SİBER UZAY VE GÜVENLİK POLİTİKASI ÜZERİNE TEORİK BİR YAKLAŞIM

Vahit GÜNTAY*

Özet

Siber güvenliğe ve siber uzaya olan ilgi her geçen gün artarken Uluslararası İlişkiler gibi alanlarda güç kavramının katettiği yol, siber alanda kendi bütünlüğüyle tartışılmaktadır. İki kutuplu yapıya dayanan Soğuk Savaş'ın bitişi, en azından zihinlerdeki sınırları kaldırırken çok yönlü ve daha dinamik bir güvenlik kavramını ortaya çıkarmıştır. Güvenliğin bile tanımı üzerinde kesin bir cümle kurulamazken siber güvenlik gibi bir kavramın saldırı-savunma stratejisi içinde değerlendirilmesi ya da politikalar oluşturulabilmesi oldukça düşündürücüdür. Güvenlik ikileminin beslendiği boyut teknolojik alandan ve gelişmelerden daha keskin şekilde etkilenmektedir ve küresel risk toplumunda siber politikalar artık daha karmaşık bir hal almıştır. Yaklaşımın çeşitliliği siber politikalar oluşturmada devletlerin elini güçlendirmektedir fakat güvenlik algısını da ortak bir barış kavramı içerisinde ütopik boyutlara taşımaktadır. Bu çalışmada siber güvenliğin algısal olarak yeni bir boyut kattığı Uluslararası İlişkiler disiplini farklı bir yönüyle irdelenmiştir. Yaklaşım oluşturmak oldukça zor bir husus olsa da çalışmanın kurgusu siber güvenlik ve uluslararası ilişkilere dair bir deneme niteliği taşımaktadır.

Anahtar Kelimeler: Siber Güvenlik, Uluslararası İlişkiler, Güvenlik İkilemi, Siber Uzay, Siber politikalar

A THEORETICAL APPROACH ABOUT CYBER SPACE AND SECURITY POLICY

Abstract

The interest about the cyber security and cyber space is increasing day by day and developing power concept is discussed with its own integrity in cyber area at International Relations discipline. After the Cold War with its bipolar system, borders were removed in minds and multiple security concept shaped with its more dynamic qualities. While it is not possible to make sentence about the concept of security, it is challenging to evaluate cyber security concept in offensive-defensive strategy or establish a policy. The dimension of the security dilemma is affected excessively by technological developments and cyberpolitics become more complicated in global risk society. The diversity of approach strengthens the states but it carries the security perception to utopic dimensions in the common peace concept. In this study, international relations discipline has been examined with its different aspect in which cyber

* Yardımcı Doçent Doktor, Karadeniz Teknik Üniversitesi, İİBF, Uluslararası İlişkiler Bölümü. E-posta: vahitguntay@gmail.com

security added a new dimension as a perception. Also it is very problematic issue to construct an approach, the concept of the study is to try an essay about cyber security and International Relations.

Keywords: Cyber Security, International Relations, Security Dilemma, Cyber Space, Cyberpolitics

Giriş

Siber güvenliğe ilişkin gelişmeler günümüzde yeni bir çatışma alanı mı oluşturdu ya da yeni ufuklar mı açtı gibi soruların cevabını vermek oldukça zor fakat siber savaş kavramının tartışıldığı bir boyutu şekillendirmiştir dersek yanılmış olmayız. Teorik olarak uluslararası sistem açısından güvenlik yaklaşımlarında bir paradigma oluşturmak zordur. Özellikle yakın zaman itibariyle uluslararası alandaki tüm ilişkiler elbette çatışma veya savaş bağlamında gelişmemiştir fakat yaklaşım oluşturma zorluğu ya da siber güvenlik alanında sadece çatışmacı bir yaklaşımla uluslararası ilişkiler disiplininde bir arayış içerisinde olmak da mantıklı gözükmemektedir. Çünkü uluslararası sistem içerisindeki gelişim tek taraflı olarak devletler temelinde ele alınamaz. Bireysel ve toplumsal beklentiler de siber güvenlik alanındaki strateji düzeyini farklı alanlara taşıyacaktır.

Siber uzayda meydana gelen tüm gelişmeler ortaya çıkış mekanizması ve gelişimi itibariyle artık tespit edilebilir düzeydedir. Siber tehdidin kimleri nasıl etkilediği ya da ilgilendirdiği boyutu bir sorunsala sahiptir. Bireylerin ya da kurumların, şirketlerin tehdit içerisinde olduğu alan ile uluslararası aktörlerin tehdit içerisinde olduğu alan aynı teorik zeminde incelenemez. Bu konu sosyolojiyi, felsefeyi ve hatta psikolojiyi de ilgilendiren bir husustur. Büyük hasarlara yol açan bir siber saldırı bireysel bir etkinlik de olabilir ya da geniş ve planlı bir siber saldırıyı durduran, açığa çıkaran sadece bir birey olabilir. Bu paradoks dahilinde siber savaş gibi bir kavramı açıklığa kavuşturmak ve kesin bir tanımını yapmak oldukça zordur. Bu doğrultuda siber güvenliğe ilişkin güncel çalışmaların temeli bir yaklaşım denemesinin de ötesine geçememektedir. Hal böyle iken devletler üzerinden çıkarım yapmak ya da kesin sonuçlardan bahsetmek bir o kadar zorlaşmaktadır.

