SİBER CAYDIRICLIK

Ozan Sabri TUNCER*

Orcid ID: https://orcid.org/000-0002-1379-6648

Özet

Siberin, hava, kara, deniz ve uzaydan sonraki bir diğer alan olarak ortaya çıkmasındaki temel etmenlerin başında internetin kullanım alanlarının artması gelmektedir. Küreselleşmenin beraberinde getirdiği bilişim ve internet teknolojisi ile bu alanda yaşanan sorunlar insanlar ve devletler için çok ciddi sonuçlar yaratmıştır. Siber alanın uluslararası sitemdeki çeşitli aktörler için bir güvenlik sorunu yarattığı ortadadır. Bu çalışmada siber caydırıcılığın ve nükleer caydırıcılığın bağlantısı anlatılmış ve siber caydırıcılık teorisinin olumsuz yönlerine değinilerek devletler, insanlar ve diğer aktörler için önemi vurgulanmıştır. Siber alanda caydırıcılık var mıdır? Bu ana sorunsal ele alınarak literatür taraması yapılmıştır. Siber alan, siber caydırıcılık, nükleer caydırıcılık, kritik öneme sahip altyapılar, siber saldırı ve caydırıcılık kavramlarıyla ilgili bilgiler verilmiştir. Sonuçta siber alanda yaşanan saldırıları belli ölçekte engellediği açıklanmış fakat yine de bazı sorunlardan dolayı istenen caydırıcılığın tam olarak sağlanamadığı vurgulanmıştır.

Anahtar Kelimeler: Siber Caydırıcılık, Siber Alan, Nükleer Caydırıcılık, Kritik Öneme Sahip Altyapılar, Siber Saldırı, Güvenlik

CYBER DETERRENCE

Abstract

One of the main factors in the emergence of cyber as another area after air, land, sea and space is the increase in the usage areas of the internet. With the informatics and internet technology brought about by globalization, problems in this environment have created very serious consequences for people and states. It is obvious that cyber creates a security issue for various actors in my upper international system. This resource is about cyber deterrence and nuclear deterrence, and its importance for states, people and other actors has been emphasized by addressing the negative aspects of cyber deterrence theory. Is there any deterrence in the cyberspace? This main problematic literature review has been conducted. Information was given on the concepts of cyber space, cyber deterrence, nuclear deterrence, critical

* SÜ Uluslararası İlişkiler Bölümü Doktora Öğrencisi E mail: tuncerozansabri@gmail.com

infrastructures, cyber attack and deterrence. As a result, the attack was prevented, but it was emphasized that other problems other than some problems could not be fully achieved.
Keywords: Cyber Deterrence, Cyber Space, Nuclear Deterrence, Critical Infrastructures, Cyber Attack, Security

Giriş

Günümüzde devletler kara, deniz, hava ve uzaydan sonra beşinci boyut olarak ele aldıkları ve her geçen gün önemi artan siber uzayı yeni bir savunma alanı olarak görmektedirler (Polat, 2020: 136). Özellikle Soğuk Savaş döneminde devletler nükleer ve konvansiyonel caydırıcılığı aktif bir şekilde kullanmış sonuç olarak ise dünyada bir nükleer savaş yaşanmamıştır. Bu çalışmamızdaki ana sorunsal şudur: siber alanda caydırıcılık var mıdır? Bununla birlikte siber caydırıcılığın ne gibi önemi bulunmaktadır? Siber caydırıcılığı sağlamanın ne gibi zorluğu bulunmaktadır? Ve son olarak da siber caydırıcılık gelecekte daha önemli bir etmen haline mi gelecek yoksa etkisini azaltacak mı? Bu gibi yardımcı sorularla literatür taraması yapılarak ele alınan ana soru çerçevesinde cevaplar aranacak ve bu cevaplarla birlikte siber caydırıcılık teorisine katkı sağlanmaya çalışılacaktır. Bu çalışmamızda ana amacımız siber alanın hayatımızdaki önemine dikkat çekmek ve gelecekte ne gibi faydasının ya da zararının olabileceğini açıklamaya çalışmaktadır.

Çalışmamızın birinci bölümünde ana sorunsal çerçevesinde nükleer caydırıcılık teorisi analiz edilmiştir. Günümüze kadar yaşanmış olan siber savaşlar araştırılarak ne gibi önlemler alındığı ve bu savaşlardan nasıl bir sonuç çıkarıldığı üzerinde durulmuştur.
Çalışmamızın ikinci bölümünde ise siber caydırıcılığın ne ifade ettiği ve neleri kapsadığı araştırılmıştır. Buradan hareketle çeşitli örnekler verilerek siber caydırıcılık teorisi ele alınmıştır.

Caydırıcılık, günlük kullanımıyla herhangi birini bir şey yapmaktan alıkoymak, onu engellemek şeklinde tasvir edilmektedir. Siber alanda da caydırıcılık buna paralel mahiyette bilişim teknolojileri alanında çeşitli ağların alt kapılarına erişimin sağlanmasıyla saldırıda bulunmak, manipüle etmek, suiistimal etmek, yetkisiz şekilde kazanmak anlamlarını taşımaktadır (Burton, 2018: 5).

Amerika 2000'li yılların başına kadar dünyanın jandarması olarak kabul edilmektedir. Çin Asya kıtasından ikinci bir rakip olarak çıkıp süper güç olma yolunda emin adımlarla ilerlemiştir. Her geçen yıl cari büyüklüğünü arttırmasıyla da dikkatleri üzerine çekmeyi başarmıştır. Hatta birçok teorisyen güç kayması gibi yaklaşımlarla bu olguyu açıklamaya çalışmıştır. Çin siber alanı ve gelişmiş teknolojisini kullanarak 5G'yi çıkarmıştır ve böylelikle Amerikan Rüyasını sarsmayı başarmıştır. Bu imaj zedelenmesinin siber alanla birlikte siber caydırıcılıkta da gelecekte kendini göstermesi tahmin edilmektedir. Bu çalışmamızda literatür taraması yapılırken güç kayması ve siber alana ait güncel bilgiler de incelenerek araştırmaya dahil edilmiştir.

Sun Tzu'nun da dediği gibi "Düşmanı ve kendinizi iyi biliyorsanız yüzlerce savaşa girebilir ve sonucundan da emin olabilirsiniz." anlayışıyla siber alan iyice araştırılarak analize dahil edilmiş ve nükleer caydırıcılık teorisinden faydalanarak siber caydırıcılık teorisi anlatılmaya çalışılmıştır (Şenol, 2016: 15).

Klasik (Nükleer) Caydırıcılık Teorisi

Literatürde çeşitli şekillerde klasik caydırıcılığın tanımları mevcuttur. Caydırıcılık kavramı TDK'ye göre: caydırıcı olmak, bir saldırganlığı önlemek ve engellemek için önlem alma işi olarak tanımlanmaktadır. Caydırıcılık; hukuksal alanda "ceza veya hapis korkusuyla suç işlemekten alıkoyma", uluslararası ilişkilere göre "karşıdaki devleti emellerinden vazgeçirme davranışı veya belirli davranışlara yönlendirme", askeri alanda ise "düşmanı çok yüksek bedel ödeyeceğine inandırarak bir hareketten vazgeçirmek için askeri güç, yaptırım ve tehditlerin kullanımı" olarak tanımlanmaktadır (Şenol, 2017: 4). Tanımlardan anlaşıldığı üzere caydırıcılığı olması istenmeyen bir oluşuma kalkışmayı engellemek şeklinde özetlemek mümkündür.

Caydırıcılığın temel hedefi saldırganlık içeren faaliyetleri engellemektir. Caydırıcılık, antik çağlardan beri Batı siyasi güvenlik doktrininin bir parçası olmuştur (Jensen, 2012: 778-779).
Bu tanımlardan farklı olarak, caydırıcılığı genel olarak iki kısma ayırarak tanımlamak mümkündür. Buradan hareketle ilk olarak caydırıcılık deyince aklımıza askeri, ekonomik, politik bir alan gelmektedir. İkinci olarak ise 1960'lardan itibaren teknolojinin özellikle uzay araçlarının, iletişim-bilgisayar sistemlerinin kullanılmasıyla evren küresel bir köy halini almıştır. Bu gibi gelişmeleri tasvir etmede kullanılan iletişim çağı da siber alanın kapsamında

yer almaktadır. Caydırıcılık ile ilgili çalışmalar referans alınarak caydırıcılık nedir? Nasıl anlaşılmalıdır? Nerelerde caydırıcılık kullanılmaktadır? Caydırıcılığın ne gibi faydaları/ maliyetleri vardır? Bu soruların cevaplarını ve özelde ise klasik caydırıcılığı daha iyi anlayabilmek adına "Savaş Nedir?" sorusuna yönelmek bizim için daha faydalı olacaktır.

