ASR Journal
ACADEMIC SOCIAL RESOURCES JOURNAL
2020, Vol:5, Issue:18, pp:535-548
e-ISSN: 2636-7637

Arrival Date : 27.09.2020
Published Date : 18.11.2020
DOI Number: 10.31569/ASRJOURNAL.108
RESEARCH ARTICLE

REALİST BİR PERSPEKTİFTE SİBER GÜVENLİK KAVRAMI

CYBER SECURITY CONCEPT IN A REALIST PERSPECTIVE

Burhan BARLAS
Muğla Sıtkı Koçman Üniversitesi, İİBF, Kamu Yönetimi, Doktora Öğrencisi, Muğla/Türkiye
ORCID ID: https://orcid.org/0000-0002-2932-3941

Reference Barlas, B. (2020). "Realist Bir Perspektifte Siber Güvenlik Kavramı", Academic Social Resources Journal, (e-ISSN: 2636-7637), Vol:5, Issue:18; pp:535-548

ÖZET

Uluslararası İlişkiler disiplini çerçevesinde her geçen gün yeni teoriler, düşünce ve fikirlerle birlikte gelişmesine rağmen, güvenliğe yönelik açıklamalarda realist perspektifte asıl önemli kavram devlet güvenliğinin korunması üzerinedir. Ancak küreselleşen dünya ve gelişen teknolojiler nedeniyle devlet kavramının yalnızca korunması gereken bir unsur olma olgusu geçerliliğini yitirmiştir. Özellikle, bireyler, örgütler ve bir çok ulus üstü kurumun bir aktör olarak uluslararası ilişkiler sistemine katılması sonucunda güvenlik konseptinde bir takım değişiklikler yapılması gerekmiştir. Ayrıca Soğuk Savaşın ardından, teknolojinin de hızla gelişim göstermesi ve internetin ve bilgisayarların giderek yaygınlaşmasıyla yeni bir ortam olan siber ortam ortaya çıkmıştır. Bu durum güvenlik algısını olumsuz etkilemiştir. Güvenlik kavramı açıklanırken artık "Siber Ortam" kavramının önemi siber ağ yöntemiyle elde edilen kazançların yanında ortaya çıkan yeni güvenliğe yönelik tehditler oluşturması açısından Uluslararası İlişkiler Disiplininin bir parçası haline gelmiş ve klasik güvenlik teorileri tarafından açıklanmaya çalışılmıştır. Özellikle Soğuk Savaş döneminde önemli bir yere sahip olan Realist bakış açısı, sorunlara çözüm bulamaması ve yeni teknolojik gelişmelerin yeni sorunlar ortaya çıkartması üzerine eski önemini yitirmiştir. Ancak bu yaşanan gelişmelere rağmen uluslararası ilişkiler teorilerini etkilemeyi başarmış olan Realizmin, Siber Güvenlik kavramını nasıl yorumladığı ve bu konuda ki temel görüşlerinin artık kabul edilip edilmeme konusu tartışılmaya başlanmıştır. Realizm üzerine yapılan yeni tartışmalar ile yeni argümanlar ortaya çıkmıştır. Bu çalışmada Siber güvenlik kavramları detaylı bir şekilde açıklanırken bir yandan siber güvenlik kavramının uluslararası güvenliği nasıl etkilediği konusu açıklanmaya çalışılacak diğer yandan ise Realist perspektifin sistemdeki değişiklikleri nasıl tanımladığını ve bu değişimleri ifade edip edemediği konusu üzerinde durulacaktır.

Anahtar Kelimeler: Realizm, Siber Güvenlik, Uluslararası Güvenlik

ABSTRACT

Despite the development of new theories, ideas and ideas every day within the framework of the International Relations discipline, the main concept in the realist perspective in the explanations for security is the protection of state security. However, due to the globalizing world and developing technologies, the fact that the concept of the state is only an element that needs to be protected has lost its validity. Especially, as individuals, organizations and many supranational institutions joined the international relations system as an actor, some changes had to be made in the concept of security. In addition, after the Cold War, with the rapid development of technology and the increasing prevalence of the Internet and computers, a new environment, the cyber environment, emerged. This situation negatively affected the perception of security. While explaining the concept of security, the importance of the concept of "Cyber Environment" has now become a part of the International Relations Discipline in terms of creating new threats to security as well as the gains obtained by the cyber network method and it has been tried to be explained by classical security theories. The Realist perspective, which had an important place especially during the Cold War, lost its former importance due to the inability to find solutions to the problems and the new problems caused by new technological developments. However, the issue of how Realism, which has managed to influence international relations theories despite these developments, interprets the concept of Cyber Security and whether its basic views on this subject will be accepted or not has started to be discussed. With new debates on realism, new arguments have emerged. In this study, while explaining the concepts of cyber security in detail, it will try to explain how the concept of cyber security affects international security, on the other hand, it will be focused on how the Realist perspective defines the changes in the system and whether it can express these changes.

Keywords: Realism, Cyber Security, International Security

1. GİRİŞ

Teknolojideki ilerlemeler ve ağa bağlı makinelerin yükselişi, belki de sosyal etkileşimde ve toplum için birçok nesil boyunca ilerlemede en dramatik değişikliklere yol açmıştır. Dijital bağlanabilirliğin hem realist bir çerçevede güç dağıtımını değiştirme ve zorlayıcı amaca ulaşma fırsatı sunması hem de devletler ve diğer örgütlerdeki güvenlik açıklarına katkıda bulunan bir faktör olarak görülebileceği düşünüldüğünde, bu ilerlemelerin güvenlik açısından önemli etkileri olmuştur.

Uluslararası İlişkilerde ortaya çıkan bir konu olarak siber güvenlik kavramı bilinse dahi dikkat çekici olan asıl durum siber güvenlik kavramının yeniliğidir. Bilgi ve İletişim Teknolojilerinin yaygınlaşmasıyla birlikte, siber güvenlik politika yapıcılar için önemli bir endişe kaynağı oluştururken, uluslararası ilişkiler teorisyenleri için büyük bir ilgi kaynağına dönüşmüştür. Gerek ekonomik kayıplara yol açma ihtimaliyle gerekse sınıflandırılmış hükümet verilerinin çalınması veya kritik altyapının hedeflenmesi yoluyla işletmelere kadar, siber güvenlik küresel olarak ülkelerin ekonomik ve ulusal güvenliği için önemli bir zorluk teşkil etmektedir.

Teknolojik gelişmelerin devamlı ve her yerde bulunması artık hayatımızın bir parçası olması yadsınamaz bir gerçektir. Bu gelişmeler hayatımızı etkiler çünkü bilgiyi nasıl ilettiğimizi ve analiz ettiğimizi değiştirmektedir; bu durum ise dünyayla etkileşim şeklimizi değiştirir. Siber sistemi oluşturan siber uzay kavramı ise artık kara, deniz, hava ve uzaydan sonra beşinci savaş alanı olarak kabul edilmektedir ve geleneksel çerçeveler bu nispeten yeni çatışma biçimini anlamamıza yardımcı olmaktadır.

Değişim bir takım bağımlılığa yol açabilmektedir ve bu nedenle siber çatışma ve siber savaş, uluslararası ilişkiler alanında endişe verici konular haline gelmiştir. Teknolojinin artması sonucunda yaşanan değişimler sonucunda telgraftan telefona, telefondan bilgisayar sistemine yani her teknolojik ilerlemeye bağımlı hale gelmekteyiz ve bu bağımlılıklar sonucunda ise yeni güvenliğe yönelik tehditlerin ortaya çıkmaktadır. Teknolojinin karmaşık doğası göz önüne alındığında, teknolojiye bağımlılık korku söylemini harekete geçirme eğilimindedir.

Uluslararası sistemdeki teknoloji, politika ve ordu arasındaki bağlantı göz önüne alındığında; teorik, ampirik ve eleştirel inceleme için olgunlaşmış yeni bir konsept ortaya çıkmaktadır. Ortaya çıkan siber güvenlik kavramı ise öncelikle uluslararası ilişkilerin temel teorilerinden olan realizmle açıklamak önem arz etmektedir. Çünkü gerek uluslararası ilişkiler adına gerekse de teorilerin ortaya çıkması için dönüm noktası olarak kabul edilebilecek öneme sahip bir konumu bulunmaktadır. Temel olarak realizm, uluslararası ilişkiler disiplininin ortaya çıkış aşamasında var olan kavramsal çerçevenin ve ontolojik, epistemolojik temellerin meydana geldiği ilk teorik sistemin önemli bir tarafını oluşturmuştur (Ateş, 2009: 13). Bu sebeple, siber güvenlik kavramını bu bakış açısına göre açıklamak disiplin için kuramsal özerkliğin oluşmasında önemli bir nitelik kazandıracaktır.