Siber tehditler evrilen bir forma sahiptir. Bu formun değişimi bağlı olduğu alanın genişlemesiyle ilgili bir durumdur. Soğuk Savaş sonrasındaki tehdit parametreleri değişince ve devletler siber uzaya bağlı hale geldikçe uluslararası ilişkiler düzeyindeki sorular da çeşitlenme imkanı bulmuştur. Teorik zemini oldukça zor tartışılan bu alan eldeki somut verilerle ve bazı gelişmelerle analiz de edilebilmektedir. Bu çalışma dahilinde bu sorulardan bir kaçına yanıt aranmaya çalışılmıştır. Zor olan, alana ilişkin siber güvenlik çerçevesi ele alınacaksa bunun hangi teorik temellerle tartışılacağı hususudur. Siber saldırılar kesin bir şekilde sonuçlandırılabilir mi ya da yapılan siber savaş tanımlarından yola çıkılarak bir siber barış ilan edilebilir mi gibi soruların değerlendirilmesi ciddi bir bakış açısına ihtiyaç duymaktadır. Artık uluslararası hukukun ilgi alanına girmiş olmanın da ötesine geçen siber alan hukuk normlarıyla da adından söz ettirmektedir.

Bu çalışma dahilinde uluslararası ilişkilerin bazı temel hususları siber uzay kavramıyla değerlendirilmiş ve bir yaklaşım denemesi ortaya konmuştur. Güvenlik ikileminin siber uzayda aşılması söz konusu mudur ya da siber silahlar ile uluslararası ilişkiler içindeki saf hali tartışma aritmetiğinin olasılığı üzerine bir çıkarım yapılmıştır. Uluslararası ilişkilerde güvenlik algısındaki değişim küresel risk toplumu ve güvenliğin bölgesel politikalara çekilmesiyle siber politikalara yakınlaştırılarak teorik bir deneme sergilenmiştir.

Uluslararası Güvenlikte Politika Üretme Sorunu

Uluslararası siyaset açısından güvenliğin içeriği, korunması gereken değerle birlikte üretilecek politikanın nasıl olması gerektiği sorusuna verilecek cevapla şekillenmektedir. Güvenlik açısından "*Kimin güvenliği?"* ya da "*Neyin güvenliği?"* sorularının cevabı güvenlik politikalarının temelini oluşturmaktadır. Güvenlik çalışmalarında bu soruların cevapları *devlet odaklı güvenlik* ya da *birey odaklı güvenlik* olması açısından iki temel yaklaşımı ortaya çıkarmıştır (Birdişli, 2016: 21).[1]

Devletin yaşamsal sınırları vardır ve bu sınırlar dahilinde uluslararası politikada aktör olma konumu güçlendirilerek güvenlik çerçevesi oluşturulmaktadır. Devlet odaklı güvenlikte var oluş ve bu varlığı devam ettirme adına kimi zaman başka devletlerdeki bireyler gözardı edilebilmekte, müdaheleler gerçekleştirilebilmekte ya da yaşanan olaylara sessiz kalınabilmektedir. Realist paradigmanın da sık sık atıf yaptığı bu durumla ilgili insan doğasının güvenilmezliği devlet odaklı güvenlik anlayışını güçlendirmektedir.

Yaşam hakkı, inanç özgürlüğü ya da mülkiyet hakkı gibi temel hak ve özgürlüklere ilişkin devletin güvenlik politikaları oluşturması ve bu politikaların merkezinde bireyin olmasına ilişkin görüşler ve çalışmalar da bir hayli fazlalaşmıştır. Siber güvenliğin içerdiği kavramsal çeşitlilikle birlikte birey-devlet ilişkisi, teknolojik gelişmelerle birlikte uluslararası yapılanmaların etkileşimi bu tartışmalar içerisinde politika üretiminde inşacı perspektifi ön plana çıkarmaktadır.

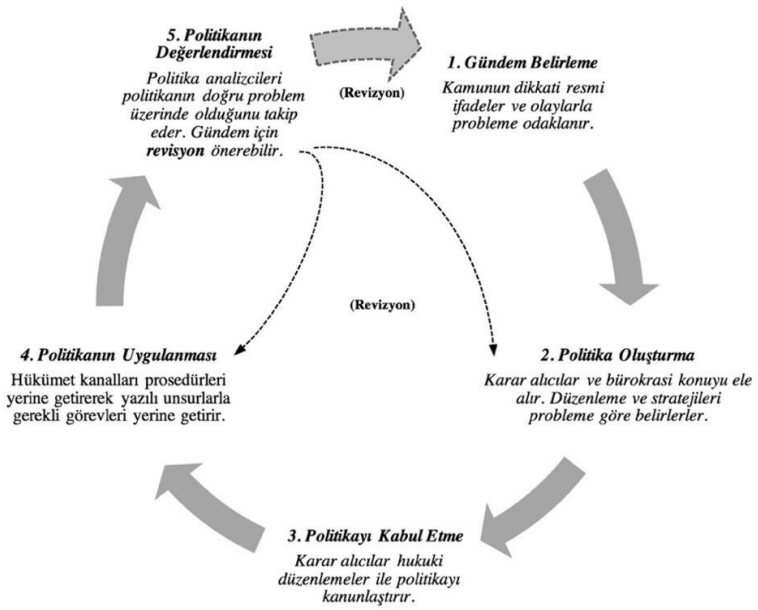
Uluslararası güvenlik açısından, devlet-birey-güvenlik üçgeninde karar alıcıların politika üretmesi ve bunun siber uzayda karşılık olarak çıkarsal bir döngü haline gelmesi, en az teorik yaklaşım kadar önemlidir ve ciddi bir birikim istemektedir. Bu durumu önemli kılan ise kimi zaman tehdit algısının ortaya çıkması ve doğru algılanması, kimi zaman ise çıkarsal bir durumun arzulanmasıdır. Sonuç olarak devletlerin varlık sebebi bu mücadelede üstün gelinmesidir.

[1] Farklı yaklaşımlar arasında *"siber güvenlik"* ve *"ulusal güvenlik"* gibi kavramların resmi dokümanlarda kullanılışında doğrudan bir kıyaslama yapılmaktan kaçınılmaktadır. Bunun sebebi "siber güvenlik" kavramının kabul edilen ortak bir tanımının olmayışıdır (Hathaway ve Klimburg, 2012:20).