Sun Tzu' ya göre savaş: "en iyisi savaşmadan düşmana baş eğdirmektir." (Şenol, 2017: 4). Düşüncesinden yola çıkılarak aslında savaşın tasvip edilmediği anlaşılmaktadır. Harp zaruri ve hayati olmalı. Hakiki kanaatim şudur: … Lakin millet hayatı tehlikeye maruz kalmayınca harp bir cinayettir (Milliyet gazetesi 1923). Yine Ulu önder Atatürk, "Dünyada milletler apartmanın sakinleri gibi kabul edilir. Eğer bir apartman, sakinlerinden bazıları tarafından ateşe verilirse, diğerlerinin yangının etkisinden kurtulmasına imkân yoktur." demiştir (TBMM Genel Kurul Tutanağı, 2016: 25). Bu sözden de anlaşıldığı üzere hangi çapta ve ölçekte olursa olsun kısacası savaş silsile yoluyla savaşan-savaşmayan herkesi bir şekilde etkileyecektir.

Walzer ise savaşın generallerin insafına bırakılmayacak kadar değerli olduğunu dile getirmiştir (Walzer, 2004: 14-15). Buradan hareketle aslında savaşın iyi bir şey olmadığı ve zaruri olmadığı hallerde bu yola başvurulmaması gerektiği anlaşılmaktadır. Hatta bu işin üstatlarına bile bırakılmaması gerektiği görülmektedir.

Savaş aslında insanlık tarihi kadar eski bir varlıktır. Savaş olgusu yüzyıllar içerisinde değişerek ve çeşitli gelişmelerle varlığını devam ettirerek günümüze kadar varlığını korumuştur. Kas gücüne dayan çeşitli silahlardan teknolojik gelişmelerle birlikte tek tuşla kullanılan çeşitli savaş araçlarına dönüşmüştür (Sağıroğlu, Alkan, 2018: 206-207).

Bu konuda Joseph Nye düşüncelerini şu cümlelerle dile getirmiştir:

> *Savaş ve askerî güç kullanımı belki azaldı ama yok olmadı, sadece şekil değiştirmekte. Olan, savaş meydanı ve cephe kavramlarının tarif edilebilir bölgeler olmaktan çıkması, sivil- asker ayırımının giderek birbirine karışmasıdır. Orta çağlarda savaşlar ancak birkaç bin kişiyle yapılıyordu. 20.yy'da gerçekleşen iki dünya savaşında, 7 ulus, 100 milyondan fazla askerîni harbe soktu. Topyekûn savaş niteliğine bürünen çatışmalarda 45 milyon insan öldü, bir kıtanın büyük bir bölümü harabeye döndü. 6 Ağustos 1945'de atılan atom bombasıyla her şey sonsuza dek değişmiş oldu. Topyekûn savaş döneminin sonuna gelinmişti. Ne var ki, silahlı çatışmaların sonu gelmedi. Sadece devletlerin birbirleriyle doğrudan giriştiği çatışma sayısı giderek azaldı*. (Nye, 2015: 17).

Teknolojinin gelişmesi hayatımızın her alanında getirdiği yeniliklerle birlikte savaş alanında da birtakım yenilikler getirmiştir. Bu yeniliklerle kara ve deniz savaşları, nükleer savaş, hibrit savaş ve siber savaş gibi kavramlar ortaya çıkmıştır.

Genellikle klasik caydırıcılık nükleer caydırıcılık kavramı ile kıyaslanarak ve birtakım analizler yapılarak açıklanmaktadır. Çünkü caydırıcılık kavramında fayda- maliyet analizi yapılması gerektiği vurgulanmaktadır. Buradan hareketle yaşanmış birkaç savaş üzerinden özellikle de İkinci Dünya savaşı sırasında ve sonrasında yaşanan nükleer silahların kullanılmasından hareket edilerek analiz yapılacaktır.

Caydırıcılık, İkinci Dünya Savaşı sonrası dönemde özellikle nükleer santrallerde önemli bir rol oynamıştır (Jensen, 2012: 778). Caydırıcılık örneği ceza yoluyla Soğuk Savaşın karşılıklı teminatlı imha doktrinidir. Burada nükleer silah kullanma tehdidi, karşı tarafın benzer bir nükleer silah kullanmasının engellenmesi anlamına gelmektedir (Iasıello, 2018: 36).

Politikacılar ve bilim insanları uluslararası politikanın nükleer gücün gölgesi altında şekillendiğini anlamışlar, nükleer gelişmelerin ortaya çıkışından itibaren atom silahı sorununu dizginleme konusundaki teorik çalışmalara ağırlık vermişlerdir. Bu çerçevede, nükleer felaket tablosu çizenlerin aksine iyimser teorisyenler nükleer silahların caydırıcılığından hareketle devletlerin güvenlik politikalarının birbirini dengeleyeceğini iddia etmişlerdir (Gartzke ve Jo, 2009: 210-211).

Buradan hareketle özellikle soğuk savaş döneminde ön planda kullanılan ve nükleer caydırıcılığın esasını teşkil eden cezalandırma yoluyla caydırıcılığın başarıyla sağlanması için üç temel koşul bulunmaktadır. Bunlar caydırıcının yetenekleri, tehdidin inandırıcılığı ve tehdidin saldırgana yansıtılmasıdır. Klasik anlayışta olumlu yönde sonuçlar veren bu şartların siber caydırıcılığın sağlanmasında da etkili olacağı düşünülmektedir (Şenol, 2017: 4-5).

Bir başka teorisyen olan Schelling ise, Amerika ve Rusya'nın çatışan ve ortak çıkarları olduğunu savunmuş, "nükleer caydırıcılık'', "kriz yönetimi'', "sınırlı savaş'', "silahların kontrolü'', "baskı ve zorlayıcı ikna'' gibi kaotik durumları müzakere çerçevesinde değerlendirerek oyun teorisini kullanmıştır (Gündoğdu, 2016: 4). Caydırıcılığın devletlerarasında psikolojik bir oyun olduğu söylenebilmektedir. En nihayetinde caydırıcılık bir stratejidir. Caydırıcılık stratejisine göre ise her yol mubahtır. Bunun en güzel örneği ABD

‘nin 1945’te Japonya’ya attığı iki adet nükleer bombadan anlaşılmaktadır. Caydırıcılık kuramını daha iyi analiz edebilmemiz için yukarıda bahsettiğimiz caydırıcılığın literatürde yapılmış olan tanımlarını bilmemiz gerekmektedir. Caydırıcılığın özelliklerini kısaca üç başlık şeklinde açıklayabiliriz.

Caydırıcılığın Temel Nitelikleri : Tehditlerin Güvenilirliği

Bu akımı savunan teorisyenlere göre caydırıcılık potansiyel saldırgan girişimlerine karşı inandırıcı olmasına bağlıdır. Tehditlerin inandırıcılığı bağlamında, “askeri kapasite’’, “sinyalizasyon ve pazarlık gücü’’, “itibar’’ ve “tehlikedeki çıkarlar’’ olmak üzere dört anahtar faktörden söz edilebilir (Huth, 1999: 30-48).

Klasik caydırıcılık anlayışına göre devletler düşman olarak algıladıklarına karşı ellerinde güçlü bir silahlı ordu bulundurmalı ve bu maliyetleri sübvanse edebilecek ekonomik güce sahip olmalıdır. Bu tehditlerin iletilebilmesi için ise diplomatik açıklamalar ve savaş dışındaki her türlü girişim-müzakere yoluyla rakiplere risk alma konusunda kararlı olunduğunu ileten mesajlardan oluşan birtakım “maliyetli sinyallere’’ ihtiyaç duyulduğunu belirtmektedir (Lieberman, 2013: 236).

Caydırma teorisyenleri spekülatif hareket eden ve bundan dolayı inandırıcılığı düşük olan “sinyaller’’ ile manipüle etmenin oldukça maliyetli olduğunu ifade etmiş ve bu sebeple özünde inandırıcılık taşıyan “sinyaller’’ arasındaki ayrıma odaklanmıştır (Kydd, 2015: 149-150). Bu sebepten dolayı inandırıcı olabilmek için bir tehdidin realitede istekli olmayan aktörün cesaret edemeyeceği birtakım maliyet ve riskleri içermesi gerekmektedir (Huth, 1999: 30-40).