Realizm kavramı uzun zamandır uluslararası ilişkiler alanında egemen bir paradigma olmuştur ve uluslararası politika hakkında genel bir varsayımlara dayanmaktadır. Devletlerin, merkezi otoriteden yoksun uluslararası bir sistem içinde bağımsız birimler olarak faaliyet gösteren ve güç ve güvenliği sağlamak için rasyonel olarak kendi çıkarlarının peşinde koşan en önemli aktörler olduğu bir gerçektir (Schmidt, 2002: 9). Uluslararası ilişkiler disiplini ve devletlerarası iletişimin, birbirleriyle olan etkileşimin giderek gelişmesi ve değişmesi sonucunda birçok etmen Uluslararası İlişkiler içine dâhil edilmeye başlanmıştır. Özellikle modernleşen ve giderek küreselleşen dünya ile teknolojik alanlarda ortaya çıkan yeni teknolojik gelişmeler gerek Uluslararası İlişkileri gerekse de bu disiplinde yer alan aktörleri etkilemiştir. Siber alanın direkt olarak devletlerarası ilişkileri etkileyen bir sistem haline dönüşmesi veya bireyler ile diğer aktörler arasındaki durumları etkilemesi sonucunda bir nevi realizm'in devlet egemen bakışı yerine bireye kadar indirgenen bu alan birden disiplin içinde dikkat edilmesi gereken bir durum haline dönüştüğü için bu alanın çalışma konusu haline gelmiştir. Özellikle egemenlik ilkelerinin ciddi şekilde kısıtlanması bu durumda etkili olmuştur (Reardon ve Choucri, 2012: 13). Temel olarak bireyler tarafından öncelikle gerçekleştirilen siber tehditler ve saldırılar devletlerin egemenliğini sorgulayan bir sistem haline

dönüşüm geçirmiştir. Devletler ise bir yandan kendi ulusal veritabanı sistemlerini korumaya çalışırken diğer yandan ise gerek iktisadi sistemleri yani bankaların gerekse günümüzde pandemi sürecinde yaşanan online eğitim sisteminin korunması için siber güvenliğe yönelik birtakım tedbirler almak durumunda kalmışlardır.

Dolaylı olarak yapılmaya başlanan bu siber saldırılar özellikle internet uzay sisteminin meydana gelmesi ve bilgisayar sistemlerinin kullanılmaya başlanmasıyla etkisini göstermiştir. İnternet ağının icat edilmesi ve bilgisayar sistemlerinin giderek yaşamınızda önemli bir kolaylık sağlayıcı sistem olarak yer edinmesi güvenlik ve saldırı sistemlerinin de yöntemini değiştirmiştir. Kısacası, uluslararası sistemde var olan ve yüzyıllar boyunca doğrudan müdahale etme yöntemi, siber uzay sistemiyle birlikte dolaylı bir yönteme dönüştüğü görülmüştür. Özellikle 21. yüzyıl, siber sisteme yönelik bir tehdidin bir kitle imha silahı gibi etkili olduğu bir yüzyıl olmuştur (Bilgiç, 2011: 130-135). Bunun en temel nedeni ise internet üzerinden yapılabilecek bir saldırının artık tüm devlet kurumlarının sistemlerini bile etkileyebilecek kadar güçlü hale gelmesidir. Siber veya sibernetik denilen bu tehdit, bireylerin, toplumların ve devletlerin güvenliğini ciddi oranda sarsmıştır.

Ortaya çıkan siber güvenlik alanı, güvenlik ve rekabete, gücün dağılımına, hücumun savunmaya göre avantajına ve caydırıcı stratejilerin faydalarına odaklanarak realizmden etkilenen perspektiflerin yeniden dirilişini sergiler ve böylelikle bunlarda realizmin rolünü tartışarak değerlendirme fırsatı sunmaktadır. Bu çalışmada öncelikle mevcut siber güvenlik söyleminde gerçekçi bir dizi belirli konuya değinilecek sonrasında ise, realist teoriye ve siber güvenlikle nasıl ilişkili olduğuna genel bir bakış açısı sunulacaktır. Ayrıca realizmin siber alandaki devlet davranışının tanımlayıcı ve kuralcı bir teorisi olarak ilgisini değerlendirilmiş ve realizmin siber güvenlikteki temel sorunları gündeme getirmeye yardımcı olmasına rağmen, genel olarak teorinin siber güvenliğin dinamiklerini açıklama açısından yeterli olup olmadığı üzerine durulacaktır.

2. SİBER GÜVENLİK KAVRAMINA KAVRAMSAL BİR YAKLAŞIM

Özellikle 21. yüzyıldan itibaren siber güvenliğe yönelik tehditler tüm dünyayı tehdit etmektedir. Bu saldırıların giderek artması nedeniyle aktörler güvenliklerini bu alanda koruyabilmek adına yeni politikalar üretmek durumunda kalmışlardır. Bu aktörlerden birçoğu, finans kaynaklarının bir bölümünü siber güvenliğe yatırarak kendi güvenliklerini sağlamak için faaliyetlere başlamışlardır. Bunun en temel sebebi ise gerek bireysel gerekse devlet sisteminin siber dünya ile giderek iç içe olmaya başlamasıyla birlikte ortaya çıkan güvenliğe yönelik tehditler riski atmış/atmaktadır. Bu nedenle siber güvenlik alanına büyük yatırımlar yapan aktörler, bu alanda bireyleri uzmanlaştırmak amacıyla yeni bir takım politikalar uygulamaya başlamıştır (Ünver ve Canbay, 2010: 96-97).

Siber kavramı, kökeni Fransızca olan "sibernetik" kelimesiyle bağdaştırılmaktadır. Temel olarak ise İngilizce kökenli "cyber" kelimesinin Türkçeleştirilmiş halidir. Siber kavramı, internetin ortaya çıkmasıyla birlikte yaygınlık kazanmış ve hemen hemen her kavramda çok sık ifade edilmeye başlanmıştır. Bu sebeple gerek uluslararası sistemde gerekse doğal yaşamda yeni bir ortama zemin hazırlamıştır. Siber ortamın ortaya çıkmasındaki en önemli unsur ise sanal sistemdir. Sanal sistem ise temel olarak internet sistemi olarak akla gelmektedir. Buradan da hareketle siber ortam kavramı internet ağını da içerisinde barındıran bir üst terim olarak ortaya çıkmaktadır. Teknolojik aygıtlardan bilgisayar ve cep telefonu sayesinde kullanılabilen internet ile hem bilişim hem de diğer tüm alanlardaki teknolojik gelişimi takip etmek kolaylık sağlamasının yanında bir bağımlılık haline gelmiştir. Bilişim teknolojisiyle ortaya çıkan sistemlerindeki bilgi ve iletişim teknolojilerini kullanarak sağlanan her türlü hizmetin tüm dünyaya ve hatta uzaya yayılmış durumda olması ve bunları birbirine bağlayan ağların mevcut olması siber ortamı oluşturmaktadır (Kara, 2013: 4).

Siber uzay kavramı ise temel olarak "Siber etki alanı, ağa bağlı tüm bilgisayarların İnternetini değil, aynı zamanda intranetleri, hücresel teknolojileri, fiber optik kabloları ve uzay tabanlı iletişimi de" içermektedir. Siber uzay, rakip kaynakların ekonomik yasalarını ve egemen gerekçelendirme ve kontrolün siyasi yasalarını izleyen fiziksel bir altyapı katmanına sahiptir (Nye, 2011: 19). Siber uzayın bu katmanlaşması siyasi söylemde kritiktir çünkü devleti analizin dışında bırakmak

imkansızdır. Devletler, Wassenaar Anlaşması (ikili kullanım teknolojilerine erişimi sınırlandıran) gibi programlar aracılığıyla teknoloji ve erişim üzerindeki tekeli hala kontrol etmektedir. İnternet üzerindeki etki alanlarını yöneten Uluslararası Atama Adları ve Numaraları Kurumu (ICANN) ve siber güvenlik konusunda çeşitli Hükümet Uzmanları Grubu raporlarını bir araya getiren Birleşmiş Milletler ile kurumlar da bir rol oynamaktadır (The Wassenaar Arrangement, 2020).