Üretilecek politikaların teorik çerçevesi sosyal bilimler gibi alanlarda kurgusal olarak daha zordur ve oluşturulan politik çerçeve bir o kadar temel düzeyde kalmaktadır. Uluslararası güvenliğe ilişkin sergilenecek bir yaklaşımın temeli, uluslararası politikada teori oluşturulmasıyla benzerlikler gözetmektedir. Sönmezoğlu (2014: 94) teori oluşturmaya ilişkin başlıca üç noktayı şu şekilde tanımlamıştır:

- *Teoriyi oluşturan önerme ve genellemelerin birbirleri ile mantıklı ve tutarlı bir bağlantı içerisinde bulunmaları,*
- *Bu önerme ve genellemelerin olgularla bağlarının kurulabilmesi,*
- *Söz konusu önermelerin belirli ölçülerde betimleme, açıklama ve tahmin kapasitesine sahip olmaları gereği.*

Şekil 1. Politika Oluşturma Diyagramı



Kaynak: The Texas Politics Project, 2016

Uluslararası politika açısından yaklaşacak olursak siber savaşlar için de benzer bir teori oluşturma mantığından söz edebiliriz. Örgütler, bireyler, uluslararası kuruluşlar ve devletler düzeyindeki farklılık, analiz düzeyini inşacı teoriye yaklaştırmaktadır. Olayların siber uzayda kendi içerisindeki döngüsel ağı, politik bir düzlem oluştururken, teori oluşturma mantığıyla benzer işlemektedir (Sard, 2014:4). Bu noktada güvenlik ikileminin siber boyutta ne ifade ettiği, küresel risk toplumunda siber politikalar ve doğal olarak karşımıza çıkacak yeni güvenlik algısı çerçeveyi ana hatlarıyla anlamamıza yardımcı olacaktır.

Güvenlik İkileminin Siber Uzayda Aşılması

"Güvenlik İkilemi (security dilemma)"[2] kavramı hem Uluslararası İlişkiler disiplini, hem de karar alıcılar için üzerinde düşünülmesi gereken önemli bir hususdur. *Güvenlik ikilemi* en temel anlamıyla bir devletin başka devletten tehdit algılayıp silahlanması durumunda, bunu tehdit olarak algılayan devletin de aynı şekilde cevap vermesi anlamına gelmektedir. Karar alıcılar, güvenlik sorunlarını nasıl çözebilecekleri konusunda farklı seçeneklerle karşı karşıya kaldıkları sürece güvenlik ikilemi hep var olacaktır.[3]

Güvenlik kaygısını ortadan kaldırma adına yasa ya da yasal bir otorite olmadığı için devletler kendi güvenliklerini kendileri sağlamakta ve kimi zaman sorunun temeline ilişkin benzer ülkelerle ortak hareket etmektedir. Her devletin kendi bünyesinde alternatifler üretmesi ve silahlanma gibi benzeri adımlarla hareket etmesi güvenlik ikilemi açısından diğer devletin güvenliğinin de azalması anlamına gelmektedir. Güvenlik ikilemi bu noktada alana ilişkin paradoksların başında gelmektedir (Karabulut, 2015: 40).

Özellikle Soğuk Savaş sonrası dönemde *güvenlik ikilemi* kavramının gelişmesinde önemli parametreler vardır. Bunlardan ilki yeni güvenlik sorunlarının artan şekilde dünya siyasetini etkilemesidir. İkinci durum ise, sorunlar uluslararası ilişkiler disiplininin dünya politikasına bakışı, sorunları algılayışı ve tanımlayışında değişikliklere yol açmıştır (Bilgiç, 2012: 339). Özellikle silahlanma yarışı hız kesmeden yoluna devam ederken, siber güvenliğe ilişkin algı da devletleri birbirlerine karşı önlemler almalarına ve harcamaların artışına neden olmuştur (Tang, 2009: 590).

Dünya siyasetini meşgul eden siber güvenlik yeni olmasının yanında, güvenlik ikilemi açısından uluslararası ilişkiler disiplinine siber savaş olgusunu da eklemiştir. Savaş olgusu ise pratikte çoğu zaman birlikteliklere ve ortak güvenlik kaygısına sebep olmuştur. Devletler arasındaki siber mücadelenin boyutu da konvansiyonel mücadelenin temelindeki çatışma olgusuyla örtüşmeye başlamıştır ve devletler bu konuda saldırı unsurlarını geliştirme seçeneklerini masaya koymuştur.

Uluslararası alanda egemenlik tartışması sadece çatışmaların oluşması yönünde adımları getirmemektedir. Aynı zamanda statükoya ilişkin ortak çıkar halini de beraberinde getirmektedir. Devletlerin farkında olduğu şey anarşinin, statükonun dağılması durumunda kötüye gidişi cesaretlendirici etki yaptığıdır (Jervis, 1978: 167). Siber uzaydaki faaliyetler tam bu noktada söz konusu durumu teşvik edici niteliktedir. Siber uzayda güvenlik ikileminin geldiği nokta, gelişen her unsurun savaşa ve çatışmaya neden olabileceği yönündeki yaklaşımla daha çok örtüşmektedir.

---

[2] *Güvenlik ikilemi*, uluslararası ilişkiler terminolojisine John H. Herz'in yazdığı *Politik Realizm ve Politik İdealizm* kitabıyla girmiştir. Ayrıca yine aynı döneme ait Hurbert Butterfield'ın *Tarih ve İnsan İlişkileri* adlı kitabında da benzer bir durum farklı bir üslupla dile getirilmektedir.