Tehditlerin güvenilirliği kavramına ilişkin olarak ise caydırıcılık literatüründe bir aktörün geçmişten gelen davranışlarının analizi, gelecekteki bu durum karşısında göstereceği tepkiye güvenilir bir belirleyicisi olup olmadığına ilişkin tartışmanın devam ettiğini belirtmek gerekmektedir (Martin, Miller, 2003: 150-152). Devletlerin tehditlerin güvenilirliği alanında birçok özelliği vardır. Buradan hareketle tehditlerin güvenilirliğini tanımlamak gerekirse özellikle devletler ve uluslararası ilişkiler disiplinine ait olarak açıklarsak bir devletin yapmış olduğu herhangi bir saldırının veya yeteneğinin diğer devlet ve devlet dışı aktörler tarafından bilinmesi şeklinde açıklanabilmektedir.

Çıkarlar söz konusu olduğunda bir anlaşmazlıkta yüksek çıkara (high politic) sahip devletlerin güç kullanımı konusunda istekli olduğu ve bu çıkarlarını korumak için yüksek maliyete katlanacakları bilinmektedir. Diğer bir taraftan önemli olmayan çıkarlar (low politic) söz konusu olduğunda ise devletlerin daha isteksiz davranacakları görülmektedir (Toft, 2001: 96). Buradan hareketle devletlerin tehditler karşısında nasıl davranacakları öncen tahmin edilememekle birlikte sadece çıkar çatışmasında fayda/maliyet analizine göre değerlendirerek hareket edecekleri anlaşılmaktadır.

Caydırıcılığın Kapasiteleri

Devletlerin caydırıcılık yeteneklerini göz önünde bulundurulduğunda devletlerin uluslararası alandaki gözlemlerini ve bu anarşik ortamdaki çıkarlarını nasıl elde edeceklerine karar vermelerinde caydırıcılık teorisinin çok önemli bir etkisi olduğu yadsınamaz bir gerçektir. Caydırıcılık, düşmanca tehditler içeren ya da potansiyel düşman konumundaki devletlere-devlet dışı aktörlere askeri, ekonomik ve anarşik olarak üstünlüğünü kullanma ve bu yeteneği açıkça göstermesi anlamına gelmektedir.

Devletler farklı seçenekler arasından bir tercih yapmak istediklerinde, yapmak istedikleri şeyi birçok açıdan irdelemektedir. Her tercihin fayda ve maliyetleri ayrı ayrı hesaplanarak başarı ihtimalleri değerlendirilmektedir (Mearsheimer, 2009: 245).

Tehdidin Karşı Tarafa İletilmesi

Caydırıcılık stratejileri bazı durumlarda çok karmaşık sonuçlar ile karşı karşıya kalmamıza sebep olmaktadır. Buradaki en temel faktör caydırıcılık stratejilerinin ortak bir anlayışının olmaması ve devletler tarafından tehdit kaynağı olan devlet ya da devlet dışı aktörlere karşı nasıl bir tutum takınacakları ile ilgili bir problemdir. Bu problemlere ek olarak devletlerin karşılaştıkları saldırılara karşı ön alıcı ya da engelleyici birtakım saldırıları karşı tarafa iletmekte yaşadığı tutumlardan kaynaklandığı görülmüştür.

Burada en güzel örnek Soğuk Savaş'ın temel çatışması olan Amerika-Rusya nükleer silah örneğidir. Amerika, Rusya'nın nükleer silah kullanması ihtimaline karşı nasıl bir tutum sergileyeceğinin net olarak bilinmemesi ve bu bilinmezliği de karşı tarafa iletememesi sonucunda dünyanın iki kutuplu sistemde az kalsın yok olmasına sebep olacaktı. Buradan

hareketle adı geçen iki devlet arasında Kırmızı Telefon (Red Line) kurulmuştur (Ataç, 2019: 6).

Doğru bir caydırıcılık anlayışının kazandırılması "karşılıklı öğrenme'' anlayışına bağlıdır (Gündoğdu, 2016: 11). Kısacası yapılan bir tehdidin karşı tarafta ne gibi sonuçlar doğuracağını doğru ve net bir şekilde anlaşılmasını sağlamak ancak karşılıklı iletişimle sağlanabilmektedir.

Oyun Teorisinin Caydırıcılık Teorisi Üzerindeki Etkisi

Caydırıcılık teorisini anlamamıza yardımcı bir diğer kaynak ise oyun teorileridir. Oyun modelleri anlayışı spesifikte nükleer caydırıcılığı anlamakta birçok teorisyen tarafından kullanılmıştır. Burada üzerinde durulan temel argüman oyun teorilerinde karşılıklı iş birliği yapılamasıdır. Aksi takdirde nükleer kriz ya da nükleer savaş kaçınılmaz olacaktır.

Caydırıcılık teorilerini anlamada ve analiz etmede yararlanılan iki yardımcı unsur bulunmaktadır. Bu unsurlar "Prisoners Dilemma" ve "Chicken Game" 'dir. Bu teori analiz edildiğinde caydırıcılığın özellikle uluslararası ilişkiler disiplininde popüler halde olduğu görülmektedir. Burada Chicken Game karşılıklı iş birliği yapmamız gerektiğini savunurken, Prisoners Dilemma ise nükleer silahlanmanın stratejik açıdan önemini vurgulamaktadır (Harvey, 1997: 60). Burada her iki oyun teorisinde de maksimum fayda sağlamak temel amaçtır. Bu sebeple devletlerarası ilişkilerde ihanet etmek yerine karşılıklı işbirliği yoluna gidilmektedir. B. Liddell Hart'ın savaşta hesaplanamayan tek ve mücadele edilemeyen iradenin insan iradesi olması anlayışından hareketle oyun teorilerinde ve uluslararası ilişkiler disiplininde iradenin ne kadar önemli olduğu bir kere daha görülmektedir. Bu insan iradesi karar alıcılar (savaş, güç kullanma, barış, ticaret) anlayışında ne kadar önemliyse caydırıcılık ekseninde de bir o kadar önemlidir (Sağıroğlu ve Alkan, 2018: 216). Burada da caydırıcılık ve oyun teorisi açısından değerlendirmede sadece insan ilişkileri ve davranışı değil aynı zamanda kültürü, yetiştiği ortam psikolojik ve sosyolojik gibi birçok faktör önem arz etmektedir.

Siber Caydırıcılık Teorisi

İnsanlığın belki de en önemli icatlarından biri olan bilgisayar, özellikle 1960'lı yıllardan itibaren insan hayatındaki yeri geliştikçe artan, derinleşen ve her geçen gün farklı gelişmelerle olumlu ya da olumsuz şekillerde karşımıza çıkmaktadır. Bilgisayarların internet aracılığıyla başka bilgisayarlarla iletişim sağlayabilmesi günümüzde çeşitli sorunları da beraberinde getirmiştir. Özellikle internet ABD ve SSCB arasında süren politik, iktisadi ve ideolojik bir çatışma olarak nitelendirilen Soğuk Savaşın bir tür çıktısıdır. O dönemin süper güçlerinin güçlü olarak nitelendirilmesinde teknolojik açıdan gelişmişlik en temel etmendir (Akyeşilmen, 2018: 25). 1957'de Sovyetler Birliği ilk yapay uydu olarak bilinen Sputnik-1'i uzaya gönderdiğinde, Amerika farklı çalışmalar başlatmıştır. ABD, SSCB'nin bu adımından sonra 1958'de Explorer-1'i uzaya göndermiştir. Bu gelişmeler iki süper güç olan devleteler arasında iletişim, ekonomi, askeri ve politik alanında tırmanarak devam etmiştir (NASA, 2017).

Siber alan olarak tabir edilen uzay/yer düşüncesi İngilizce Bilim Kurgu literatüründen alınan interneti somutlaştırarak hayatımıza kazandırılan bir kavramdır. Kısacası siber uzay kavramı hayatımıza bilim kurgu edebiyatından alınarak uyarlanmıştır (Akyeşilmen, 2018: 12). Somut bir alan olmayan siber alan teknolojinin gelişmesiyle birlikte hayatımızın her alanda önemli bir parçası olmuştur.

Soğuk Savaş sonrası süper güçler bu sefer de siber uzay dediğimiz alanda hâkimiyet kurmak için birbirleri ile kıyasıya yarışa girmiştir. Burada en büyük sorun siber alanın ne kadar geniş olduğu hâkimiyetinin ise karasal ve denizel alan savunmasından daha zor olduğudur.