Siber uzay terimi, günümüzde halen etkisini sürdürmektedir. Ancak siber uzay kavramının yerine Ulusal Siber Güvenlik Stratejisinde kavramın ismi siber ortam kavramına dönüşüm geçirmiştir. Bunun en büyük nedeni ise siber ortam kavramı, kavramsal çerçeve olarak birçok alanda ve bölgede etkili olmaktadır. Günümüzde hizmet sektörü tamamen siber ortamda gerçekleşmektedir. İnternet başta olmak üzere, gelişmiş teknolojik sistemler sayesinde internetin olmadığı ve bilgisayarların sayısal verilere ulaştığı alanlarda da siber ortam söz konusu olmaktadır. Buradan da anlaşılacağı üzere kısaca siber ortam için şu ifade kullanılabilir: internet uzay ağının etkilediği alanlar başta olmak üzere, internetin sisteminin olmadığı fakat yine bilgisayar sistemleri aracılığıyla ortaya çıkan sayısal bilgi verileri ve yine internet üzerinden düzenleme gerektiren elektronik aygıtlar vasıtasıyla da ulaşılabilen tüm imgesel alanlar siber ortamı oluşturmaktadır (Hill ve Hughes, 1998: 17-21).

Siber ortam teknolojik açıdan bir çok fayda sağlamıştır. Ancak unutulmaması gereken bir etmen ise fayda kadar önemli ölçüde zararlara da yol açmaktadır. Bu yolların çoğu internet ortamında gerçekleşmektedir. Örneğin, internet aracılığıyla iletişim teknolojilerini kullanıp, herhangi bir kimseyi rahatsız etmek veya küçük düşürücü sözlerde bulunmak gibi faaliyetler veya bir kimseye ait bilgilerin ele geçirilip o bilgilerle kişinin tehdit edilmesi gibi durumlar sayılabilir. Bu zararlar genel olarak güvenliği tehdit etmekte ve güvensizlik ortamına sebebiyet vermektedir. Bu durum siber güvenlik kapsamına girmekte ve yeni bir alan oluşturmaktadır. Kısacası siber ortamı meydana getiren bilişim sistemlerinin saldırıları gerçekleştiren hackerlardan, sistem ele geçirme veya sistemleri tamamen ortadan kaldırma amaçlı virüslerden ve tehditlerden korunması amacıyla siber güvenlik alanları/ortamları oluşturulmaya çalışılmıştır. Bu kapsamda siber güvenlik, siber ortama zarar verebilecek saldırıları önlemeye çalışmakta veya bu zararları en aza indirmeye ya da tamamen ortadan kaldırmaya yönelik faaliyetler gerçekleştirmektedir denilebilir (Nojeim, 2010: 125-126).

2.1. Siber Güç

Siber güç terimi, hesaplama teknolojilerinin devam eden politik önemini vurgulamaktadır. Politika, etkinin dağılımı ile ilgilidir ve siber güç, uluslararası ve yerel ortamlarda kaldıraç, erişim ve gücü kontrol etme girişimlerinin bir başka türüdür. Siber güç kavramı, siber uzayda tipik kontrol ve tahakküm biçimlerini uygulama yeteneği olarak tanımlanmaktadır (Valeriano ve Maness, 2015: 28). Devletlerin elinde bulundurduğu kaynaklar sebebiyle, devletlerin siber gücü kullanma konusunda üstünlüğe sahip olmaya devam etmesini olağan bir durumdur. Bu çerçevede ise devletler hala siber şiddet üzerinde tekel durumunu korumakta ve devlet dışı aktörlerin siber gücü kullanma çabaları çoğu zaman başarısız olmaktadır.

Ancak unutulmaması gereken bir durum bilişim sistemlerinin kolay taşınılabilirliği ve siber ortama her yerden erişim sağlanabilmesi nedeniyle devlet dışı aktörler ve teröristler bu gücü kullanmak için her yolu denerler, fakat taktikleri genellikle etkisizdir veya eylemlerini gizlemek isteyen ulus-devletler için sadece örtü olarak kullanılmıştır (Valeriano ve Maness 2015: 164-187). Yani kısaca devletler, siber savaş araçlarını, devlet dışı aktörlerin rakipleriyle rekabet etmesi muhtemel olmayan insan gücüne, araştırma ve geliştirmeye ve eğitime yatırım yapmak için elindeki kaynakları en iyi şekilde kullandıklarından dolayı yine en iyi konumda olmaya devam etmektedir.

Siber güç kavramı konusunda özellikle disiplinde kullanılan tanım ve terimleri keşfetmek için siber güvenlik alanında çok zaman ve çaba harcanmıştır. Siber güvenlik, dijital ve hesaplama teknolojilerinden gelen tehdit fırsatlarını ifade etmektedir. Tüm güvenlik teorileri gibi, mükemmel koruma fikri de yalnızca bir teori olarak kalmaktadır. Ağ tabanlı tehditlerden kaçınmanın tek yolu, tüm elektronik cihazları internet ağına bağlamamaktır ancak bu durum teknolojinin kullanılma durumu çerçevesinde ne kadar yararlıdır konusu tartışmaya açıktır.

Siber güç, kavramı "siber alanın elektronik olarak birbirine bağlı bilgi kaynaklarını kullanarak tercih edilen sonuçları elde etme yeteneği" olarak tanımlanmış ve uluslararası ilişkileri dönüştürme potansiyeli öne çıkan bir tartışma haline gelmiştir. Realist literatürde siber güç teorisi olmamasına rağmen, realizm, aktörler arasındaki güç dağılımını ve bunun çatışmayla nasıl ilişkili olduğunu düşünmek için bir çerçeve sunmaktadır (Nye, 2011: 123).

Siber güç ile yapılan çatışmaların ve savaşların diğer gerçek alanlarda yapılan savaşlara göre görece düşük maliyeti nedeniyle, geleneksel olarak daha zayıf durumların daha güçlü durumlara meydan okuduğu ve sistemdeki güç dağılımını yeniden yapılandırdığı varsayılmaktadır (Lango, 2016: 12).

2.2. Siber Tehdidin Doğası

Son yüzyılın en önemli icatlarından birisi olarak görülen internet sistemi, elektronik haberleşmenin yanında diğer bütün işlemlerin daha hızlı ve kolay bir şekilde yürütülmesini sağlamıştır. Özellikle küreselleşme çerçevesinde bilişim ağı sayesinde haberleşme alanında meydana gelen değişimlerle birlikte iletişim ağını genişletmiştir. Ancak bu durum her ne kadar yarar sağlasa bile bir takım önemli ve yeni güncel problemleri yanında getirmiştir. Özellikle kişisel kullanım aracı olan cep telefonu ve bilişim teknolojilerin bireylerde bağımlılık yaratması sonucunda öncelikle fiziki ve diğer yandan ise ruhsal birtakım problemlere yol açmıştır (Kara, 2013: 14-15). Bir yandan radyasyon yayma durumu nedeniyle kanser vakalarının artması, bedensel metabolizmalarda bozulma (göz bozukluğu, fiziksel rahatsızlıklar) siber tehdidin bir nebzede olsa fiziki zararları olarak karşımıza çıkmaktadır. Ancak siber alanda yaşanan saldırılar sonucunda bireyler yine dolaylı olarak da olsa birtakım problemlerle karşılaşabilmektedirler (baraj sistemlerine yönelik yapılan siber saldırılar sonucunda gerçekleşen elektrik kesintileri sonucunda bireyler dolaylı bir şekilde etkilenebilmektedirler).

Özellikle bu teknolojik aygıtların giderek çoğalması ve geniş bir alanda kullanılması sonucunda, siber saldırılar çerçevesinde en büyük tehdidi oluşturmaktadır. Günümüzde devlet dışı aktörlerin ve teröristlerin sosyal medya kullanarak bireyleri etkilemeleri ve kendilerine dahil etmeleri olası bir durumdur. Ayrıca aynı Fethullahçı terör örgütü'nün (FETÖ) yaptığı "Bylock" gibi uygulamalar kullanarak haberleşme ve iletişim yoluna gitme imkânı da sağlamaktadır. Kişisel verilerin korunması konusunda ortaya çıkan açıklar sonucunda ise bireysel anlamda finansal kayıplara veya sanal ortamda oluşturulacak olan sosyal medya hesaplarıyla yanlış bilgilerin oluşturulması özellikle otokrasinin olduğu devletlerde bir ötekileştirme unsuru olarak kullanılabilir, bu sayede ise bir başkasına zarar verilebilir. Temel olarak bireylerin, sosyal medya üzerinden bir saldırıyla karşı karşıya kalması durumudur. Diğer yandan ise yine tehditlere de maruz kalabilmektedir. Tüm bunlar siber saldırılar/saldırganlar olarak görülmektedir (Hoffman ve Schweitzer, 2015: 72- 74).