[3] *Güvenlik ikilemi* kavramının ilk ortaya konuş biçimi, Soğuk Savaş döneminde disipline egemen olan realist düşüncenin öğelerini yansıtır. Öncelikle, güvenlik ikilemi kavramı devlet-merkezci bir yaklaşım dahilinde üretilmiştir.

Neden olunan çatışma, sadece çıkarsal veya egemenlik alanına ilişkin mücadelenin sonuçlarını birer çıktı olarak devletlere vermemektedir. Örneğin; 1998 yılında ortaya çıkan ve *Çernobil Virüsü* olarak da bilinen *CIH virüsü*, 1999 yılında etkin hale gelmiş ve birçok kullanıcının verilerini kaybetmesine yol açmıştır. 2000 yılında *Mellisa, Love Bug* ve *Killer Resume* gibi büyük mali kayıplara neden ola virüsler yine bu durumun çeşitliliğine ilişkin bir örnektir (Bayraktar, 2015: 155).[4]

Gelişen her unsur sahip olduğu altyapıyla birlikte devletlerin çıkar arzusunu körüklemektedir. Güvenlik ikileminin de temelinde bu durum vardır. Uluslararası ortamda güvenlik oluşturma adına caydırıcı olma, kendi sınırlarını aşıp çatışmaya dönüşmektedir (Booth, 2012: 481). Uluslararası düzenleme ve yasa koyucu olmadıkça şartlar daha da ağırlaşmaktadır. Konu kendi içerisinde döngüsel bir soruna dönüşmektedir. Şekil 2'de görüldüğü üzere A devletinden tehdit algılayan B devleti silahlanabilmekte, ittifaklara katılabilmekte ve siber mücadele içinde siber saldırı seçeneklerini kullanabilmektedir. Fakat B devletinin silahlanması bu kez A devletinin güvenlik kaygılarını ön plana çıkarmakta ve bu durumda A devleti de silahlanma kapasitesini artırmaktadır.[5]

Şekil 2. Ülkeler Arasındaki Güvenlik İkilemi Diyagramı

Kaynak: Krickovic, 2016: 116

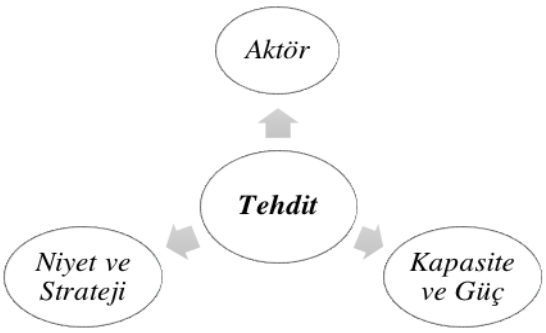
Küresel Risk Toplumunda Siber Politikalar

[4] Diğer bir husus ise siber uzayın toplum ve kitle hareketleri üzerindeki etkisini gösteren Facebook, Twitter, Youtube gibi sosyal paylaşım siteleri üzerinden yaşanan Arap Baharı örneğidir. Arap Baharı'nı *"Facebook Devrimi"* olarak nitelendiren ve Arap Baharı'nda sosyal medyanın gücü görüldükten sonra, siber uzayın politik gücünün önemli bir savaş yeteneği olduğunu niteleyenlerin sayısı oldukça fazladır.

[5] Türkiye ve Yunanistan'ın 1990'lı yıllar boyunca birbirlerine karşı silahlanmaları bir güvenlik ikilemi oluşturmuştur. Özellikle yakın coğrafyalarda sorunlar yaşayan devletlerin attıkları her adım belirli düzeylerde tehdit boyutu dahilinde algılanmaktadır.

Modernliğin beraberinde getirdiği çevresel, ekonomik ve güvenliğe ilişkin kimi riskleri konu alan *risk toplumu* yaklaşımı, riskin sosyolojik boyutunu inceleyen çalışmalar arasında önemli bir yere sahiptir. Modern toplumların birer risk toplumu haline dönüştükleri iddiasına ilişkin tartışmalar büyük oranda Çernobil'deki nükleer facia sonrasında alevlenmiştir (Elmas, 2013: 101).[6] Şekil 3'te görüldüğü üzere Soğuk Savaş döneminde tehdidin boyutları aktör, strateji ve güç arasında sıkışmışken günümüzde bu duruma öngörülemez tehditler de eklenmiş ve risk toplumu yaklaşımı açısından gelişmeleri olumsuz yönde etkilemiştir. Coğrafi olarak kırılganlıkların artışında risk toplumu yaklaşımıyla açıklanabilecek ciddi veriler vardır.[7] Risk toplumu açısından oluşturulacak politikalarda tehdidin çok yönlülüğü içerisine siber tehditler de yerleşmiştir.

Şekil 3. Soğuk Savaş Döneminde Tehdidin Üç Boyutu



Kaynak: Williams, 2005: 7.

Özellikle 11 Eylül 2001 tarihindeki İkiz Kulelere saldırı uluslararası güvenlik politikaları, toplumsal analizler açısından en az Soğuk Savaş'ın sona erdiği Berlin Duvarı'nın yıkılışı kadar önemli bir yere sahiptir. Alman sosyolog Ulrich Beck (2009: 157), ortaya attığı risk toplumu kavramı ile beraber küresel terörizm probleminin bu noktaya gelişinde Batı medeniyetinin teknoloji, ordu ve disiplin aracılığıyla Asya'dan Amerika'ya siyasi anlamda baskın bir rol izlemesinin önemli rol oynadığını düşünmektedir.

