tahrip edebileceği veya askeri yetenekleri düşürebileceğine dair gerçek bir korku vardır(Segal, 2011). İnternet aslında başlangıçta sadece Amerika Birleşik Devletleri'ndeki küçük bir araştırmacı grubunun kullanımı ve rahatlığı için tasarlanmış olmasına rağmen bugün ABD için ciddi anlamda bir güvenlik sorunu olmuştur. Siber dünyada belirsizliğin çok fazla olması ABD gibi bir ülkenin bile kolaylıkla saldırılara maruz kalmasına sebep olmaktadır. Bu sebepten siber yönetişim konusu ABD için önemli bir konudur. ABD her ne kadar eleştirildiği üzere siber yönetişim kuralları ve ya mekanizmalar ile kendi çıkarlarını koruma çabası içinde olsa da bu mekanizmaların ve kuralların varlığı siber uzayda yönetişimin sağlanmasına katkı sağlamaktadır.

Rusya

Son on yıldır Rusya'nın dış politikası bir dizi konuda uluslararası fikir birliğine meydan okumaktadır. Bu meydan okuma siber uzayla alakalı konularda da kendini göstermektedir. Rusya siber konularda batı söylemini değiştirmek istemektedir. ABD'nin elinde bulundurduğu uluslararası internet ekosistemi rejimini çok yönlü hale getirmek için çalışmalar yapmaktadır. Rusya bunu yaparken hem bölgesel forumlarda hem de Birleşmiş Milletler de internet yönetişimi ve siber güvenlik politikalarını benzer düşüncelerle koordine etmeyi amaçlamaktadır.(Nocetti, 2015). Örneğin 2003 yılında internet ve bilgi güvenliği konusunda hükümetler arası bir uzmanlık gurubunun kurulmasını önermiştir. BM Genel sekreterliğine vermiş olduğu raporda, bu kurulmasıyla bilgi güvenliği konusunda çok taraflı ve uluslararası yeni bir aşamaya geçileceğini savunmuştur. Ayrıca bu gurubun uluslararası topluma bilgi güvenliği ile ilgili tüm konuları incelemek için eşit bir fırsat sunacağı belirtilmiştir. 2004 yılında kurulan bu gurup anlaşmazlıklar nedeniyle başarısız olmuş kendinden beklenileni karşılayamamıştır.

Rusya siber ile alakalı konularda böylesine kuruluşların oluşması için öncülük ederken diğer yandan da bazı devletlerin siber ile ilgili faaliyetlerinden rahatsızlığını dile getirmiştir. Rusya, özellikle ABD'nin siberi diğer egemen devletleri kendi dünya görüş ve değerleriyle alt etmek için kullanacağı bir araç olarak görmektedir. Fakat Rusya ABD'yi böylesine eleştirirken

kendisi de farklı davranmamaktadır. Güvenlik endişelerini bahane ederek ve daha fazla hiyerarşi savunarak, Rusya küresel siber konuların siyasallaşmasına katkıda bulunmakta ve siberi iç siyasi çıkarları doğrultusunda yeniden şekillendirmeye çalışmaktadır. Bu nokta da Rusya küresel siber yönetişime "neo Hobbes'çu" bakış açısı ile bakmaktadır. Yani siber ile alakalı konuların uluslararası anarşiyi güçlendirdiğini ve daha kaotik bir ortam oluştuğunu düşünmektedir. Siber ile alakalı konular artık sadece teknik bir mesele olmaktan çıkıp uluslararası politikayı derinden etkileyen yüksek politika haline dönüşmüştür. (Nocetti, 2015).