Günümüzde dünya üzerinde internet kullanan insan sayısının yaklaşık olarak 4.5 milyarın üzerinde olduğu ve bu sayının dünya nüfusu sayısına oranının ise yaklaşık %59 olduğu bilinmektedir (We Are Social:c2020:15). Gelişen teknoloji ile birlikte milyarlarca insanın internet kullanımı artmış ve gelişen teknoloji sayesinde nesnelerin internetleşmesi kavramı ortaya çıkmıştır. Akıllı telefon kullanımı, bilgisayar, tablet, akıllı ev sistemleri akıllı arabalar bunun en güzel örnekleridir. Bunların yanında gelişen teknoloji ile devletlerde altyapı ve haberleşmelerinde internetten faydalanmışlardır. Askeri, elektrik, su, haberleşme, finansal hizmetler gibi çok kritik öneme sahip alanlarda da devletler internetten faydalanılmaktadır (Akyeşilmen, 2018: 11-13).

Artan internet kullanımı birçok sorunu da beraberinde getirmiştir. Bu sorunlar devlet ve birey açısından önem arz etmektedir. Literatürde siber alanın karmaşıklığı ve genişliği hakkında birçok görüş bulunmaktadır. Siber uzay alanı tüm iletişimin kaynaşması anlamına gelmektedir. Ağları, veri tabanları ve bilgi kaynaklarını içeren küresel bir sistemdir (Liaropoulos, 2013: 15). Choucri'ye göre ise siber uzay; geçiciliğe göre geleneksel zamansallığı yakın ile anlık olarak değiştirmektedir. Fiziksellik coğrafyanın sınırlarını ve yetki alanlarını aşmakta, akışkanlıkları sürekli vardiyalar halinde ve yeniden yapılandırmaktadır. Katılım (aktivizm ve politik yorum), atıf ile birlikte aktörlerin kimliklerini gizlemekte ve hesap verilebilirliği zorlu kılmaktadır (Choucri, 2012: 5).

Christopher Haley siber caydırıcılık teorisini üç temel yöntem üzerinden analiz ederek açıklamıştır. Bunlardan ilkinin maliyetleri ve sonuçları analiz ederek saldırıları gidermek olduğunu belirtmiş ve bunun için de güçlü bir savunmaya ihtiyaç olduğunu belirmiştir. İkinci olarak misilleme üzerine odaklanarak bazı başarılı saldırıların sonucunda bu fiili yapan saldırganlara karşı ağır cezalar uygulamaktır. Böylece diğer saldırıya istekli kişilere karşıda bir önleyici adım atmış olduğunu belirtmiştir. Üçüncü ve sonuncu olarak saldırının saldırı yapan tarafa dayatılmasının önemi üzerinde durmuştur (Haley, 2013).

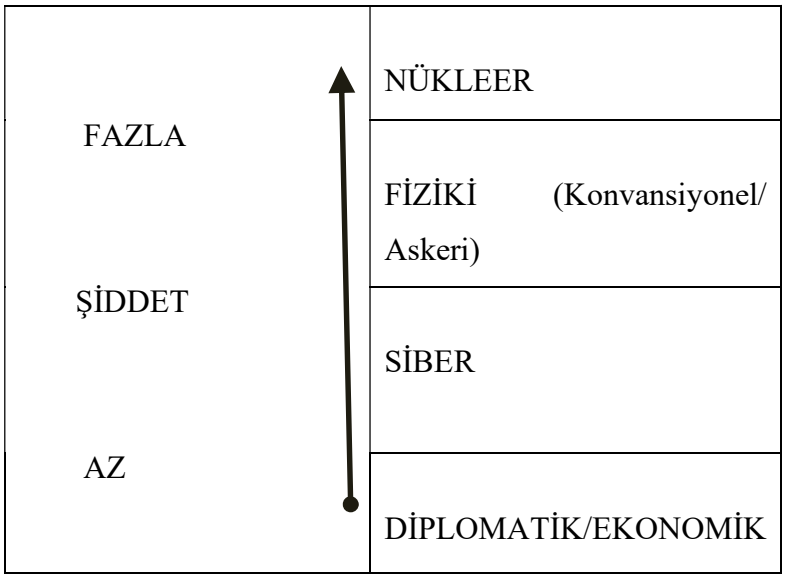
Eric T. Jensen "Siber Caydırıcılık" adlı çalışmasında Haley'nin atıf yaptığı siber saldırganlara karşı yasal cezalara önem verirken Jensen siber caydırıcılığın klasik caydırıcılıktan farklı olarak görünmezlik, misilleme, esneklik gibi farklılıklar sonucunda saldırganların cezaları uygulamaktan sakınabileceklerini savunmuştur (Jensen, 2012: 778-780).

Andrew Lıaropoulos'a göre siber uzayın kavramsal belirsizliğine önemli bir katkıda bulunan ve bu alanı karakterize eden saldırı kavramıdır. Siber saldırı ve siber savaş, siber casusluk ve siber sabotaj gibi ilgili terimler çok çeşitli eylemleri kapsayabilmektedir (Lıaropoulos, 2013: 158). Özellikle günümüzde gelişmiş internet ve teknoloji alt yapısıyla birlikte küresel salgının ortaya çıkmasıyla milyarlarca insanın uzaktan erişim ile her türlü günlük işlerini yapmasıyla ortaya çıkan çok büyük bir güvenlik açığı bulunmaktadır. Günümüzde bu kadar gelişen teknolojiye rağmen artan bu güvenlik açığı bile siber uzay dediğimiz alanın ne kadar karmaşık olduğunu ve kontrol edilmesinin ne derece güç olduğunu açıklamaktadır.

Libicki'ye göre siber caydırıcılık; "siber alanda saldıranın saldırısını boşa çıkarma ve saldırısına karşılık verme yoluyla saldırısından vazgeçirme" şeklinde tanımlanmıştır (Şenol,

2016: 5). Siber caydırıcılık stratejisi rakibi maliyetlere inandırarak hedefe saldırmasını etkilemek ve saldırı sonuçlarının potansiyel faydadan daha ağır olacağını karşı tarafa ikna etmektir (Iasıello, 2018: 36). ABD eski Genelkurmay Başkan Yardımcısı olan Orgeneral James Cartwright'a göre siber caydırıcılık; siber alanda saldıranların bize yapmak istediklerinin aynısını onlara yapma yeteneği şeklinde ifade edilmiştir (Libicki, 2009: 15).

Siber alanın bu kadar geniş ve kontrolü zor bir saha olması birçok olumlu ve olumsuz faktörü de beraberinde getirmiştir. Çünkü siber caydırıcılığın iki temel özelliği vardır. Caydırıcılık teorisinin ilk bileşeni güçlü bir savunma olmalıdır. İkinci bileşeni ise yapılan saldırılara karşı misilleme yapma gücüdür (Haley, 2013). Bunun siber caydırıcılık politikası için birkaç temel çıktısı vardır. Bu çıktılardan ilki sağlam bir savunma iken onu takip eden bir diğer çıktı ise sağlam ve donanımlı-korunaklı yazılımlardır (Haley, 2013).



ŞEKİL 1: Siber Caydırıcılığın Etkisel Olarak Nükleer Etkiye Göre Şiddeti (Libicki, 2019: 29).

Yukarıdaki şekilde de görüldüğü gibi en yüksek caydırıcılık oranı nükleer güçle caydırma iken bunu takiben fiziki (konvansiyonel-askeri) caydırma, siber caydırma en son da ise diplomatik-ekonomik caydırmayı kabul edilmektedir. Temel olarak literatürde genellikle siber caydırıcılık teorisi klasik nükleer caydırıcılık teorisiyle ilişkilendirilerek açıklanmaya çalışılmıştır.

Literatür taramasında siber caydırıcılık ile ilgili iki farklı görüşün hâkim olduğu analiz edilmiştir. Bir grup teorisyen siber caydırıcılığın birtakım zorluklar ve muğlaklıklar barındırdığı için bu teorinin pratikte işe yaramayacağı görüşünde olmuşlardır. Karşı tarafta ise bir grup teorisyen geliştirmiş olduğu birtakım bakış açıları ve benzer argümanlar ile siber caydırıcılık teorisinin pratikte işe yarayacağı görüşünü benimsemişlerdir (Sağıroğlu, Alkan, 2018: 210).

Libicki'ye göre ise nükleer caydırıcılık teorisinin birtakım argümanları olan tarafların yetenekleri, misilleme tahdidinin karşı tarafa iletilmesi ve tehdidin güvenilirliği koşullarının siber caydırıcılık teorisinde işe yaramayacağı düşünülmüştür (Libicki, 2011: 10). Burada önemli tartışmalardan biri ise nükleer gücün kullanılması tehdidi konvansiyonel caydırıcılık için karşı tarafa misilleme yoluyla caydırıcılıkta işe yararken, siber caydırıcılık teorisinde bunun işe yarayıp yaramayacağı sorunudur (Şenol, 2017: 4-5).
Siber saldırılara karşı caydırıcılığın birtakım belirsizlikleri nedeniyle nükleer caydırıcılık teorisinde kullanılan caydırıcılığın siber caydırıcılıkta başarılı olunamayacağı düşünülmüştür. ABD'nin nükleer alanda sağladığı başarıyı siber alanda başaramayacağı düşünülmüştür (Şenol, 2017: 4-5). Nitekim bu düşünce siber saldırılar sonucu ABD Savunma Bakanlığından sızan bilgiler ile desteklenmektedir (Seren, 2018: 9).