Teknoloji, ordu ve disiplin modern toplumların gündemine dahil ettiği siber güvenlik politikalarının yönünü değiştirmiştir. Sadece teknolojik gelişmelere ilişkin riskler değil, aynı zamanda uluslararası alanda yeni bir mücadele alanı olarak toplumların değişen riski haline gelen siber savaşlar kaygıları artırmıştır. Geçmişte yaşanan facialar bilinen haliyle kaza gibi görünse de, devletlerin ve farklı grupların kritik altyapılara müdahale edebilir yöndeki gelişmişlikleri ve olanaklar *küresel risk toplumu*

[6] Çernobil gibi kaza anında sebep olduğu yıkımlardan ziyade bu gibi teknoloji ürünü facialarının meydana getirdiği asıl problem, bilimsel otoritelerin geleceğe dair topluma inanılır cevaplar verememesi ve buna bağlı olarak da bireylerin gelecek yaşamlarının kendilerine ne getireceğini kestirememesinde yatmaktadır.

[7] Risk toplumu tartışmalarına ilişkin yaklaşımı sadece felaket toplumuna dönüşüm olarak algılamamak gerekir. Anthony Giddens (1998), bu duruma ilişkin şu tespiti yapmaktadır: *"Risk toplumu düşüncesi, dünyanın daha tehlikeli bir hal aldığını iddia ediyormuş gibi görünebilir, ancak bu gerçekte böyle değildir. Aksine bu, devamlı artan bir biçimde geleceği üzerine kendisini meşgul ederek risk düşüncesini ortaya çıkaran bir toplumdur."*

yaklaşımıyla örtüşmekte, teknik ve bilimsel ilerlemenin, bireyin hayatını daha da kolaylaştıracağı yönündeki savunma geri planda kalmaktadır.

Elmas (2013: 113) risk toplumunda belli risklerin gerçek olması durumunda ortaya çıkabilecek kimi felaketlerin varlığından bahsetmekte ve bu felaketlerin kontrol edilemeyen etkilerinin söz konusu olduğunu vurgulamaktadır. Bu durum risk toplumu yaklaşımının kaos ve anarşi dolu yeni bir toplum modeli ortaya koymaya çalıştığı şeklinde değerlendirilmemelidir. Bu yaklaşım modern sanayileşmenin ve modern teknolojilerin dolaylı olarak ve istemeden sebep olduğu etkilerinin, modern kurumlar tarafından kontrol edilememesi ve nasıl yönetileceğinin bilinememesi durumunu tartışmaya açmaktadır. Siber politikalar oluşturma ya da oluşturamama arasındaki itici güç de bir yönüyle buradan kaynak almaktadır.

Siber suçların ya da daha dar kapsamlı siber terör faaliyetlerinin modernleşmenin getirmiş olduğu risklerden ve tehditlerden olduğu açıkça görülmektedir. Son yıllarda uluslararası arenada devletler hem kendi kurumlarını hem de kendi ilkelerini dönüştürmekte ve siber risk ve tehditlere yönelik politikalar üretme yoluna gitmekte ve bu durum siber orduların ortaya çıkmasına neden olmaktadır (Erendor, 2016: 119). Bu açıdan bakıldığında siber politikalar oluşturulması ve uluslararası alanda etki doğurmasına ilişkin risk toplumunun algısal değişimi ve gelişimi önemli bir çerçeveyi oluşturmaktadır. Kritik altyapılara ilişkin oluşabilecek tehlikeli girişimler moderniteyi karşı bir silaha dönüştürebilir. Karar alıcıların algısal düzeyi ve gelecek vizyonu moderniteyle doğru orantılı şekilde yükselmelidir.[8]

Yeni Güvenlik Algısı ve Siber Uzay

Küreselleşme süreci ile birlikte güvenliğe yönelik tehditlerin farklılaşması yeni bir güvenlik tanımlamasını gerekli kılmıştır. Geleneksel tehdit algılamaları ve bu unsurlarla mücadele yöntemleri yeni güvenlik tehditleriyle mücadele konusunda yetersiz kalmaktadır. Bu yetersizlik yeni bir güvenlik tanımlamasının yanı sıra bu tanımlamadan hareketle yeni mücadele araçlarını da devreye sokmayı gerekli kılmaktadır (Karabulut, 2015: 119). Yeni mücadele araçları ise sadece fiziksel ya da sanal boyuttaki unsurları kapsamamaktadır. Toplumlar arasındaki hareketlenmeler ve çoğu zaman bu toplumlar arasındaki dini ve etnik farklılıklar dahi kapsam dâhilinde olabilmektedir.

Mücadele araçları içerisinde gelişimini ve farklılaşmasını hızla sürdüren siber saldırı araçları geleneksel tehdit anlayışını yeni güvenlik yaklaşımı içerisinde belirginleştirmiştir. NATO'nun tehdit tanımlamaları, ABD'nin özellikle siber güvenlik alanında vermiş olduğu öncelik ve yeni bir harekat alanı oluşturan

[8] Danışmanlık şirketi Marsh&McLennan'ın Davos Zirvesi için hazırladığı *"2016 Yılı Küresel Riskler Raporu"* çevresel sorunlardan zoraki göçe, enerji fiyatlarından siber saldırılara kadar birçok alanda dünyanın en riskli dönemini yaşadığını ortaya koymuştur. Raporda ilk kez; beş kategoriden dördü, yani çevresel, jeopolitik, toplumsal ve ekonomik riskler ilk beş en yüksek etkiye sahip riskler arasında yer almıştır. Teknolojik risklere de dikkat çekilirken, siber saldırıları kapsayan teknoloji riski hem gerçekleşme olasılığı hem de etkisi bakımından 11. sırada yer almıştır. Siber saldırılar, 27 ekonominin ilk beş riski arasında yer almaktadır.

siber savaş bu temel değişim içerisinde en somut tespitlerdir. 1990'lardan itibaren küreselleşme olgusunun hız kazanmasıyla *"artık hiç bir şey eskisi gibi olmayacak"* sözünü doğrularcasına, her alanda çok hızlı ve önüne geçilemez bir değişim süreci başlamıştır. Böylece önceki devirlerde benimsenen ekonomik, politik ve güvenlik stratejilerinin dayandırıldığı parametrelerin çoğunun sarsıldığı ya da ortadan kalkmaya yüz tuttuğu bir sürece girilmiştir. Bireyler arasında etkileşimin arttığı günümüzde politik alan farklı unsurlarıyla genişlemeye başlamıştır.