Yukarıda da bahsedildiği üzere Rusya siber yönetişime katkı sağlamak yerine onu daha sorunlu bir hale getirmektedir. Bunun en açık göstergesi yapmış olduğu siber saldırılardır. Bunlardan ilki Estonya saldırısıdır. Rusya 2007 yılında Estonya'ya karşı DDoS saldırılarını yapmıştır. Bu saldırı siber alanda yapılmış ilk büyük ölçekli ve koordineli saldırıdır. Bu saldırı ile Rusya bir yaklaşık olarak bir ay boyunca Estonya'nın internet sitelerini engellemiş uluslararası bağlantıları kapatmış ve internetle alakalı her şeyi kontrol altına almıştır(Connell & Vogler, 2017). İkincisi Gürcistan'a yapılan saldırıdır. 2008 yılında Rusya zombi bilgisayarlar ile Gürcistan'ın siber sistemine saldırı gerçekleştirmiştir(Markoff, 2008). Bu saldırı ile dönemin Gürcistan Cumhurbaşkanı Michael Saakaşvili'nin internet sitesi hedef alınmış ve yaklaşık yirmi dört saat boyunca site Rus hackerler tarafından kontrol altında tutulmuştur(Danchev, 2008). Yine bu saldırıdan çok kısa bir süre sonra 5 Ağustos 2008'de Osinform Haber Ajansı ve Osradio siber saldırıya uğramıştır. Rusya bu saldırıların arkasında başka kişilerin olduğunu belirtmiş ve suçlamaları reddetmiştir. Her ne kadar Rusya resmi söylemde bu saldırıları reddetse de saldırıların Rus Hükümetinin bilgisi ile yapıldığı uluslararası toplum tarafından bilinen bir gerçektir. Rusya Estonya ve Gürcistan'a karşı yapmış olduğu saldırılar ile her iki ülke üzerinde de baskı kurmak ve bu doğrultuda kendi çıkarlarını korumak istemiştir. Bir başka ifade ile Rusya siber gücünü bir caydırıcılık aracı olarak kullanmıştır. Sonuç olarak Rusya siber yönetişime katkı sağlamak ve siber uzayı daha normatif hale getirmek yerine onu kendi çıkarları doğrultusunda daha etkili şekilde kullanmaktan hiçbir zaman çekinmemiştir.

Çin

Çin dünyanın en fazla internet kullanışına sahip ülkesidir ve buna paralel olarak siber yönetişime aktif olarak katılmak istemektedir. Özellikle son on yılda siber yönetişim için yoğun bir küresel rekabet içine girmiştir(Cuihong, 2018). Örneğin bunun için Şubat 2014'te Siber İşler Merkezi Öncü Grubu Ofisi Kurulmuştur. Çin Devlet Başkanı Xi Jinping, bu ofisin

kurulmasındaki temel amacın internet güvenliği ve bilişim çalışmalarını farklı sektörler arasında yürütmek ve ulusal siber stratejileri hazırlamak üzere tasarlandığını belirtmiştir(Xin, 2017). Çin siber uzayla alakalı kurum ve kuruluşlarla bu alanda daha fazla etkin olmak istemektedir.

Çin mevcut uluslararası siber yönetişim rejimini çok fazla eleştirmekte ve siber yönetişimin ABD merkezli olmasından rahatsız olmaktadır(No, 2017). Bunun için küresel yönetişim vizyonunu geliştirmek adına yaptığı çalışmalar arasında internetle alakalı kendi vizyon ve uygulamalarını diğer ülkelere model olarak sunmakta bulunmaktadır. Örneğin siber yönetişime ilişkin 2017 Aralık ayında düzenlenen ve aralarında Apple ve Google'ın Ceolarınında bulunduğu Dünya İnternet Konferansı da Çin Devlet Başkanı Xi Jinping siber egemenlik olarak adlandırdığı bu projeyi desteklediğini açıklamıştır(Zaagman, 2018). Çin'in siber egemenlik kavramı iki temel ilkeye dayanmaktadır. Birincisi, Bir ülkenin bilgi alanında istenmeyen dış etkiler yasaklanmalıdır. Böylesi etkilerin yasaklanması ülke vatandaşlarının rejim tarafından zararlı olarak addedilen fikir ve düşüncelere maruz kalmasını engellemiş olacaktır. İkincisi ise, İnternet yönetimini değiştirmek ve daha normatif hale getirmek için Birleşmiş Milletler gibi forumların mevcut organlarına ek olarak akademisyenleri ve uluslararası şirketleri de içinde barındıran yeni organlar oluşturulmalıdır(Nagelhus & Gjesvik, 2017). Her ne kadar Çin siber egemenliği bu şekilde tanımlasa da ülkesinde internete erişim yollarını daima kontrol altında tutmuştur. Çin Hükümeti ve devlet kontrolündeki tüzel kişilikler internetin fiziksel omurgasına sahip olmuştur(Herold, 2011). Örneğin Çin sanal özel ağlar ve (TOR) The Onion Router gibi kompleks protokoller ile internet erişiminin kontrolünü sağlamaktadır(Choucri & Clark, 2013). Özellikle ülke içerisinde facebook, twitter ve google gibi uygulamaların kullanımı yasaklanmış bunlara alternatif uygulamalar geliştirilmiştir. Kısacası siber egemenlik söylemi siber uzayda politik kontrollere odaklanmakta ve Çin'in siber politikalarını meşrulaştırmaktadır. Diğer yandan küresel siber uzayın yönetimini devlet merkezci girişimlere indirgemektedir(Shen, 2016).