Libicki'ye göre siber caydırıcılık teorisi olumlu sonuçlar verebilir. Bunun için üç temel ve altı yardımcı soruya cevap vermek gerekmektedir.

Temel Sorular;

1. Saldırının kim tarafından gerçekleştirildiği biliniyor mu?
2. Karşı tarafın değerleri risk altında tutulabilir mi?
3. Saldırının tekrarlanması mümkün mü?

Yardımcı Sorular ise;

1. Misilleme işe yaramaz ise silahsızlandırmayı sağlayabilir mi?
2. Bu iki grup dışında başka bir grubun bu mücadeleye katılması söz konusu olur mu?
3. Saldırıya misilleme için bir ölçü var mı?
4. Misilleme kendimiz için doğru bilgi verir mi?
5. Karşılıklı çatışmadan sakınılabilir mi?
6. Saldırgan tarafa saldırmanın kayda değer olmadığı durumlarda ne yapılmalı? (Libicki, 2009: 120).

Will Goodman ise 2010 yılında yayımladığı "Siber Caydırıcılık Pratikte Teoriden Daha Zor" adlı makalesinde siber caydırıcılığın teoride kolay pratikte ise zor olduğunu belirtmiştir. 2007 ve 2008 Estonya- Gürcistan siber saldırılarından analiz yaparak teorisini temellendirmiştir. Goodman'ın siber caydırıcılık teorisi Libicki'nin siber caydırıcılık anlayışına uygundur. Goodman'ın temellendirdiği sekiz temel kavram; kar-zarar, cezalandırma, engelleme, çıkar, caydırıcılık, güven, korku ve inandırıcılıktır. Bu kavramlar siber caydırıcılık teorisinde Libicki anlayışı ile benzerlik göstermektedir (Goodman, 2010: 109).

Siber caydırıcılık ile ilgili olarak akademisyenler, uzmanlar ve askeri yetkililerin ortak kanıya vardıkları sonuç siber alanda siber güç kullanılarak siber caydırıcılıkta başarı sağlanabilir kanısıdır. Siber caydırıcılığın uygulanabilirliği açısından en güzel örnek 2014 yılında yoğun siber saldırılara maruz kalan Sonny şirketinin Kuzey Kore lideri ile ilgili filmin yayından kaldırılması olarak gösterilmektedir (Şenol, 2016: 7-8). Bu olayda saldırgan tarafın istediğini elde etmesine karşılık saldırıya maruz kalan tarafın başarısız olmasında Amir Lupovici'nin 2011 yılında yaptığı çalışmasında caydırıcılığın yetenekleri ve cezalandırma şartlarının sağlanmasındaki başarısızlığı olarak nitelendirmiştir (Lupovici, 2011: 54).

Caydırıcı Teoriler

Literatürde birçok teorisyen siber caydırıcılık kavramında devletlerin karşılıklı etkileşimine odaklanmışlardır (Lupovici, 2016: 326). Libicki siber caydırıcılıkta sadece devlet aktörlerine odaklanmamızı söylemiştir (Libicki, 2009: 26). Siber caydırıcı görüşün önerilen bir çıkarımı bize savunmacının istediği çeşitli istenmeyen faaliyet çeşitlerini ve bunu yapan aktörleri araştırmaktadır. Devlet dışı aktörlerin siber savaşı nasıl kullandıklarına ilişkin çok fazla veri yokken, bu savaşı neden yaptıklarına dair de ampirik bir sonuç yoktur. Savunmacının stratejisi açısından devletler, devlet ve devlet dışı aktörlerin faaliyetlerini engellemek için siber caydırıcılığı kullanmaktadır (Lupovici, 2016: 326).

Literatürde siber ve kinetik arasındaki kesişmeler aktörler aracılığıyla siber caydırıcılığı kavramsallaştırmak anlamına gelmektedir. Teorisyenler bu alanlar arasındaki etkileşimleri çeşitli şekillerde kabul etmişlerdir. Libicki siber caydırıcılığı etkileyen kinetik araçların farklı yönlerini tartışmış, sonuç olarak ise siber tehditleri caydırmak için siber araçların kullanımına değinmiştir (Libicki, 2009: 145-150).

Siber caydırıcılık ve kinetik caydırıcı araçlar, çeşitli şekillerde kesişebilmektedir, Birincisi, siber saldırıyı caydırmak adına savunucunun caydırıcı duruşunu geliştirmek için siber ve kinetik araçların birbirini tamamlayabilmesidir. Bazı bilim adamları, bir siber saldırıyı caydırmayı amaçlayan misilleme faktörünün caydırıcı tehdidinin siber savaşla sınırlandırılması gerekmediğini, aynı zamanda savunma aktörünün çeşitli yeteneklerine de dayanabileceğini ileri sürmektedir. Bu yetenekleri ise askeri silahlar, diplomatik ve siyasi araçlar, iç güvenlik birimleri, adalet sistemi ve uluslararası hukuk şeklinde sıralamak mümkündür (Lupovici, 2016: 329).

İkincisi, siber ve kinetik araçlar, kinetik yollarla kullanılan biraz daha geleneksel bir saldırıyı caydırmak için birbirini tamamlayabilmektedir. Bunun önemli bir örneği Askeri İşlerde Devrim (RMA) sistemlerinde zaten görülebilir. Bu tür sistemleri, diğer şeylerin yanı sıra komuta ve kontrol yeteneklerini geliştirmekte ve böylece caydırıcılık güvenilirliğini arttırabilmektedir (Morgan, 2003: 21).

Son olarak siber ve kinetik araçların bir savunmacının kinetik misilleme saldırısı tarafından caydırılan aktörlerin faaliyetlerini siber uzaya yönlendirdiği durumlarda başarılı olmaktadır. Özellikle saldıran grup karşı tarafın misilleme gücünün zayıflığını anlarlarsa başarı sağlanmış demektir (Lupovici 2016: 329). Sonuç olarak ise siber ve kinetik araçların bir arada kullanılması caydırıcı etkinliği arttırabilmektedir.

Siber Caydırıcılığa Yapısal Yaklaşım

Literatürde siber caydırıcılık alanında bir diğer zorluk ise bu alanın teoride karşılaştığı birtakım eksikliklerdir. Choucri, temel zorlukların siber ve kinetik araçların nasıl etkileşime girdiğini açıklama, bu alandaki değişiklikleri keşfetme ve çeşitli aktörleri kapsama ihtiyacı olduğunu belirtmiştir (Choucri,2012: 16).

Yapılandırmacı yaklaşımlardan alınan kavramların bütünleştirilmesi, düşünceyi ve edebiyatı bir adım öteye taşımaktadır. Aktörlerin davranışını daha iyi anlamak için özneler arası anlayışların varlığını, bilginin sosyal olarak inşa edildiğini ve dile ile sosyal bağlama bağlı olduğunu kabul etmek gerekmektedir (Lupovici, 2016: 330). Libicki' ye göre ise yapısal yaklaşım fiziksel katman (teller), sözdizimsel katman (protokoller) ve anlamsal katman (bilgi) ayı zamanda öznelerarası katmandır (Libicki, 2009: 12).

Siber caydırıcılığın yapılandırmacı bir yaklaşıma doğru yapılandırması bir siber caydırıcılık yaklaşımını tam olarak sunmak için bu makalenin ve muhtemelen tek bir makalenin kapsamı dışında olsa da siber caydırıcılığın anlaşılmasında çok önemli olan iki ana unsuru dikkate almaktadır: anonimlik ve şiddet. Bu unsurlar, siber uzayın maddi ve fiziksel özelliklerinin, sosyal bağlamda gelişen fikirlerin aracılığı ile aktörlerin davranışını nasıl etkilediğini açıkça göstermektedir (Lupovici, 2016: 331).