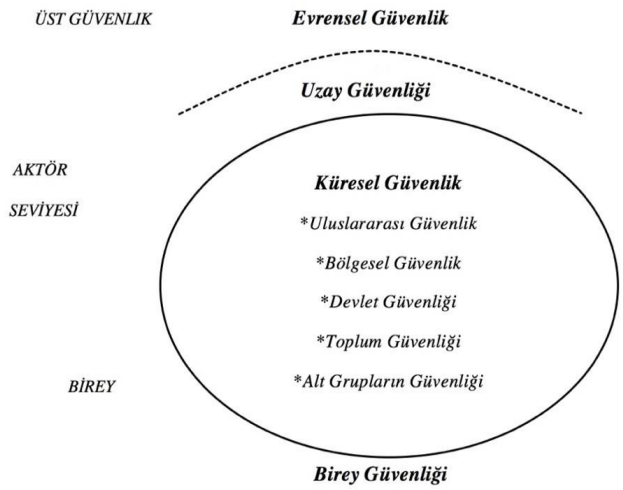
Soğuk Savaş sonrası dönemde küreselleşme sürecinin itici gücüyle tehdit olgusunda niceliksel bir artış, niteliksel boyutta bir çeşitlenme meydana gelmiştir. Bu yeni dönemde öncelikle askeri olduğu kadar ekonomik, sosyal, dini ya da kültürel, ideolojik, çevresel, toplumsal ve sağlıkla ilgili yeni tehdit unsurları ortaya çıkmıştır (Erdoğan, 2013: 269). Siber terör de bu boyutta etken bir araç olarak yerini almıştır.[9] Siber terörün kendi içerisindeki boyutsal nitelik ile uzayda yapılan çalışmalar, insanların sosyal hayatta yaşadıkları her yeri içerisine dahil etmiştir (Der Derian, 2009: 121).

Güvenliğin derinleşmesi ve genişlemesi, temel olarak güvenlik tehditlerinin çoğalmasıyla doğru orantılı bir süreçtir. Bunun yanı sıra tehditlerin küresel bir şekilde ele alınmasının gerekliliği, tehditlerin teknolojik gelişim ve küreselleşme gibi etmenlerle daha yaygın bir hale gelmesidir. Bu bağlamda güvenlik, küreselleşme ve teknoloji ilişkisini irdelemek gerekmektedir. Küreselleşme ve teknolojinin ortaya çıkardığı akışkanlık ve sınırların geçirgenliği, bireye ve devlete yönelik tehditlerin dozunu da artırmıştır (Aksu ve Turhan, 2012: 71).

Yeni güvenlik anlayışının siber güvenlik boyutu, Şekil 4'te görüldüğü üzere tüm güvenlik unsurlarının temelde, belirli verilere sahip olmasıyla da kapsayıcılık açısından en üst düzeyde yer almaktadır. Küresel güvenlik açısından ele alınan tüm unsurlar uzay boşluğunda teknolojik unsurlarla birbirlerine yakınlaştığı ölçüde siber teröre maruz kalabilecektir ve sorunsal alan daha da genişleyecektir. Verilerin artan bir hızla entegre edildiği siber alan kaygıları daha da artırmaktadır.

Şekil 4. Güvenliğin Katmanları

[9] Küreselleşmenin, dolayısıyla *kültürel emperyalizmin* aktörleri olarak algılanan gelişmiş ülkelere karşı gösterilen reaksiyonların belki de en basit örneği tek kişilik ordu konumuna gelebilmiş hackerların siber ortamda gerçekleştirdikleri saldırılar olmuştur.



Kaynak: Yılmaz, 2014: 12

Güvenliğin Bölgeselleşmesi ve Siber Politikalar Oluşturma

Bölgesellik ve güvenlik birbiriyle pek çok farklı şekilde ilişkilendirilebilmektedir. Özellikle Barry Buzan'ın (1991: 190), *"bir grup ülkenin temel güvenlik kaygılarının, gerçekçi bir şekilde birbirinden ayrı düşünülemeyecek kadar birbirine bağlanması"* şeklindeki tarifi özellikle siber güvenlik ve oluşturulacak politikalar açısından açıklayıcıdır. Bölgesel olarak çatışmalarda, devletlerarasındaki belirleyici faktörler siber politikaları etkilemektedir ve ittifak arayışında yakın coğrafyadan uzaklaşılmasını sağlamaktadır ki bu durum siber politikalar açısından çoğu zaman tehlikeli bu durumdur.

Özellikle kritik altyapılar açısından yakın coğrafyalardaki ülkelerin birbirine bağlılığı düşünülecek olursa ittfak arayışının ve siber politikalar oluşturmada güvenliğin bölgeselleşmesi farklı yaklaşımlar oluşturma gayesinde önem kazanacaktır. Bu yaklaşım ile ilgili olarak özellikle Türkiye gibi ülkelerin çevresindeki devletlerde, siber saldırılara ilişkin olay döngüsü, yakın coğrafyalardaki ortak samimiyeti gerekli kılmaktadır. Bunun temelindeki etken yakın coğrafyalar arasındaki hafızadır.