Ancak bireylerin yanında devlet kuruluşları ve diğer aktörlerde siber güvenliğe yönelik daha geniş bir anlamda tehdit algısı içerisine girebilirler. Bu anlamda siber teröristler, devlet kurum ve kuruluşlarına karşı yapacakları faaliyetlere göre hem içeriden kaynaklanan saldırılar hem de dışarıdan kaynaklanan saldırılar uygulayabilirler (Bıçakçı, 2012: 214). Devlet kurumlarının içerisinden kaynaklanan saldırılarda, kurumların bilgi ve iletişim ağına erişimi olan herhangi biri tarafından yapılan saldırılardır. Dışarıdan kaynaklanan saldırılar ise; kurum dışından veya uluslararası sistem üzerinden yapılmaya çalışan saldırılardır. Yani kurumda çalışmayan kişiler tarafından kurum içi eylemlere müdahale edilmeye çalışılmasıdır. Bu çalışmalar, sistemi ortadan kaldırma ve bilgileri stratejik bilgileri ele geçirmek üzerine olabilir ve genellikle hackerlar ve teröristler tarafından uygulanmaktadır (Kara, 2013: 9).

Siber güvenlik bilimindeki son eğilimin çoğu, siber tehdidin doğasını değerlendirmeyi amaçlamaktadır. Tehdit çerçevesini kabul etmenin politika geliştirme üzerinde feci bir etkisi olabilir. Tehditlerin abartılı göründüğü düşünüldüğünde, yapılandırmacı çerçevelerin siber tehdit algılarını incelemede kritik olduğu görülmektedir. Siber tehditlerin doğası ve bunlarla ilişkili anlatılar büyük ölçüde sosyal olarak yapılandırılmıştır ve başka türlü özgür toplumlarda İnternetin güvenlikleştirilmesini sağlayabilmektedir (Guitton, 2013: 23).

Siber tehdidin doğasının genellikle tartışmadaki aşırılıklar tarafından ezildiğini ve nüansların söylemde tipik olan abartılı perspektiflerden daha kritik olduğunu hatırlatması açısından önemlidir. Potansiyel hasarı kontrol altına almak için konsantre hükümet ve özel eylem gereklidir, ancak tehdidi olduğundan fazla tahmin etmek, terörizm tehdidini olduğundan fazla tahmin etmekle benzer bir etkiye sahip olacaktır. Oyun teorisi ve veri analizi yoluyla, düşmanlara karşı siber kaynakları kullanmanın en uygun zamanlamasının nasıl tahmin edilebileceğini göstermektedir. Belirli koşullar, devletlere, hedef devletin bilgisayar sisteminin güvenlik açığından yararlanma fırsatı ve nedeni vermektedir (Axelrod ve Iliev 2014: 1298). Kısacası, siber tehditlerin ezici çoğunluğu, düşmana zarar vermek isteyen uzun süredir devam eden rakipler arasında meydana gelir ve bölgesel anlaşmazlıklar çerçevesinde ortaya çıkmaktadır.

2.3. Siber Çatışmanın Doğası

Uluslararası ilişkiler etkileşimlerinde kullanılan siber kötülüğün şeklini tanımlamak için siber çatışma terimini ortaya çıkmıştır. Siber çatışma, "diplomatik veya askeri etkileşimleri etkilemek, değiştirmek veya değiştirmek için bilgisayar teknolojilerinin kötü niyetli ve yıkıcı amaçlarla kullanılması" dır. (Valeriano ve Maness, 2015: 21) Bu tanım, siber etkileşimlerde tipik olan aksaklık ve casusluk kampanyaları gibi daha düşük kötü niyet seviyeleri içeren tehditler arasındaki tüm etkileşimleri, siber savaşa kadar kapsamaktadır. Yeni teknolojilerin veya fikirlerin dönüştürücü olabileceği fikri hem kışkırtıcı hem de yanıltıcıdır. Teknolojideki büyük ilerlemeler, doktrinsel bir değişikliğe neden olmak için nadiren yeterli bir şekilde olurlar ve askeri etkililik hesaplamasını değiştirmedeki devrilme noktası da bulunmamaktadırlar.

Bu durumda ise mevcut uluslararası ilişkiler teorilerinin siber çatışma araştırmalarına herhangi yararlı bir şekilde katkıda bulunamayacağını ve siber tehdidin uluslararası etkileşimlerdeki zararı arttıracağı için eşi görülmemiş bir durum olduğunu iddia eden bir olgudan daha net bir şekilde görülmemektedir. Siber çatışmaların teorik boyutunu anlamak için yeni olgular ve yeni düşünme yolları gereklidir ve sosyal bilimler alanının şu anda bu konuda geniş çaplı bir açıklama yapmak teorik çerçevede yetersizdir (Kello, 2013: 8). Çünkü teknoloji ve bilişim sistemleri çok hızlı değişiyor ve her yeni bir sistemsel açık bulunması durumunda bu açıklığı kapatabilmek adına yeni uygulamalar ortaya çıkmaktadır. Bu sebeple teorilerin düşünsel boyutu şu an için yetersiz kalmaktadır.

Siber çatışmanın doğasında var olan bir diğer kavram ise siber abluka kavramıdır. Öncelikle hizmet reddi (DDoS) olmak üzere, belirli siber çatışma yöntemlerini mağdur devletin saldırganlar tarafından ekonomik olarak boğulabileceği deniz ablukalarına benzetilebilmektedir. Örneğin, Rusya'nın Estonya'da 2007 yılında uygulamış olduğu saldırı sonucunda (DDos saldırıları), birçok sıradan vatandaşın için günlük ekonomik hayatını kesintiye uğramıştır. Rusya'nın 2. Dünya Savaşı sonrasında Nazi savunmasına karşı Estonya'ya dikmiş olduğu heykelin 2007 yılında kaldırılması büyük tepki görmüş ve Rus siber teröristleri tarafından yapıldığından şüphelenilen saldırılar sonucu ülkenin ulusal bilgi sistemleri, internet hizmet sağlayıcıları ve bankaları çok büyük zarar görmüştür. Tarihteki ilk siber saldırı olarak görülen bu olayda, Rusya "siber abluka" yaparak ekonomik zararlara yol açmıştır (Russell, 2014, 56-58). Siber saldırıların doğasını kestirmek kolay değildir. Her yerden ve herhangi bir sisteme karşı gerçekleşebilir.

3. SİBER GÜVENLİK KAVRAMI VE ULUSLARARASI GÜVENLİK

Uluslararası sistemde doğal olarak bulunan anarşik yapısını ortadan kaldırmak adına devlet merkezli ve askeri odaklı ortaya çıkan güvenlik algısı, 1990'lardan modernleşerek devletlerin yanında bireyleri de içerisine almaya başlamıştır. Özellikle teknolojik gelişmelerle ortaya çıkan küreselleşme kavramıyla birlikte, uluslararası güvenliğin yalnızca askeri boyutlarda olmadığını görmekteyiz. Bunun temel sebebi ise küreselleşme, birden fazla etmenin bir araya gelmesiyle oluşan bir bütünlük sistemi durumudur. Diğer bir anlamda ise; yaşanan olayların ve üretilen fikirlerin, diğer medeniyetlerin kültürlerinin ve dünyaya bilişim teknolojileriyle hızlı bir şekilde yayılması durumu olarak da açıklayabilmek mümkündür (Steger, 2009: 5-9).

Tüm bunların ortaya çıkabilmesinin en büyük etmeni ise internet bilişim ağının son yüzyıldan beridir kullanılıyor olmasından kaynaklanmaktadır. Bu çerçevede siber uzay kavramı ve birbirine bağlı olduğu ağlar sayesinde, tüm dünya devletleri tarafından kullanılmakta ve teknolojilerini bunun etrafında geliştirmektedirler. Diğer yandan bireysel bazda bile herkes yavaş yavaş bilgi iletişim çağında kendine bir yer bulmuştur. Sosyal medya ağları ile iletişim, E-bankacılık ile finans işleri, E-devlet ve E-oylama ile kamusal işlerin kolayca sağlanabilmesi büyük bir kolaylık sağlamıştır ama öncesinde bahsettiğimiz gibi getirdiği yarar kadar yeni tehditleri de yanında getirmiştir (Horowitz, 2004: 130-140).