Siber uzayda saldırı yapanın kim veya kimler olduğu bilinmediğinden literatürde çok sayıda teorisyen ilişkilendirme sorununu siber caydırıcılıkta kilit bir rol olarak görmektedir. İlişkilendirme sorunu, çeşitli şekillerde caydırma yeteneğini karmaşıklaştırmaktadır. Birincisi, savunucuların kimliğini kesin olarak izleyemedikleri zaman, hatta sonradan bile bir rakibe tehdit iletmeleri çok zordur. İkincisi, somut delil toplamak için gereken süre arttıkça, misilleme saldırısını gerçekleştirmenin meşruiyeti azalmaktadır. Ne kadar çok zaman geçerse, savunucunun karşılaştığı istenmeyen olaya misilleme şansı o kadar azalmaktadır (Libicki, 2009: 42). Eric T. Jensen "kendinizi saldırılardan korumanın yolu düşmanınıza karşı görünmez olmalısınız" sözü bu hususta dikkate değerdir. Eğer düşman saldırmak istediği sistemleri veya bilgisayarları bulamazsa, savunma yapan taraf ne kadar güçlü olursa olsun eğer hedefi bulamazsa saldırı yapmaktan sakınacaktır (Jensen, 2012: 817). Goodman ise ilişkilendirmeyi siber saldırı ve misillemede kesinlikle zorluklar yaratır şeklinde tanımlamıştır (Goodman, 2010: 124).

Şiddet sorunu ise siber caydırıcılığı etkileyen bir başka tartışılan kavramdır. Bazı akademisyenler, şiddetin anlamının siber sorunları yasal bir perspektiften nasıl etkilediğine dair çalışmaya başlamıştır. Bu çalışmalar esas olarak, siber tehditlerle karşılaşıldığında güç kullanımının meşru olduğu koşulları belirlemek için BM şartının 4. ve 51. Maddelerinin yorumlanmasına odaklanmaktadır. Bir misilleme cevabı, silahlı bir saldırıya cevap ise haklı çıkarılırken, siber savaş araçları çalıştırıldığında silahlı saldırıyı neyin oluşturduğu sorusu tam olarak cevaplanamamaktadır (Lupovici, 2016: 334).

David J.Lonsdale'ye göre savaş eğilimleri caydırıcılığı dizginlemek istemektedir. Aslında ahlaki meşruiyet caydırıcılık için savaşa kadar uzanmaktadır çünkü caydırıcılık için birincil niyet ikinci bir misilleme niyetini kullanmayı gerektirmektedir (Lonsdale, 2018: 415).

Siber uzayda neyin bir savaş eylemi oluşturduğuna dair de bir belirsizlik vardır. Libicki, bir savaş eyleminin uluslararası düzeylerde görülebileceğini öne sürmektedir. Örneğin, evrensel veya çok taraflı düzeyde ve ayrıca tek taraflı düzeyde. Bununla birlikte, BM tüzüğünün yorumlanması ve siber savaş konusunda küresel bir antlaşmanın bulunmaması ile ilgili tartışmalarda gösterildiği gibi evrensel bir tanımı da yoktur. Aynı şekilde, bir siber saldırıya uğrayan herhangi bir devlet tek taraflı olarak bunun bir siber saldırı olduğunu ilan etmesi mümkündür. Savaş durumunda, siber saldırının ilan edilmesi, bu görüşün meşru olup olmadığı ve dolayısıyla misillemenin haklı olup olmadığı sorusu kalmaktadır (Libicki, 2009: 180).

Şiddet hem sosyal hem de hukuki boyutla ilgilidir. Bir aktörün misillemesi, şiddet içeren bir eylemin alınmasını takip ederse daha meşru olur. Bu nedenle caydırıcı bir tehdit, bu durumlarda sorunun şiddetli bir saldırı olarak görülüp görülmeyeceği konusunda fikir birliğinin olmadığı durumlarda olduğundan daha inandırıcıdır. Önemli olan nokta, sorunun ille de ne kadar hasara neden olduğu değil, daha ziyade ona neden olmak için kullanılan araçların nasıl çerçevelendiğidir (Lupovici, 2016: 337). Sonuç olarak siber caydırıcılık teorisinde şiddet sorunsalı siber alanda aktörlerin siber araçlar kullanmasına neden olabilmektedir fakat şiddet kullanılması sorunsalının belirsizliği bu araçların başarısız olduğu anlamına gelmemektedir.

Siber Caydırıcılık Stratejileri

Soğuk Savaş sonrası süper güçler bu sefer de siber uzay dediğimiz alana hâkimiyet kurmak için birbirleri ile kıyasıya yarışa girmiştir. Burada en büyük sorun siber alanın ne kadar geniş olduğu, hâkimiyetinin ise karasal ve denizel alan savunmasından daha zor olmasından kaynaklanan birtakım sorunlar çerçevesinde teorisyenler siber caydırıcılık stratejileri geliştirmişlerdir. Siber caydırıcılığın kapsamlı ve korunaklı olması için güçlü bir savunma ağı kurmak ve yönetmek gerekmektedir. Siber saldırılar çok küçük çıkarlar için olabileceği gibi devletler ve özel sektör için hayati sayılabilecek temel fonksiyonlara karşı da yapılabilmektedir. Siber saldırılar sadece zarar vermek için değil, politik ve stratejik hedefler için de yapılmaktadır (Kugler, 2009: 10). Bu sebepten dolayı başta devlet ve devletlerarası kurumlar olmak üzere birçok alanda siber güvenlik stratejileri geliştirilmektedir. Burada temel amaç siber güvenliği tam olarak sağlamak olmasa da zararlarını minimum düzeye indirebilmektir. Bu nedenle başka büyük devletler olmak üzere birçok devlet kendi

bünyesinde siber strateji hamleleri yapmışlardır. Örneğin Avrupa Birliği ile ABD arasında ortaklaşa siber güvenlik strateji hamleleri yapılmıştır. Özellikle İngiltere ve ABD siber caydırıcılık alanında önemli bir gelişme göstermiştir (Korhan, 2016: 153-154).

Siber caydırıcılık alanında stratejik hamleler yapan bir diğer ülke ise 2009 yılında kurmuş olduğu Bilgi ve İletişim Güvenliği Departmanı içinde Kritik Altyapı Koruması Bilgi Güvenliği Çalışma Grubu olan Brezilya'dır (Kugler, 2009: 12).

Soğuk Savaş dönemi klasik caydırıcılık için kurulmuş olan devletlerarası kurum NATO'dur. NATO bu amaç için Portekiz ve Oberammergua'da bulunan siber akademi okulları aracılığıyla ittifak halinde olan ülkelerle toplu siber saldırılara karşı ortak bir tutum almaktadır. Burada da ittifak devletlere savunma hedeflerini oluşturmak için iki yıllık bir eğitim verilmektedir (NATO Dergisi, 2016). Hatta bu amaçla NATO müttefiki olan ülkemizde de Türk Silahlı Kuvvetleri içerisinde 2017 yılında Siber Savunma Harekât Merkezi Komutanlığı kurulmuştur (Savunma Sanayi Bakanlığı Dergisi, 2017).

Sonuç olarak 2000'li yıllardan başlayarak gelişim gösteren siber alan her gün önemini arttırmaktadır. Sadece devletler değil devletlerarası kurumlar, hatta çok uluslu şirketler başta olmak üzere birçok büyük ölçekli şirket siber saldırıları minimum düzeye indirmek için önlemini almaktadır. Şimdiye kadar yapılan siber saldırılardan anlaşıldığı üzere siber saldırıları tamamen durdurmak neredeyse imkânsız iken, amaç bu saldırılar sonucu oluşan zararları en düşük seviyede tutabilmektir (Kugler, 2009: 10-15).

Sonuç

İçinde bulunduğumuz çağ teknoloji çağıdır. Küreselleşme ve beraberinde yaşanan gelişmeler insanlığa sınırsız imkân tanırken bazı sorunları da beraberinde getirmiştir. Siber alan bu sorunların vücut bulduğu alanların başında gelmektedir. Özellikle bilişim teknolojileri alanında devletlerin kritik alt yapılarına karşı yapılan kötü amaçlı saldırılar bu sorunlara örnek teşkil etmektedir. Bireyler, devletler ya da devlet dışı diğer aktörler, aralarında yaşanan anlaşmazlıkları ya da uyuşmazlıkları barışçıl yollarla çözemediklerinde siber caydırıcılık faktörünü bir araç olarak kullanabilmektedir. Bunun da ötesinde caydırıcılık farklı amaçlar için de başvurulan bir yöntemdir. Soğuk Savaş döneminde devletler birbirlerine karşı

saldırganlığı önlemek için nükleer silahlara başvurmayı tercih etmiştir. Nükleer caydırıcılık devletler için temel stratejilerden biri haline gelmiştir.