Sonuç

Siber uzayda büyük güçler arasındaki mücadele sürekli artmaktadır. Zira siber uzayda yaşanan gelişmeler devletlerin politikalarını doğrudan etkilemektedir. Bunun için fiziksel alanda olduğu gibi siber alanda da devletler arasındaki mücadele kaçınılmaz olmuştur.

Özellikle bu mücadele uluslararası ilişkilerin en önemli aktörleri olan Rusya, Çin ve ABD arasında daha yoğun şekilde yaşanmaktadır.

Soğuk Savaşın bitmesiyle birlikte tek süper güç haline gelen ABD bu üstünlüğünü siber alanda da devam ettirmiştir. Özellikle doksanlı yıllarda internetin gelişmeye başlaması ve siberin uluslararası ilişkilere dahil olmasında ABD'nin önemli katkısı vardır. ABD siber alanda elde ettiği bu üstünlüğü sürdürmek istemektedir. ABD hem ulusal hem uluslararası alanda bu üstünlüğü devam ettirmek için uluslararası örgütleri de bu amaçları doğrultusunda kullanmaktadır. Birleşmiş Milletler bünyesinde oluşturulan İnternet Yönetişim Formu ve ICANN buna örnek olarak gösterilebilir. ABD siber yönetişim konusunda özellikle ICANN modelini savunmaktadır. Çok paydaşlı ve katılım oranı yüksek olan bu kuruluşun siber yönetişim hususunda en etkili mekanizma olduğu savunulmaktadır. Fakat kararlarının bağlayıcı olmaması bu kuruluşun eksik ve yetersiz olduğunun en açık göstergesidir. Bu durum diğer ülkeler tarafından eleştirilmektedir. ABD'nin ICANN ile fiziksel alanda olduğu gibi siber alanda da kendi çıkarlarını korumak istediği iddia edilmektedir. Bu söylemin en büyük destekçisi siber alanda etkili olmaya çalışan Rusya'dır. Rusya siber alanda batı özelliklede ABD üstünlüğünü istememektedir. Bunun için bölgesel ve küresel çapta faaliyetler yürütmektedir. Söylem olarak ABD'nin siber politikalarına karşı çıksa da Rusya da ABD'den farklı politikalar yürütmemektedir. Yapmış olduğu yoğun siber saldırılar bunun en açık göstergesidir. Kısacası Rusya Da siber alanda yönetişimi geliştirmek yerine bu alanda daha fazla etkili olmak ve gücünü maksimize etmek istemektedir.

Uluslararası İlişkilerin büyüyen gücü Çin de siber alanda etkili olmak istemektedir. Tıpkı Rusya gibi Çin de siber alanda ABD üstünlüğünden rahatsız olmakta ve bu alanda kendini geliştirmek istemektedir. Çin siber konularda diğerlerinden farklı olarak siber alanda etkinliğini kendi alternatif modellerini ve politikalarını uygulayarak yapmak istemektedir. Siber yönetişim konusunda Çin *siber egemenlik* olarak kavramsallaştırılan politikayı savunmaktadır. Buna göre ulusal alanda devlet siber konulara müdahale edebilecek ve istediği konuda sınırlama getirebilecektir. Uluslararası alanda ise siber daha normatif, daha katılımcı ve daha şeffaf olmalıdır. Görüldüğü üzere Çin'in siber yönetişim konusunda savunduğu model kendi içinde bile çelişmektedir. Buradan Çin'in ulusal çapta kendi baskıcı politikalarına dayanak aradığı görülmektedir. Küresel alanda ise daha rahat edebilmek için iyi siber yönetişimi savunmaktadır.

Sonuç olarak siberin önemli aktörleri olan ABD, Rusya ve Çin siber yönetişim konusunda bir takım söylemlere sahip olsalar da esasen kendi çıkarlarını korumak istemektedirler. Yapılan çalışmada her üç devletinde siber uzayda gerçek manada siber yönetişimi sağlamak yerine sibere hükmetmeye çalıştıkları sonucuna ulaşılmıştır. Zira günümüzde sibere hükmedenin fiziksek dünyaya da hükmedeceği düşüncesi devlet merkezci bakışın en önemli sorunudur ve bakış açısı değişmediği müddetçe bu sorun siber alanda sıkıntı oluşturmaya devam edecektir.

Kaynakça

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

Almeida, V. (2016). *Cyberspace Governance Concepts and Framework.* https://cyber.harvard.edu/~valmeida/pdf/Lecture2.pdf. (Erişim Tarihi: 08.12.2018).

Choucri, N., Clark, D. (2013). Who Controls Cyberspace. Bultein of The Atomic Scientists. Vol. 69, No. 5, pp.21-31.