Siber güvenliğe yönelik olgular, özellikle tehditler ve çatışmalarla birlikte hem devletleri hem de bireylerin güvenliğine yönelik bir takım yeni sorunlar ve faydalar meydana getirirken, bir ihtimal 21. Yüzyılı kapsayacak en önemli güvenliğe yönelik tehditlerden ve olgulardan birisi haline gelerek oluşturmuş olduğu siber algı kuramıyla neredeyse tüm aktörleri ilgilendirmektedir (Bıçakçı, 2013: 1-4).

Özellikle 21. Yüzyıldan sonra aktörler siber güvenliğe yönelik tehditler karşısında, Ulusal Siber Güvenlik Stratejileri ve Eylem Planları üzerine çalışmalar yapmıştır/yapmaktadır. Bu politikaların en önemli sebebi ise siber güvenliğe yönelik tehditleri bertaraf etmek ve sistemlerin işlevselliğini korumak olmuştur. Uluslararası güvenliğin korumak adına son dönemlerde hem aktörlerin hem de bireylerin siber güvenlik algısı konusunda bilinçlendirilmesi gerekmektedir. Böylece devletler özel kuruluşlar kurarak bireyleri siber güvenlik çerçevesinde eğitir ve böylece bireyler kendi savunma sistemini oluşturarak bir nevi siber asker durumuna dönüşebilir (Jordan, 1999: 202-215).

Estonya'da yaşanan siber saldırıların ardından 21. Yüzyıl, uluslararası güvenliğe yönelik tehditlerin devam ettiği bir yüzyıl olmuştur. Kırgızistan'da yapılan 2007 seçimlerinde seçim komisyonunu hedef alınarak yapılan siber saldırılar sonucunda sistemin kilitlenmesi sağlanıp ve devre dışı kalmıştır. Buradan da görüleceği üzere seçimlerin bile sanal ortamda yapıldığı bir dönemde siber saldırılar eğer fark edilmezlerse oy dağılımında yapılan değişikliklerle seçimlerin sonucu çok kolay bir şekilde değiştirilebilmektedir. Ayrıca 2009 yılında Çin ve Kuzey Kore tarafından gerçekleştirilen saldırılar ile ABD ve Güney Kore'nin bilgi ve iletişim teknolojilerinin devre dışı bırakılması bir başka örnek olarak karşımıza çıkmaktadır. Buradan da anlaşılacağı üzere artık mermi yerine siber silahlar kullanılarak sistemler üzerinden savaş yeni bir yöntem olarak karşımıza çıkacaktır (Ünver ve Canbay, 2010: 99).

Elbette yaşanan bu saldırıları engellemek yine öncesinde bahsettiğimiz gibi siber yöntemlerle olacaktır. Geçen her yüzyıl içerisinde uluslararası sistemde savaşların şekli ve yöntemi değişiklik göstermiştir. Bir nebze her geçen yıl bir önceki yıla eklenerek giderek güncellenen ve gelişen bir teknolojinin sonucudur. Temel olarak siber savaşlar topyekün savaşlara göre daha az maliyetli olması gelecek yıllarda siber savaşların çok daha artacağının göstergesidir (Kara, 2013: 40-43).

Sonuçta siber saldırılar, artık bilgisayar başından kontrol edilebilen savaşlar haline dönüşmüştür. Bu durumda ise tehdit algısını arttıran saldırıların ne zaman ve nereden geleceği veya hangi sistemi etkileyeceği konusunda belirsizlikler bulunmaktadır. Ayrıca bu dönemde saldırıya maruz kalan aktörler ve bireyler, siber güvenlik hakkında yeterli bilgiye ve ekipmana sahip olmadıklarından dolayı saldırıdan haberleri bile olmayabilmektedir. Yapılan saldırıların etkisi zamanla ortaya çıktıkça aktörler bundan haberdar olabilmektedirler. Örnek olarak; 10 Kasım 2009'da Brezilya ve Paraguay'ın birlikte kullandıkları Itaipu Barajına yapılmış saldırıdır (Ünver ve Canbay, 2010: 99). Yapılan saldırı sonucunda baraj sistemi kilitlenmiş ve her iki ülke bir takım elektrik kesintisi problemleri yaşamıştır. 2010 yılında gerçekleşen Stuxnet virüsü ile ABD ve İsrail'in İran'a yönelik nükleer sistemlerini durdurmak amacıyla gerçekleşen siber saldırı örneklerden bir diğeridir (Akyeşilmen, 2016: 1).

Geliştirilen zararlı yazılımlar, sistemleri etkileyen virüslerin, elektrik sistemlerinin kontrolü ve kesintilerin yaşanması, önceki örnekte bahsedildiği gibi seçimlere müdahale edilmesi ve daha birçok olayların ardında bu siber saldırı ihtimali bulunmaktadır. Uluslararası örgütler bile bağlı

oldukları sistemin güvenliğini sağlamak adına siber saldırıları kullanmak durumunda kalmışlardır. Bu çerçevede, Ancak Kosova Savaşı sırasında Sırbistan'a yönelik ABD-NATO hava harekâtından önce Sırbistan Hava Savunma Sistemlerine yapılan siber saldırı sonucunda sistem ele geçirilmiştir. Böylelikle Savunma Sistemleri, kilitlenmiş ve sistemlerini kullanamadıklarından dolayı ise karşılık verememişlerdir. Bu durum, öncesinde bahsettiğimiz gibi artık güvenliğe yönelik tehditler için yalnızca bir düğmenin yeterli olma durumunu ortaya koymaktadır (Hughes, 2009: 3-7).

21. yüzyılda ortaya çıkan bu siber mermi kavramı, her ne kadar sanal ortam üzerinde kullanılsa bile aktörler ve bireyler, kendi güvenliklerini sağlamak adına her türlü çabayı göstermek durumundadır. Çünkü güvenlik sadece devletleri ilgilendiren bir olgu değildir. Temel olarak devlete yönelik yapılan bir saldırı dolaylı bir şekilde de olsa bireyi etkilemektedir. Ancak modern güvenlik teorileri çerçevesinde ise devletler bireylerin güvenliğini korumak durumundadır, bu sebeple devletler bu konu üzerinde yatırım yaparak yeni siber güvenliğe yönelik önlemler almak durumundadır. Burada ki durum realizmde olduğu gibi bireyler tüm haklarını devlete vermemiştir, yalnızca güvenlik haklarını devlete sunmuşlardır bu sebeple devletler bireylerin kişisel haklarına saygılı olmalı ve onları kısıtlayıcı uygulamalardan örnek olarak sosyal medya ağlarına erişimin kısıtlanması gibi faaliyetlerden uzak durmalıdır. Başka bir değişle, demokratik sistem içerisinde var olan kurallara uyulması, toplumda barışı sağlayıcı ilkelerin oluşması, güvenlik algısının suiistimal edilmemesi, uluslararası işbirliği ortamının sağlanması, öte yandan ifade özgürlüğü başta olmak üzere, temel hak ve hürriyetlerinin güvence altına alınması ve hukuki işlemlerin çiğnenmemesi gerekmektedir. Bütün bu uygulamalar siber güvenliğin kullanılabilmesi çerçevesinde önem taşımaktadır. Çünkü siber güvenlik, toplumsal ve uluslararası güvenliğin sağlanmasında en önemli yapı taşlarından biridir (Bıçakçı, 2012: 205-226).

Burada diğer önemli olan bir etmen ise uluslararası sistemde bulunan terör kavramının da şekil değiştirme durumudur. Modern çerçevede David Rapaport tarafından tanımlanan terör kavramı özellikle teknolojinin giderek güncellenmesi ve icat edilen yeni kitle imha silahlarının ortaya çıkarttığı korku faktörünün çoğalması terörü yıllara göre şekillendirmiştir. Rapaport'a göre terör kavramının tanımlanmasında 4 ana dalga bulunmaktadır bunlar temel olarak anarşist, anti-kolonyal, yeni sol ve son olarak 20. Yüzyılda oraya çıkan dini dalgadır. Ancak belki günümüzde ortaya çıkabilecek yeni bir terör basamağı olarak siber dalgayı da bu kategoriye de ekleyebiliriz (Rapoport, 2002).

4. REALİST BİR PERSPEKTİFTE SİBER GÜVENLİK KAVRAMI

Realist gelenek, Thukydides'in MÖ 5. yüzyılda Peloponnesos Savaşı'na ilişkin analizine kadar uzanmaktadır ve burada uluslararası politikanın kaotik doğa durumunu ve iktidarın siyasi hayatta kalma açısından önemini vurgulamaktadır (Vasquez, 1995: 9-19). Bununla birlikte, farklı bir uluslararası ilişkiler teorisine eklemlenmesi, büyük ölçüde, rasyonel olarak hareket eden, kendi çıkarına sahip devletler arasındaki iktidar mücadelesine odaklanan Hans Morgenthau'ya atfedilebilir.