Günümüzde aktörler siber alanda savunma ve saldırganlığı azaltmak için siber caydırıcılık teorisini geliştirme yoluna gitmiştir. Nükleer caydırıcılık ya da diğer bir tabirle klasik caydırıcılık ile siber caydırıcılık arasındaki temel farklılıkları şu şekilde sıralamak mümkündür:

Misilleme sorunu

Kapasite sorunu

Kimlik sorunu

Aktör sorunu

Uluslararası ortamın doğası gereği oluşan denetim algısı sorunu (Ermiş, 2015: 112 ve Şenol, 2016: 14-15).

Soğuk Savaş sürecinde ve sonrasında süper güç olan devletlerin birbirlerine karşı nükleer silaha başvurmaları caydırıcılık etkisi yaratarak işe yaramıştır. Özellikle 2000'li yılların günümüze kadar olan sürede siber alanda siber caydırıcılığın belli başlı sorunlar sebebiyle yüzde yüz caydırıcılık sağlamadığı görülmüştür. Siber caydırıcılığın henüz istenen caydırıcılığı sağlamadığını savunan teorisyenler de bulunmaktadır (Ermiş, 2015: 114).

Siber caydırıcılığın birtakım zorlukları bulunmaktadır. Nükleer saldırıların oluşmasını engelleyen temel faktör olan caydırıcılık teorisi, günümüzde siber alanda yaşanacak olan bir çatışmayı durdurmakta yetersiz kalabilmektedir. Örneğin ABD'nin nükleer alanda sağladığı başarılı bir caydırıcılığı, gelişmiş teknolojisine rağmen siber alanda sağlayamayacağı öngörülmektedir. (Libicki, 2009: 130). Bu görüş, 2011 yılında ABD Savunma Bakanlığınca hazırlanan raporlardan sızan bilgilerden, "siber saldırıların savaş sebebi sayılacağının ve askeri operasyonlarla karşılık verilebileceğinin açıklanması" ile savunulmaktadır (Nacita & Reith, 2018: 78).

Nükleer silahları kullanılması ve karşılık verilebilirliğinin az da olsa bilinmesi nükleer caydırıcılığın aktif olarak kullanılmasını sağlamıştır. Siber caydırıcılıkta ise özellikle siber saldırıyı yapanın kim olduğunun bilinmemesi gibi birtakım sorunların beraberinde getirdiği zorluklarla siber caydırıcılığın başarılı bir savunma aracı olarak kullanılmasının zorlaştırdığı anlaşılmaktadır.

Temelde hem siber hem de nükleer caydırıcılığın birbirinden farklı olması nedeniyle bu iki teoriyi karşılaştırmada da farlılıklar olacaktır. Bazı teorisyenler siber caydırıcılık teorisinin nükleer caydırıcılık teorisi ile açıklanamayacağı kanaatindedir. Burada teorisyenler aktör, etki ve denetim düzeyi bakımından temel belirsizlikler olduğunu düşünmektedir (Ermiş, 2015: 116). Siber alanda özellikle siber saldırılar için kullanılan birtakım argümanların temelde nükleer caydırıcılık için kullanılan argümanlardan farklı olması ve bu argümanların devlet dışı aktörler tarafından kullanılıp geliştirilebilmesinden ötürü siber caydırıcılığın tamamen sağlanacağı görüşüne karşı çıkmışlardır. Kimi teorisyenler ise siber alanda henüz çok büyük bir siber savaş olmadığından ve bu savaşta da en gelişmiş siber savaş araçları kullanılmadığından dolayı siber caydırıcılığın sonucunu tahmin etmenin zor olduğu düşüncesindedir (Sağıroğlu, Alkan, 2018: 211-217).

Sonuç olarak ülkelerarası ilişkilerde, siber caydırıcılığın 21. yüzyıl diplomasisinin bir aracı olacağı gittikçe daha açık hale gelmektedir (Bilişim İnovasyon Derneği, 2018: 12). Özellikle devletlerin siber alanda anarşik yapısı ve güç dağılımı göz önünde bulundurulduğunda siber caydırıcılığın daha fazla öneme sahip olacağı açıktır. Sadece devletler değil bireyler ve devlet dışı aktörler de gelişen teknoloji ile siber alanda herhangi olumsuz bir durumla karşılaşmamak için kendilerince birtakım önlemler alacaktır.

Teknolojinin gelişmesiyle ve nesnelerin internetleşmesi ile birlikte siber alanın daha fazla güvenlik isteyen bir alan haline geleceğini düşünmek zor olmasa gerektir. Bu yaklaşımla birlikte siber caydırıcılığın ilerleyen yıllarda hangi boyutta ve nasıl kullanılacağı, başka argümanlar ile birleşeceği ve böylece etkinliğini arttırma yoluna gideceği anlaşılmıştır. Siber alanda caydırıcılığın etkinliğini arttırabilmesi içinde yeni birtakım gelişmiş yazılım ya da ileri teknoloji argümanlar kullanılacağı anlaşılmaktadır. Siber caydırıcılık bu sayede etkisini arttıracaktır. Uluslararası alanda olmasa bile devletlerin kendi iç işlerinde hiyerarşik yapıyı korumak ve güç kaybını önlemek için birtakım yaptırımlar kullanarak siber alanda özellikle siber suçlarda caydırıcılığı aktif olarak sağlayacakları beklentisi oluşmaktadır.

Kaynakça

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

Arreguin-Toft, I.(2001). How the Weak Win Wars A Theory of Asymmetric Conflict. *International Security*. Vol.26, No.1, pp.93-128. https://web.stanford.edu/class/polisci211z/2.2/Arreguin-Toft%20IS%202001.pdf [Erişim Tarihi:15.12.2020]

Burton, J.(2018). Cyber Deterrence: A Comprehensive Approach?. https://ccdcoe.org/uploads/2018/10/BURTON_Cyber_Deterrence_paper_April2018.pdf [Erişim Tarihi:16.12.2020]

Choucri, N.(2012). *Cyberpolitics in International Relations*. England: The MIT press London

DIGITAL IN 2020. https://wearesocial.com/digital-2020 [Erişim Tarihi:06.12.2020]

Ermiş, U.(2015). *Siber Caydırıcılık Kavramının Nükleer Caydırıcılık Olgusu ile Karşılaştırmalı Analizi.*(Yayımlanmamış yüksek lisans tezi).Uludağ Üniversitesi Sosyal Bilimler Enstitüsü.Bursa. https://acikerisim.uludag.edu.tr/bitstream/11452/10408/1/427442.pdf [Erişim Tarihi:07.12.2020]

Gartzke, E. & Jo, D.(2009). Bargaining, Nuclear Proliferation, and Interstate Disputes. https://wjspaniel.files.wordpress.com/2018/09/gartzke-and-jo.pdf [Erişim Tarihi:16.12.2020]

Geçer, K.T. v.d.,(2013). *Atatürk'ün Sözlerinde Asker ve Asker Mesleği.* Ankara: Genel Kurmay Basımevi. https://www.msb.gov.tr/Content/Upload/Docs/askeritariharsiv/ataturksozlerindeasker.pdf [Erişim Tarihi:12.12.2020]

Goodman, W.(2010). Cyber Deterrence: Tougher in Theory than in Practice?. *Strategic Studies Quarterly*. https://www.airuniversity.af.edu/Portals/10/SSQ/documents/Volume-04_Issue-3/Goodman.pdf [Erişim Tarihi:11.12.2020]

Gündoğdu, E.(2016). Uluslararası İlişkilerde Caydırma Teorisi. *Marmara Üniversitesi Siyasal Bilimler Dergisi,* Cilt.4, Sayı.2, ss.1-22. https://dergipark.org.tr/tr/download/article-file/222974 [Erişim Tarihi:12.20.2020]

Haley, C.(2013). A Theory of Cyber Deterrence. https://www.georgetownjournalofinternationalaffairs.org/online-edition/a-theory-of-cyber-deterrence-christopher-haley [Erişim Tarihi:10.12.2020]

Harvey, F.P.(1997). *The Futures Back: Nuclear Rivarlry, Deterrence Theory, and Crisis Stability after Cold War*, London: McGill-Quenn's University Press. https://books.google.gm/books?id=dxeUmWufv5QC&printsec=frontcover#v=onepage&q&f=false [Erişim Tarihi:13.12.2020]

Huth, P.K.(1999). DETERRENCE AND INTERNATIONAL CONFLICT: Empiricial Findings and Theoretical Debates. *Annual Review of Political Science*. Vol.2, Sayı.25, pp.25-

48. https://www.annualreviews.org/doi/pdf/10.1146/annurev.polisci.2.1.25 [Erişim Tarihi:13.12.2020]