CoE. (2016). *Internet Governance: Council of Europe Strategy 2016-2019.* https:// rm. Coe. int/ internet governance – strategy – 2016-2019- update version(Erişim Tarihi: 02.12.2018).

Connell, M. Vogler, S. (2017). Russia's Approach to Cyber Warfare. CNA Analysis and Solution.

Cuihong, C. (2018). Global Cyber Governance: China's Contibution and Approach. China Quarterly of International Strategic Studies. Vol. 4, No. 1, pp.55-76.

Danchev, D. (2008). How Russia May Have Attacked Georgia's Internet. http://www.newsweek.com/how-russia-may-have-attacked-georgias-internet-88111. (Erişim Tarihi: 25.12.2018).

Herold, D. (2011). *An inter-nation-al Internet: China's contribution to global Internet governance*.http://ira.lib.polyu.edu.hk/bitstream/10397/5782/1/Herold_Inter-nation_Al%20internet_China.pdf. (Erişim Tarihi: 08.12.2018).

IGF. (2018). Internet Governance Forum. https://www.intgovforum.org/multilingual/content/about-igf-faqs. (Erişim Tarihi: 11.12.2018).

Kaufmann, D. Kraay A. (2002). Growth without Governance. World Bank Policy Research Working Paper No. 2928.

Kurbalija, J. (2014). *An Introduction to Internet Governance.* Geneva, Switzerland: Diplo Foundation.

Layne, Karen. Lee, Jungwoo. (2001). Developing fully functional E-government: A four stage model. Government Information Quarterly. Vol. 18, No. 2, pp.122-136.

Marcus, G. (2015). Human Rights and New Digital Paradigm. Contemporary Challenges in Securing Human Rights. Institute of Commonwealth Studies, School of Advanced Study, University of London, pp.35-44. https://sas-space.sas.ac.uk/6205/1/06marcus.pdf. (Erişim Tarihi: 14.12.2018).

Markoff, J. (2008). *Before The Gunfire Cyberattacks*. The New York Times. https://www.nytimes.com/2008/08/13/technology/13cyber.html. (Erişim Tarihi: 25.12.2018).

Mihr, A. (2014). Good Cyber Governance: The Human Rights and Multi Stakeholder Approac. Georgetown Journal of International Affairs. pp.24-34.

Nagelhus, N., Gjesvik, L. (2017). China's Cyber Sovereignty. Norwegian Institute of International Affairs Policy Brief. file://S%C4%B0BER%20UZAY/NUPI_Policy_Brief_2_17_Schia_Gjesvik.pdf. (Erişim Tarihi: 08.12.2018).

Nagy, V. (2012). The geostrategic struggle in cyberspace between the United States, China, and Russia. Atlantic Association in the Mathematicals Sciences. Vol. 11, No. 1, pp.13-26.

Nocetti, J. (2015). Contest and Conquest: Russia and Global Internet Governance. International Affairs. Vol. 91, No. 1, pp.111- 130.

No, N. (2017). New Cyber Strategy of China and the Alterations in the Field. Journal of Political Sciences & Public Affairs. Vol. 5, No. 5.

Nye, J. (2014). *The Regime Complex for Managing Global Cyber*. London: Centre for International Governance Innovation and the Royal Institute for International Affairs.

Rotberg, R. (2014). Good Governance Means Performance and Results. International Journal of Policy, Administration, and Institutions. Vol. 27, No. 3. pp.511-518.

Segal, A. (2011). Cyberspace Governance: The Next Step. Asia Program and International Institutions and Global Governance Program

Shen, H. (2016). China and global internet governance: toward an alternative analytical framework. Chinese Journal of Communication. Vol. 9, No. 3, pp.304-324.

Singh, P. (2016). Internet Governance: Is the Internet Really Free of US Control?. Economic & Political Weekley. Vol. 51, No. 42.

The White House. (2018). *National Cyber Strategy of United States of America*. https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf.(Erişim Tarihi: 07.12.2018)

United Nations Escape. (2009). *What is Good Governance?*. https://www.unescap.org/sites/default/files/good-governance.pdf. (Erişim Tarihi: 10.12.2018).

Wallace, I. (2014). *India, the U.S., and Internet Governance.* https://www.brookings.edu/wp-content/uploads/2016/06/23-india-us-internet-governance-wallace.pdf. (Erişim Tarihi: 11.12.2018)

Xin, Li. (2017). China's cyber governance undergoes revamp. Global Times. http://www.globaltimes.cn/content/1070628.shtml. (Erişim Tarihi: 29.12.2018)

Zaagman, E. (2018). Cyber Sovereignty and the PRC's Vision for Global Internet Governance. China Brief. Vol. 18, No. 10,