1970'lerde kurulan neo-realizm içinde, savunma ve saldırgan gerçekçilik arasında bir ayrım bulunmaktadır. Her ikisi de hayatta kalmanın devletin birincil nedeni olduğu konusunda hemfikirdir, ancak savunmacı realistler için çoğu devlet, bir güç dengesini hedefleyen ve böylece istikrarlı bir uluslararası sistemi sürdüren statüko güçlerdir (Waltz, 1979). Saldırgan realistler ise, devletlerin anarşik bir sistemde hayatta kalmalarını sağlamak için güçlerini en üst düzeye çıkarmayı amaçladıklarını savunmaktadırlar (Mearsheimer, 2001: 37).

Realizmin en yeni kolu olan neo-realizmde, devlet davranışını yalnızca yapısal faktörlere değil, aynı zamanda karar vericilerin algılarını ve yanlış algılamalarını içeren yerel düzeydeki değişkenleri de açıklamaktadır (Ripsman ve diğerleri, 2016: 33-35).

Realizm, devlet davranışını açıklayamaması nedeniyle veya verimli politika rehberliği sunamadığı için sorgulanmıştır. Örneğin, devletlerin realist literatürde öne çıkan bir hipotez olan güç dengesi

mantığına uygun davrandığına dair kanıt eksikliğine işaret edilmektedir (Rosecrance ve Stein, 1993: 17-21). Çelişkili öngörüleri ve empirik ilerleme eksikliği, realizmin "ilerici" paradigmadan ziyade "dejeneratif" bir paradigma olarak eleştirme yöneltir. Dahası, istatistiksel araştırmalar, realistlerin ulusal güvenliği artırdığını iddia ettiği, askeri birikimler ve ittifaklar gibi faktörlerin genellikle ters etki yaptığını ve çatışma olasılığını artırdığını göstermektedir (Senese ve Vasquez, 2008: 217-218). Bununla birlikte, güvenlik ve çatışma konularına odaklanmasıyla realizm, acil siber güvenlik sorunlarını aydınlatmak için doğal bir başlangıç teorisi gibi görünmektedir.

Güç kavramı realizmin merkezinde yer alır çünkü devletlerin yalnızca kendi çıkarları doğrultusunda hareket etmesi sonucunda devletin bağımsızlığını korur ve hayatta kalmasını sağlayabilir. Morgenthau'nun iddia ettiği gibi: "uluslararası politikanın nihai amacı ne olursa olsun, güç her zaman asıl amaçtır" (Morgenthau, 1948: 13). Realistler, gücü genellikle bir devletin sahip olduğu doğal kaynaklar, endüstriyel kapasite, askeri güç ve nüfus gibi devletin varlıklarına eşitler (Morgenthau, 1948: 80–84). Bu tür yeteneklerin devletler arasında dağılımının, uluslararası sistemde istikrar açısından önemli etkileri olduğu düşünülmektedir. Örneğin, çok kutuplu, iki kutuplu veya tek kutuplu bir güç konfigürasyonunun daha barışçıl bir dünya yaratıp yaratmadığı uzun zamandır devam eden bir tartışma olmuştur (Mearsheimer, 2006: 78-80).

Realizmin temel varsayımlarından biri, devletlerin uluslararası siyasette en güçlü ve bu nedenle en önemli aktörler olduğudur. Bununla birlikte, bilgi devrimi, geleneksel güç dinamiklerini tehdit eden devlet dışı aktörlerin daha fazla katılımı nedeniyle devletin önceliğine meydan okur (Eriksson ve Giacomello, 2006: 229). Güç yayılması teorisinde olduğu gibi, devlet dışı aktörler uluslararası ilişkilerde giderek daha önemli hale gelmekte ve bu durum özellikle bireysel suçluların, örgütlerin ve terörist grupların erişim imkanından yararlanabildiği siber alanda özellikle daha derinden ortaya çıkmaktadır. İnternet ağı yani sanal sistem, devletin egemenliğini tehdit etmek için teröristler adına farklı bir savaş ortamı oluştururken ve aktörler kendilerinin hem güvenlik sağlayıcıları hem de güvenlik açığına yol açan sistemlerin ortaya çıkmasına neden olabilmektedirler (Nye, 1990: 160).

Realizm, bazıları tarafından siber uzayı anlamak için yararlı bir çerçeve olarak kabul edilmektedir. Temel olarak siber uzay kavramı realist perspektifte "realist caydırıcılık, kriz yönetimi ve çatışma teorileri, siber uzayın istikrar mı yoksa istikrarsızlaştırıcı mı olduğunu, siber teknolojilerin yeni bir çatışma veya barış kaynağı olup olmayacağını ve devletlerin siber silah yarışına girecek mi" anlamak için kullanılabilmektedir (Reardon ve Choucri, 2012: 6).

Realizm, anarşik bir dünyada tehdide bir yanıt olarak siber silah yarış davranışının kaynağını açıklamaya yardımcı olabilmektedir. Güvenlik ikilemi kavramı, saldırı yeteneklerindeki bir birikimin, savunma yeteneklerindeki bir birikimden daha uygun maliyetli olduğu durumlarda en yoğun olduğu şekilde ortaya çıkmaktadır. Saldırı ve savunma yetenekleri birbirinden ayırt edilemez olduğunda güvenlik ikilemi de daha ciddi bir boyuttadır (Jervis, 1978, 187-194). Eğer böyle bir durum olursa, devletler iyi niyetlerinin sinyalini veremezler ve kabiliyetteki herhangi bir artışın potansiyel bir tehdit olarak görülmemesi için hiçbir neden yoktur (Jervis, 1978: 199-206). Ancak siber ortamda yetenekleri ayırt etmek çok zordur. Birincisi, tanım gereği bilinmediği için hükümetlerin saldırıların gerçek etkisini hemen anlamaları imkansızdır. Dahası, aktörlerin siber askeri kuruluşlar kurmaları sonucunda devletler hem savunma hem de saldırı rollerine sahip olma eğilimindedir ve bütçelerini veya personelini bu çerçevede artırdıkları söylenirse, saldırı veya savunma amaçlı yatırım yaptıkları sistem gereğince belirlenemez. Bu durum ise siber uzayda güvenlik arayan devletler arasındaki belirsizliği ve rekabeti besler ve güvenlik ikileminin boyutlarını siber uzay düzeyine yani belirsizlik tehdidi algısına çıkartır.

Bazı realistlere göre silahlanma yarışları savaş olasılığını arttırmaktadır (Evera, 1998: 13), ancak diğerleri için askeri yapılanmalar revizyonist bir gücü caydırmak için gerekli bir araçtır (Glaser, 2004: 63-64). Özellikle siber savaş öncesi nükleer savaş algısı bu durum için bir örnek teşkil etmektedir. Temel olarak Soğuk Savaş sırasında her iki kutupta bulunan nükleer silahlar bir nebzede olsa caydırıcılık sağlamışlardır. Bu nedenle kritik bir soru, güvenlik rekabetinin gerçek çatışmaya

yükselip yükselmeyeceğidir. Geçmiş dönem teorilerine göre silahlanma yarışları ve anlaşmazlıklar devletler arasında savaş ihtimalinin olduğu bir durumu göstermekteydi (Gibler ve diğerleri, 2005: 134). Buradaki endişe, siber silah yarışlarının benzer bir sonuca yol açıp açmayacağıdır. Diğer yandan ise "Siber uzaydaki çatışma, neyin bir savaş eylemi oluşturduğuna ilişkin belirsizlikler ve saldırı yetenekleri arayan devlet ve devlet dışı aktörlerin sayısının artması nedeniyle benzersiz bir şekilde tırmanmaya yatkındır" (Lord ve Sharp, 2011: 29).

Bununla birlikte, yaşanan siber saldırılarının sonucunda ortaya çıkan etmenler sonucunda, siber saldırıların giderek daha sık uygulanmasına rağmen, bu artışın daha yıkıcı siber savaş biçimlerinden ziyade düşük seviyeli kesinti ve casusluk taktikleriyle ilişkili olduğunu göstermektedir (Jensen, Maness ve Valeriano, 2016: 17). Ancak burada unutulmaması gereken olgu kilit bilgi sistemlerine yönelik yapılan saldırılar sonucunda askeri alanlarda olmasa bile sosyal, ekonomik ve çevresel alanları tehdit etmektedir. Realizmin öngörmüş olduğu kavramsal sistematiğe uymak yerine, devletler topyekün savaşlardan kaçınmakta ve bunun yerine siber ortamda diğer aktörlerin sistemlerini kısıtlayarak onları zayıflatmak daha ekonomik gözükmektedir. Gelecek dönemlerde siber saldırılara yönelik artışın bir trend haline gelip gelmeyeceğini söylemek için henüz çok erken olabilir, ancak otuz yıllık dijital çatışmalar sonucunda eyaletlerin siber uzayda doğrudan yıkım ve şiddetten şu etapta kaçınmaktadırlar.