Iasıello, E.(2018). Is Cyber Deterrence an Illusory Course of Action?. *ASPJ Africa&Francophonie.* Vol.9, No.1, pp.35-51. https://www.airuniversity.af.edu/Portals/10/ASPJ_French/journals_E/Volume-09_Issue-1/iasiello_e.pdf [Erişim Tarihi:16.12.2020]

Jensen, E.T.(2012). Cyber Deterrence. *Emory International Law Rewiew*. Vol.26, pp.773-824. https://law.emory.edu/eilr/_documents/volumes/26/2/symposium/jensen.pdf [Erişim Tarihi:14.12.2020]

Korhan, S.(2016). Cyber Deterrence in International Relations. *Cyberpolitic Journal*. Vol.1, No.1, pp.147-161. http://cyberpolitikjournal.org/index.php/main/article/view/96/94 [Erişim Tarihi:06.12.2020]

Kugler, R.L.(2009). Deterrence of Cyber Attacks. https://ndupress.ndu.edu/Portals/68/Documents/Books/CTBSP-Exports/Cyberpower/Cyberpower-I-Chap-13.pdf?ver=2017-06-16-115053-773 [Erişim Tarihi:15.12.2020]

Kurtul, A. v.d., Siber Güvenlik raporu. http://www.bilisiminovasyon.org.tr/webfiles/userfiles/files/siber_guvenlik_raporu.pdf [Erişim Tarihi:15.12.2020]

Kutlu, A.K.(2019). Soğuk Savaş. *Güvenlik Yazıları Serisi*. Sayı.35, ss.1-11. https://trguvenlikportali.com/wp-content/uploads/2019/11/SogukSavas_KKAtac_v.1.pdf [Erişim Tarihi:06.12.2020].

Kydd, A.H.(2015). International Relations Theory: The Game-Theoretic Approach. *Cambridge Core*. https://www.researchgate.net/publication/325490077_International_Relations_Theory_The_Game-Theoretic_Approach [Erişim Tarihi:07.12.2020]

Liaropoulos, A.(2013). "Great Power Politics in Cyberspace: U.S.A.and China are drawing the lines between confrontation and cooperation", Marian Majer, Robert Ondrejcsak(ed.), *Panaroma of global security environment*, Bratislava: Centre for European and North Atlantic Affairs https://www.researchgate.net/publication/264327157_Great_Power_Politics_in_Cyberspace_USA_and_China_are_drawing_the_lines_between_confrontation_and_cooperation [Erişim Tarihi: 07.12.2020]

Libicki, M.C.(2009). *Cyberdeterrence and Cyberwar,* Santa Monica: Rand Corporation. https://www.rand.org/content/dam/rand/pubs/monographs/2009/RAND_MG877.pdf [Erişim Tarihi:08.12.2020]

Libicki, M.C.(2011). Cyberwar as a Confidence Game. *Strategic Studies Quarterly*.Vol.5, No.1, pp.132-146. https://www.airuniversity.af.edu/Portals/10/SSQ/documents/Volume-05_Issue-1/Libicki.pdf [Erişim Tarihi:16.12.2020]

Lieberman, E.(2013). Reconceptualizing Deterrence: Nudging toward rationality in Middle Eastern rivalries. *The Journal of Public and International Affairs Academy of Political Science.* Vol.128, No.3, pp.544-546. https://onlinelibrary.wiley.com/doi/epdf/10.1002/polq.12090 [Erişim Tarihi:09.12.2020]

Londsdale, D.(2018). Wafighting for Cyber Deterrence: a Strategic and Moral Imperative. *Philosophy&Technology*. Vol.31, No.1, pp.1-21. https://www.researchgate.net/publication/313292463_Warfighting_for_Cyber_Deterrence_a_Strategic_and_Moral_Imperative [Erişim Tarihi:14.12.2020]

Lupovici, A.(2011). Cyber Warfare and Deterrence: Trends and Challesges in Research. Military and Strategic Affairs. Vol.3, No.3, pp.49-62. https://www.inss.org.il/wp-content/uploads/2017/02/FILE1333533336-1.pdf [Erişim Tarihi:10.12.2020]

Lupovici, A.(2016). The "Attribution Problem" and the social construction of "Violence": Taking cyber deterrence literature a step forward. *International Studies Perspectives*. Vol.17, No.3, pp.322-342. https://doi.org/10.1111/insp.12082 [Erişim Tarihi: 10.12.2020]

Martin, D.G. & Miller B.(2003). Space and Contentious Politics. *Mobilization: An International Quarterly*. Vol.8, No.2, pp.143-156. https://www2.clarku.edu/departments/geography/pdfs/Deb%20Martin/martin.miller.Pp.%20143-156.pdf [Erişim Tarihi:17.12.2020]

Mearsheimer, J.J.(2009). Reckless States and Realism. *International Relations*. Vol.23, No.2, pp. 241-256. https://www.mearsheimer.com/wp-content/uploads/2019/06/Reckless-States-and-Realism.pdf [Erişim Tarihi:10.12.2020]

Morgan, P.(2010). Applicability of traditional deterrence concept and theory to the cyber realm. *Proceedings of a Workshop on Deterring Cyberattacks*. pp.55-76. https://www.nap.edu/read/12997/chapter/7 [Erişim Tarihi:18.12.2020]

Nacita, I., Reith, M.(2018). Cyber War and Deterrence. *Air&Space Power Journal*. Vol.32, No.2, pp.74-83. https://www.airuniversity.af.edu/Portals/10/ASPJ/journals/Volume-32_Issue-2/ASPJ-Summer-2018.pdf [Erişim Tarihi:11.12.2020]

NASA.(2017). https://www.nasa.gov/mission_pages/explorer/explorer-overview.html [Erişim Tarihi:13.12.2020]

NATO SCHOOL.(2020). https://www.natoschool.nato.int/ [Erişim Tarihi:10.12.2020]

Nye, J.(2015). Can Cyber Warfare Be Deterred. https://www.project-syndicate.org/ [Erişim Tarihi:11.12.2020]

Polat, D.Ş.(2020). NATO'nun Yeni Operasyon Alanı: Siber Uzay. *Güvenlik Bilimleri Dergisi,* Uluslararası Güvenlik Kongresi Özel Sayısı., ss.??? https://dergipark.org.tr/tr/download/article-file/986543 [Erişim Tarihi:15.12.2020]

Sağıroğlu, Ş. & Alkan, M.(2018). "Hibrit Savaş Kapsamında Siber Savaş ve Siber Caydırıcılık", Şeref Sağıroğlu, Mustafa Alkan(ed.), *Siber Güvenlik ve Savunma Farkındalık ve Caydırıcılık*, Ankara: Grafiker Yayınları https://www.sasad.org.tr/uploaded/Siber-Guvenlik-ve-Savunma-Farkindalik-ve-Caydiricilik.pdf [Erişim Tarihi:08.12.2020]

Seren, M.(2018).ABD Ulusal Güvenlik Strateji Belgesi: Amerikan Savunması ve Caydırıcılığı. *STM Teknolojik Düşünce Merkezi,* ss.1-14. https://thinktech.stm.com.tr/uploads/raporlar/pdf/832018143027377_stm_abdulusalguvenlikstratejibelgesi.pdf [Erişim Tarihi:15.12.2020]

Şenol, M.(2016). Siber Güçle Caydırıcılık Ama Nasıl?. *Gazi Üniversitesi Uluslararası Bilgi Mühendisliği Dergisi*. Cilt.2, Sayı.2, ss.10-17. https://dergipark.org.tr/tr/download/article-file/290469 [Erişim Tarihi:07.12.2020]

Şenol, M.(2017). Türkiye'de Siber Saldırılara Karşı Caydırıcılık. *Uluslararası Bilgi Güvenliği Dergisi,* Cilt.3, Sayı.2, ss.1-9. https://dergipark.org.tr/tr/download/article-file/396047 [Erişim Tarihi:09.12.2020]

T.C. Cumhurbaşkanlığı Savunma Sanayi Başkanlığı.(2017). https://www.ssb.gov.tr/Website/contentList.aspx?PageID=1083&LangID=1 [Erişim Tarihi:12.12.2020]

TBMM.(2016). https://www.tbmm.gov.tr/develop/owa/tutanak_g.birlesim_baslangic?P4=22611&P5=H&page1=24&page2=24 [Erişim Tarihi:17.12.2020]

Türk Dil Kurumu Sözlükleri.(2019). https://sozluk.gov.tr/ [Erişim Tarihi:06.12.2020]

Walzer, M.(2004). *Arguing About War*. New Haven&London: Yale University Press. https://books.google.com.tr/books/yup?id=sCkI0m7QffAC&pg=PR7&hl=tr&source=gbs_selected_pages&cad=1#v=onepage&q&f=false [Erişim Tarihi:15.12.2020]