Şu ana kadar dünyanın farklı bölgelerinde oluşturulan bölgesel güvenlik çerçeveleri, Avrupa dışında gelişme aşamasındadır ya da başarıya ulaşamamıştır. Bundaki temel etken, devletlerin *Avrupa Birliği* yapılanmasına her yönden benzemeye çalışmasıdır. Avrupa'nın bu konudaki çıkarımı tarihsel olarak gergin ve savaşa eğilimli Almanya-Fransa çatışmasının tanımladığı güvenlik yapısını, bölgesel işbirliği ile savaşın artık çatışmaları çözebilmek için seçenek dahi olmadığı bir güvenlik topluluğuna dönüştürmüştür ve ciddi bir supranasyonal nitelik ortaya çıkmıştır (Hettne, 2012: 357).

Siber politikada çıktılar oluşturma adına genelde G-8, özelde ise bu çatı altındaki İngiltere, Fransa, Almanya, İtalya ile Japonya, Kanada, Rusya ve ABD arasındaki siber suçlarla olan mücadelede güvenliğin bölgeselleşmesi açısından eldeki veriler kayda değerdir. Yapılan toplantılarda, 1995 yılından beri bölgesel gelişmelerle birlikte siber suçlarla mücadele konusu ele alınmaktadır. Bu toplantılar

neticesinde çalışma grupları oluşturulmuş, siber suçlarla mücadelede eylem planları hazırlanmış ve faaliyete geçirilmiştir.

Diğer taraftan *Siber Savunma Politikası* hedefi altında NATO, siber saldırılara karşı önem teşkil eden tüm iletişim ve bilgi sistemlerinin korunmasını, ittifak üyelerine sağlamak için NATO yeteneğinin kuvvetlendirilmesi hususunda müdahalelerde bulunmuştur. NATO'nun en üst karar organı olan Kuzey Atlantik Konseyi, *Siber Savunma Programı*'nı desteklemektedir (Keleştemur, 2015: 440).[10]

Etkileşimin yoğunluğu siber politikalar oluşturma açısından güvenliğin bölgeselleşmesi adına karşımıza örneklerini verdiğimiz NATO gibi yapılanmalara benzer şekilde örgütlenme mantığını ve politikalar üretme gereğini karşımıza çıkarmaktadır. İttifak ve strateji oluşturma anlayışının oluşmasında yakın çevredeki gelişmeleri takip etme ve siber güvenlik adına bu gelişmeleri doğru okuyabilme, işbirliği oluşturulabilmesi adına daha kazançlı gözükmektedir. Siber alanda girişimler, günümüz gerçekliğinde rasyonel boyutlarda tartışılmalıdır.

Güvenliğin bölgeselleşmesi perspektifinden bölgesel işbirliği, bölgesel bütünleşme ve bölgesel birlik açısından ülke içi yapılanmalar da önemli bir yere sahiptir. Bölgeselleşme düzeyinin gevşek olduğu bölgesel işbirliğinde bu yapılanmalar sorunlara sebep olabilmektedir ve bu yüzden daha küçük, mikro yapılarda bölgesel birlikler daha da yapıcı kararlar alabilmektedir ve manevra yetenekleri daha kuvvetli olabilmektedir.

Sonuç Olarak

Uluslararası ilişkiler adına güvenlik en temel haliyle devletleri daha çok ilgilendiren bir husus gibi görünse de değişen dünya kavramı bu hususu temellerinden sarsmıştır. Bireyler ve devletlerin etkileşimi teknolojik gelişmelerle birlikte iç içe geçmiştir. Devlet odaklı düşünülen bir uluslararası ilişkiler perspektifi de bu konuda güvenlik algısının anlaşılmasını zorlaştırmaktadır. Çalışma içerisinde vurgulanan güvenlik ikilemi ve risk toplumu gibi kavramların tartışıldığı boyut çok yönlü ilişkiler ağında dikkat çekicidir. Her şeyden önce insan doğasındaki çatışma güdüsü ve bu doğaya güvenilmezlik her türlü aracın şiddete evrilmesi yönüyle önemli tespitlerdir.

Uluslararası güvenlik açısından, devlet-birey-güvenlik ilişkisi karar alıcıların adımlarında çıkar kavramını yine ön plana çıkarmaktadır. Siber uzay bu bağımlılığın çehresini genişletmiştir. Bu konuya ilişkin teorik bir yaklaşım sergilemede, olgusal bütünlüğün açıklanamayışı ciddi bir sorundur. Devletlerin varlık sebebinin mücadeleye dayandığı düşünülürse siber uzay oldukça karanlık ve tehlikeli bir seçenektir. *"Siber güvenlik"* kavramının içindeki güvenlik aslında savunma odaklı bir anlayışın

[10] NATO da tıpkı ülkeler gibi siber saldırılara maruz kalmaktadır. Özellikle yığın e-posta saldırıları, web sitelerinin çökmesine yönelik saldırılar ve NATO sunucularına karşı sürekli saldırılar düzenlenmektedir. Diğer taraftan NATO, siber casusluk faaliyetlerinin de artmakta olduğunu, bu konuyla ilgili olarak da savunma faaliyetlerinin artması ve güçlendirilmesi gerektiğini belirtmektedir.

ürünüdür. Siber alandan kendini koruma ya da en az zararla sorunları atlatma aslında kavramın bütünlüğü açısından daha açıklayıcıdır.

Uluslararası politika temelinde tanımının bütünlüğü yönüyle dahi zorlandığımız *siber savaş* gibi kavramlar hukukunun ve temellerinin belirlenemediği bir düzeydir. Güvenlik ikileminin siber boyutta ne ifade ettiği ya da küresel risk toplumunda siber politikaların uygulanabilirliği gibi hususlar konuya sadece bir yaklaşım sunabilmektedir. Siber güvenlikte teknik hususlarda kesin sonuçlar ve tanımlar karşımıza çıkarken siber politikalar üretmek ya da siyaset bilimi çerçevesinde analizler yapmak bir hayli zordur. Uluslararası alanda bir yasal otorite olmadığı için devletler kendi güvenliklerini sağlamada maliyetsiz ve daha az rahatsız edici seçeneklere yönelmektedir.