Realizm aynı zamanda, bir düşmana zarar verme veya zarar verme tehdidinde bulunarak kişinin iradesine zorlama kapasitesine atıfta bulunarak, siber yeteneklerin devletlere zorlayıcı güç verip vermediği sorusunu da gündeme getirmektedir (Schelling 1966: 1-34). Bununla birlikte, teknoloji, geleneksel askeri operasyonların yıkıcılığından yoksun olduğundan ve hedef devlet tarafından ciddiye alınma olasılığı daha düşük olduğundan, siber zorlamanın etkinliği konusunda ciddi şüpheler bulunmaktadır. İnternet tabanlı savaş yazısının sınırlamalarına dikkat etmek gerekmektedir: "Bir rakibin bir ülkenin altyapısını, iletişimini veya askeri yeteneklerini boşa çıkarması bir sonuç getirir ancak, verilen zararın ulusal yetenekler veya kararlılık dengesinde kalıcı bir değişime dönüşmesini sağlamak daha derinden bir etkiye ve sonuca neden olmaktadır" (Gartzke, 2013: 2). Buradan da anlaşılacağı üzere siber silahların ancak geleneksel askeri operasyonlarla eşzamanlı olarak kullanıldığında etkili olmaktadır. Rakip devletler arasındaki siber olaylarla ilgili veriler sonucunda, hedefin davranışını değiştirmeyi amaçlayan zorlayıcı siber eylemlerin, daha küçük ölçekli kesinti veya casusluk ile karşılaştırıldığında genellikle etkisiz olduğu gerçek bir durumdur. Bu bulgular, geleneksel iktidar ve savaş nosyonlarının siber alana illa ki iyi tercüme edilmediğini ve siber gücün şu an için uluslararası siyaseti dönüştürücü olmadığını göstermektedir.

Ayrıca realist teorinin temel unsurlarından birisi olan insan doğası gereği kötüdür kavramı siber ortam içinde geçerlidir. Kötü amaçla hareket eden teröristlerin siber saldırı yapma durumu realizmin bu durumuna örnek olmaktadır. Ancak devletler birey haklarını kontrol altına aldıkları takdirde bu kötülüğü ve kaos durumunun önüne geçebilmektedirler. Bunun yanında devletler kendi siber gücünü oluşturmak adına bireyleri kontrol altına alır ve onları başka devletlere yönelik siber saldırılar için kullanabilmektedirler.

Realist perspektif ancak kimi zamanlarda siber güvenliği açıklamakta yetersiz kaldığı durumlarda ortaya çıkmaktadır. Bu durumlar ise devlet kavramının temel bir aktör olarak görülme olgusu realizm çerçevesinde geçerli sayılmaktadır. Fakat siber ortamda bundan söz etmek imkânsızdır. Sonuçta siber ortamda bireyler bir aktör olarak gerek bireylere gerekse devletlere siber saldırılarda bulunabilmektedirler. Realist bakış açısına göre temel güvenlik devlet güvenliğinin korunmasına yöneliktir. Öncelikle asıl amaç devletin varlığını sürdürmesi kendi güvenliğini sağlamasıdır. Fakat bu durum siber ortam için geçerli değildir sonuçta devlet dışında bu ortamda, bireyler, örgütler, kurumlar bulunmaktadır yani devletler güvenlik algısını modernleştirerek sanal ortamda işlev gören sistemleri/aktörleri de korumak durumundadır. Realizm içerisinde bireyler aktör olarak görülmez fakat, siber alanda belirtilerek paydaş olarak görülmektedirler. Sonuçta siber saldırıyı yapanlar yalnızca devletlerden oluşmamaktadır bireysel çıkarlar uğruna bile saldırı düzenlenebilmektedir.

Diğer bir realist kuram ise devletlerin olmadığı ortamda anarşik bir sistem olgusudur. Bu durum siber ortam için geçerlidir fakat devletler tekil aktörler olarak bu anarşik ortamı karşılayacak güçte değillerdir. Burada devletler diğer örgütler ve bireylerle işbirliği yapmak durumundadır. Yani düzenin kurulabilmesi adına devletler diğer aktörleri realist görüşün aksine birer paydaş olarak görmek durumundadır.

Realist perspektife göre güç kavramı amaca ulaşmak için asıl etken olurken zaman içerisinde özellikle neo-realistlerle güç kavramı amaca ulaşmak için kullanılan bir araç olarak görülmektedir. Bu durum siber alan içinde geçerli, siber tehditlere karşı güçlü bir alt yapının olması gerekir. Saldırılara karşı güvenlik ve önlem alınması gerekmektedir. Bu amaçla ise birçok ülke siber güvenliğe yönelik eylem planları belirlemekte, ulus üstü organizmalarla birlikte işbirliğine gidilmektedir. Ayrıca siber alan ve realist alan evrensel olarak görülmektedir. Bu çerçevede özellikle küreselleşme ve teknolojik gelişmeler sayesinde her iki olgu tüm dünyada bariz bir şekilde hissedilebilmektedir.

5. SONUÇ

Siber güvenlik alanı yeni olmasa da perspektifin entelektüel bilgi birikimi gelişmektedir. Gelecekte yapılacak işlerin çoğu, siber sorular üzerinden kurumsal düzenlemelerin doğasına meydan okuyacak kritik epistemolojik yaklaşımların yanı sıra yöntemlerin, deneyselliğin ve kanıtların daha fazla dikkate alınmasını gerektirmektedir. Siber eylemlerin etik sınırlamaları hem sivillere hem de diğer aktörlere verilebilecek zararlar düşünüldüğünde, siber eylemlerin stratejik sınırlamalarını ve olumlu olasılıklarını göstermek için daha fazla özen gösterilmesi gerektiği durumu açıkça görülmektedir.

Siber güvenlik kavramı Uluslararası İlişkiler teorisi perspektiflerinden öğrenebileceği çok şey vardır. Ortaya çıkan politika alanlarının gerici perspektiflerle doldurulması gerekmez. Teorik bir çerçevede hiç kimse, siber güvenlik sorularının büyük çoğunluğunun üstesinden gelmeye ve cevap vermeye çalışamaz. Bunun yerine soruların, beceri ve yetenekleri birleştiren ekipler tarafından ayrıştırılması ve araştırılması gerektiğini düşünürler. Bu kritik alanda ilerleme sağlamak için işbirliği ve dikkatli bir ilişki kurmaya ihtiyaç vardır. Bu sebeple devletler aynı realist çerçevede olduğu gibi tekil bir şekilde görülemezler.

Siber alanın araştırma, eğitim, iş ve sosyal etkileşimler için önemi nedeniyle, alandaki eylemler büyük risk ama aynı zamanda büyük olasılıklar da getirmektedir. Bağlı olunan sistem temel olarak savunmasızdır, ancak güvenlik açığı her durumda zarara yol açmayacaktır. Güvenlik açığı, dijital bağlantının önemi göz önünde bulundurulduğunda, karşılıklı olarak garanti altına alınmış istikrara giden yol olarak görülebilmektedir. İstikrar ve kaos arasındaki çizgi her zaman siber uzayda sömürülme tehlikesi altında olduğundan, gelecek dönemlerde siber ortam, çatışma ve kaos içerisinde olmayabilir, tam aksine, örneklere rağmen işbirliğinin hakim olabilme olgusu bir ölçüde güven vermektedir.

Çoğunlukla ulusal güvenlik ve iktidar meseleleriyle ilgili bir teori olarak, realizm, siber çatışmayı anlamak için içgüdüsel uluslararası ilişkiler perspektifi gibi görünmektedir. Realizmin siber alandaki güvenlikle ilgili önemli sorunları tanımlamak için uygun bir çerçeve olarak kaldığını ve bazen uluslararası ilişkilerin bazı kalıcı özellikleri hakkında yararlı bilgiler sağlayabileceğini görülmektedir. Bununla birlikte, çatışmayla ilgili realist teoriler, siber çatışmanın benzersiz dinamiklerini açıklamada çoğunlukla yetersiz kalmaktadır.

Siber alan, birçok yönden, anarşik yapısı ve kurumsal yönetim eksikliğiyle, devletlerin birbirinden korktuğu ve buna yanıt olarak yeteneklerini geliştirdiği gerçekçi bir dünyaya benzemektedir. Yine de siber silah yarışlarının, siber çatışmaya dönüşüp tırmanmayacağı belirsiz bir durumdur. Realizm, ayrıca siber güç kavramını açıklarken, ona kimin sahip olduğu ve bunun uluslararası istikrarla nasıl bir ilişkisi olduğu hakkında ilginç sorular ortaya çıkartmayı amaçlamaktadır. Sonuçta güvenlik ikileminin ortaya koyduğu bir tehdit algısını siber ortamda belirlemek çok güçtür. Siber gücün geleneksel güç dinamiklerini dönüştürüp dönüştüremeyeceği konusunda örnekler ve yapılan

saldırılar durumun böyle olmayacağını göstermektedir. Şimdiye kadar gördüğümüz eğilim, siber etkileşimlerin daha az yıkıcı biçimleri şeklinde ortaya çıkmış ve gelişmiş siber savaşın şu çerçevede yaşanmadığı gözlemlenilmiştir.

Saldırı ve savunma dengesi, siber alanı açıklamak için kullanılan realist bir teorinin bir örneğidir, ancak siber alan hakkındaki varsayımlarında ve siber çatışmayla ilgili tahminlerinde ampirik olarak yanlış görülmektedir. Gerçek dünyadaki siber çatışma vakaları, suçun genellikle varsayıldığı kadar kolay olmadığını ve çok fazla siber çatışma görmemiş olmamız sebebiyle teorinin yanlış yerleştirildiğini göstermektedir. Caydırıcılık fikrini nükleer silahlar gibi ithal etmek ayrıca yanlış yargılanıyor ve siber silahların gerçekliği bağlamında çok az anlam ifade etmektedir.

Bir saldırı silahı olarak siber teknolojinin kullanımıyla ilgili belirsizlik nedeniyle, devletler siber alanda dikkatli hareket etmeli ve dayanıklı savunmalar oluşturmaya odaklanmalıdır. Gerçekten de düpedüz siber savaştan kaçınarak, birçok devlet şimdiye kadar siber uzaydaki davranışlarında önlem almaya çalışmıştır ve bu durum realist teorisyenlerin ilgisini çekmiş ve teorik çalışma için bir alan yaratmıştır.

Burada gündeme getirilen sorunlar göz önüne alındığında, savaşın kinetik biçimlerini açıklamak için geliştirilen realist teorilere otomatik olarak geri dönmek yerine, deneysel gözlemlere veya siber alanın tümden gelen mantığına dayalı yeni teorilerin geliştirilmesini teşvik edilmesi gerekmektedir. Daha fazla deneysel araştırmayla, siber silah yarışlarının devletler arası ilişkiler üzerindeki etkisi, siber yeteneklerin devlet ve devlet dışı aktörler arasında dağılımı ve yoğun güvenlik rekabetine rağmen kısıtlama nedenleri ve saldırgan bir avantajın algılanması gibi temel konular hakkında daha kesin anlayışlar elde edebiliriz.

KAYNAKÇA

Ateş Davut. (2009). "Uluslararası İlişkiler Disiplininin Oluşumu: İdealizm / Realizm Tartışması Ve Disiplinin Özerkliği", Doğuş Üniversitesi Dergisi, Cilt: 10, Sayı: 1

Axelrod, Robert and Rumen Iliev. (2013). "Timing of Cyber Conflict." *Proceedings of the National Academy of Sciences,* 111 (4): 1298-1303.

Bıçakçı Salih. (2012). "Yeni Savaş ve Siber Güvenlik Arasında NATO'nun Yeniden Doğuşu", Uluslararası İlişkiler, Cilt 9, Sayı 34.

Bıçakçı Salih. (2013). "21. Yüzyılda Siber Güvenlik", Mustafa Aydın (ed.), İstanbul: Bilgi Üniversitesi Yayınları.

Bilgiç Ali. (2011). "Güvenlik İkilemini Yeniden Düşünmek Güvenlik Çalışmalarında Yeni Bir Perspektif", Uluslararası İlişkiler Dergisi, Cilt 8, Sayı 29.

Eriksson, Johan and Giampiero Giacomello. (2006). "The Information Revolution, Security, and International Relations: (IR) Relevant Theory?". International Political Science Review 27(3): 221–244.

Gartzke, Erik. (2013). "The Myth of Cyberwar: Bringing War on the Internet Back Down to Earth". International Security 38(2): 41–73.

Guitton, Clement. (2013). "Cyber insecurity as a national threat: overreaction from Germany, France, and the UK?" *European Security,* 22 (1): 21-35.

Hill Kevin A. and Hughes John E. (1998). Cyberpolitics: Citizen Activizm in the Age of the Internet, Lanham & Maryland: Rowman & Littlefield Press.

Hoffman Adam and Schweıtzer Yoram. (2015). "Cyber Jihad in the Service of the Islamic State (ISIS)", Strategic Assessment, Cilt 18, No 1.

Horowıtz Shale. (2004). "Restarting Globalization after World War II; Structure, Coalitions, and the Cold War", Comparative Political Studies, Vol 37, No 2.

Hughes Rex B. (2009). "NATO and Cyber Defence: Mission Accomplished?", Atlantisch Perspectief, Cilt 1, No 4.

Jervis, Robert. (1976). Perception and Misperception in International Politics. Princeton: Princeton University Press.

Jordan Tim. (1999). Cyber Power: An Introduction to the Politics of Cyberspace, London: Routledge.

Kara Mahruze. (2013). Siber Saldırılar-Siber Savaşlar ve Etkileri, Yayınlanmamış Yüksek Lisans Tezi, İstanbul: Bilgi Üniversitesi.

Kello, Lucas. (2013). "The Meaning of the Cyber Revolution: Perils to Theory and Statecraft." *International Security* 38 (2): 7-40.

Lango, Hans-Inge. (2016). "Competing Academic Approaches to Cyber Security". Conflict in Cyber Space: Theoretical, strategic and legal perspectives, edited by Karsten Friis and Jens Ringsmose, 7–26. London: Routledge.

Lord, Kristin M. and Travis Sharp. (2011). "America's Cyber Future: Security and Prosperity in the Information Age". Center for a New American Security, 1: 1–62

Mearsheimer, John J. (2001). The Tragedy of Great Power Politics. New York: W. W. Norton & Company

Morgenthau, Hans J. (1948). Politics among Nations: The Struggle for Power and Peace. New York: Alfred A. Knopf.

Nojeim Gregory T. (2010). "Cybersecurity and Freedom on the Internet", Journal of National Security Law & Poiıcy, Vol 4, No 119.

Nye, Joseph S. (1990). "Soft Power". Foreign Policy 80: 153–171.

Nye, Joseph. (2011). The Future of Power. New York: Public Affairs.

Reardon, Robert, and Nazli Choucri. (2012). "The Role of Cyberspace in International Relations: A View of the Literature". Paper presented at the 2012 ISA Annual Convention, San Diego, CA. 1 April.

Ripsman, Norrin M., Jeffrey W. Taliaferro, and Steven E. Lobell. (2016). Neoclassical Realist Theory of International Politics. New York: Oxford University Press.

Rosecrance, Richard, and Arthur Stein. (1993). The Domestic Bases of Grand Strategy. Ithaca: Cornell University Press.

Russell, Alison L. (2014). *Cyber Blockades*. (Washington: Georgetown University Press).

Schelling, Thomas C. (1966). Arms and Influence. New Haven, CT: Yale University Press.

Schmidt, Brian C. (2002). "On the History and Historiography of International Relations". In Handbook of International Relations, edited by Walter Carlsnaes, Thomas Risse, and Beth A. Simmons, 3–22. London: Sage Publications

Senese, Paul D. and John A. Vasquez. (2008). The Steps to War: An Empirical Study. Princeton: Princeton University Press.

Steger Manfred B. (2009). Globalization: A Very Short Introduction, Hampshire: Oxford Univeristy Press.

Ünver Mustafa ve Canbay Cafer. (2010). "Ulusal ve Uluslararası Boyutlarıyla Siber Güvenlik", Elektrik Mühendisliği Dergisi, Sayı 438.

Valeriano, Brandon and Ryan C. Maness. (2015). Cyber War versus Cyber Realities: Cyber Conflict in the International System. New York: Oxford University Press.

Vasquez, John A. (1995). Classics of International Relations. London: Pearson.

Waltz, Kenneth N. (1979). Theory of International Politics. London: AddisonWesley.