Dünya siyasetini meşgul eden siber güvenlik bireyler ve devletler adına cazip bir seçenektir ve amaç çıkar mücadelesi ise daha iyi bir seçenek de günümüz koşulları adına yoktur. Konvansiyonel ya da nükleer mücadeleye dayalı güç çarpışmaları yıkıcı etkilerini daha kesin şekillerde göstermektedir. Siber uzay bu konuda daha kapalı ve çoğu zaman da yıpratıcı tercihleri bizlere sunmaktadır. Aslında gelişen ve değişen her silah, şartlar devletlerin çıkar arzusunu körüklemektedir. Yeniliğin beraberinde getirdiği çevresel, ekonomik ve güvenliğe ilişkin sorunlar da siber güvenliğin çehresinde gerçekleşmektedir.

KAYNAKÇA

Aksu, Muharrem ve Turhan Faruk (2012), "Yeni Tehditler, Güvenliğin Genişleme Boyutları ve İnsani Güvenlik", *Uluslararası Alanya İşletme Fakültesi Dergisi,* 4(2), 69-80.

Bayraktar, Gökhan (2015), *Siber Savaş ve Ulusal Güvenlik Stratejisi,* İstanbul: Yeniyüzyıl Yayınları.

Beck, Ulrich (2009), *World at Risk*, Cambridge: Polity Press.

Bilgiç, Ali (2012), "Güvenlik İkilemini Yeniden Düşünmek: Güvenlik Çalışmalarında Yeni Bir Perspektif", Mustafa Aydın ve diğerleri (Ed.), *Uluslararası İlişkilerde Çatışmadan Güvenliğe,* 1. Baskı içinde (337-352), İstanbul: İstanbul Bilgi Üniversitesi Yayınları

Birdişli, Fikret (2016), *Teori ve Pratikte Uluslararası Güvenlik: Kavram-Teori-Uygulama,* Ankara: Seçkin Yayıncılık.

Booth, Ken (2014), *Dünya Güvenliği Kuramı*, (Çev. Çağdaş Üngör), İstanbul, Küre Yayınları.

Buzan, Barry (1991), *People, States & Fear: An Agenda For International Security Studies in the Post Cold War Era,* 2nd Ed., Hemel Hampstead: Harvester Wheatsheaf Publishing.

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

Der Derian, James (2009), *Critical Practices of International Theory Selected Essays*, New York: Routledge Publishing.

Elmas, M. Salih (2013), *Modern Toplumun Güvenlik Çıkmazı: Tehdit, Risk ve Risk Toplumu Perspektifinden Güvenlik,* Ankara: USAK Yayınları.

Erendor, Mehmet Emin (2016), "Risk Toplumu ve Refleksif Modernleşme Çerçevesinde Siber Terörizm: Tanımlama ve Tipoloji Sorunu", *Cyberpolitik Journal,* 1(1), 114-134.

Erdoğan, İbrahim (2013), "Küreselleşme Bağlamında Yeni Güvenlik Algısı", *Gazi Akademik Bakış Dergisi,* 6(12), 265-292.

Giddens, Anthony (1998), *Ulus Devlet ve Şiddet,* (Çev. Cumhur Atay), İstanbul: Kalkedon Yayınları.

Hathaway, Melissa E. ve Klimburg, Alexander (2012), "Preliminary Considerations: On national Cyber Security", Alexander Klimburg (Ed.), *National Cyber Security: Framework Manual,* 1. Baskı *içinde* (1-44), Tallinn: NATO CCD COE Publication.

Hettne, Björn (2012), "Teori ve Pratikte Güvenliğin Bölgeselleşmesi", Mustafa Aydın ve diğerleri (Ed.), *Uluslararası İlişkilerde Çatışmadan Güvenliğe,* 1. Baskı *içinde* (353-365), İstanbul: İstanbul Bilgi Üniversitesi Yayınları.

Jervis, Robert (1978), "Cooperation Under the Security Dilemma", *World Politics,* 30(2), 167-214.

Karabulut, Bilal (2015), *Güvenlik: Küreselleşme Sürecinde Güvenliği Yeniden Düşünmek*, Ankara: Barış Kitabevi.

Keleştemur, Atalay (2015), *Siber İstihbarat*, İstanbul: Level Kitap.

Krickovic, Andrej (2016), "Catalyzing Conflict: The Internal Dimension of the Security Dilemma", *Journal of Global Security Studies,* 1(2), 111-126.

Libicki, Martin C. (2007), *Conquest in Cyberspace: National Security and Information Warfare,* Cambridge: Cambridge University Press.

Sard, Michael (2014), "Cyber-Politics: The Technological Arms Race between States and Citizens", *Eurasia Group,* https://www.pwc.com/jp/en/japan-knowledge/arch ive/assets/pdf/cyber-politics-1408.pdf (14.06.2016).

Sönmezoğlu Faruk (2014), *Uluslararası Politika ve Dış Poltiika Analizi,* 6. Baskı, Der İstanbul: Der Yayınları.

Tang, Shiping (2009), "The Security Dilemma: A Conceptual Analysis", *Security Studies,* 18(3), 587-623.

The Texas Politics Project (2016), "Policy Making and Policy Implementation", https://texaspolitics.utexas.edu/archive/html/bur/features/0303_01/policy.html (09.06.2016).

Williams, Michael (2005), *The Politics of Risk: The US, Europe and Proactive Security in the 21st Century,* http://citation.allacademic.com/meta/p_mla_apa_research_citation /0/7/1/0/6/pages71061/p71061-1.php (09.08.2016).

Yılmaz, Sait (2014), *Uzay Güvenliği,* İstanbul: Milenyum Yayınları.