PROTOKOL

2022 | YIL 3 SAYI 2

KARADENİZ TEKNİK ÜNİVERSİTESİ STRATEJİK ARAŞTIRMA MERKEZİ DERGİSİ

KARADENİZ TEKNİK ÜNİVERSİTESİ

STRATEJİK ARAŞTIRMA MERKEZİ

PROTOKOL DERGİSİ

İLETİŞİM

Karadeniz Teknik Üniversitesi

İktisadi ve İdari Bilimler Fakültesi, No:2-06

Telefon: 04623773227

Faks: +90 462 325 3205 – 325 3185

E-Posta: sam@ktu.edu.tr

Web: www.ktu.edu.tr/sam

Yayın Türü:

Ulusal Süreli

SAHİBİ

Doç. Dr.
Özgür TÜFEKÇİ

Karadeniz Teknik Üniversitesi
Stratejik Araştırma Merkezi Müdürü

KTÜ SAM Protokol Dergisi kamu yönetimi, uluslararası ilişkiler, iktisat, işletme ve sosyoloji başta olmak üzere sosyal bilimler alanında, kısa makalelere yer veren akademik bir dergidir. Kısa makalelerin yanı sıra rapor, derleme, konferans notları, örnek olay, kitap tanıtımı vb. makale dışı yazılara da dergi bünyesinde her sayıda belirli oranda yer verilecektir.

KTÜ SAM Protokol Dergisi Şubat ve Ağustos aylarında olmak üzere yılda iki kez yayımlanır.

KARADENİZ
TEKNİK ÜNİVERSİTESİ
Stratejik Araştırma Merkezi

SAM

PROTOKOL

2022 | YIL 3 SAYI 2

KARADENİZ TEKNİK ÜNİVERSİTESİ STRATEJİK ARAŞTIRMA MERKEZİ DERGİSİ

İÇİNDEKİLER

PROTOKOL

SİBER CAYDIRICILIK: DEVLETLER SİBER CAYDIRICILIĞI ÖĞRENEBİLİR Mİ?

Yüksek Lisans Öğrencisi Kadriye Koyuncu
Karadeniz Teknik Üniversitesi
kadriyekoyuncu107@gmail.com

ÖZ

Güvenlik algılarının asırlar geçtikçe boyut değiştirmesiyle birlikte geleneksel konvansiyonel güvenlik algılarına yenileri eklenmiştir. Siber güvenlik bunların en yeni olanıdır. Son yıllarda devlet kurumlarına yönelik artan siber saldırılar nedeniyle siber caydırıcılık kavramı öne çıkmış ve bu konuda çeşitli tartışmalar, iddialar ortaya atılmıştır. En çok tartışılan sorunlar arasında ise siber caydırıcılığın mümkün olup olmadığı ve siber caydırıcılığın kapsamının ne olması gerektiğidir. Bu yeni güvenlik alanının sınırlarının belirsizliği devletlerin en büyük handikaplarından biridir. Zira sanal alem denilen alanda kimlikler kolayca gizlenebilir ve tespit edilmesi çok zordur. Siber caydırıcılık kavramı da bu belirsizlik nedeniyle tartışmalıdır. Bundan dolayı devletler siber güvenliklerini sağlamak için siber caydırıcılık faaliyetlerine önem vermeye başlamışlardır.

Anahtar Kelimeler: Siber Caydırıcılık, Caydırıcılık, Devletler ve Siber Caydırıcılık

Giriş

Tarih boyunca çeşitli medeniyetler kendilerini diğer medeniyetlerin olası saldırılarına karşı korumak amacıyla önlemler almışlardır. Bu önlemler genellikle kaleler, surlar, duvarlar inşaa etmek şeklinde olmuştur. Bunların yanında düşmanın eylemlerini yönlendirmek ve olası saldırılarından vazgeçirmek için çeşitli caydırıcılık yöntemleri kullanılmıştır. O dönemlerde caydırıcılık kavramı teoride çok dile getirilen bir olgu olmasa da pratikte çokça kullanılan bir yöntemdi. Dönemin önemli şahsiyetlerinin ifadelerinden bu durum anlaşılabilir. Örneğin Çinli stratejist Sun Tzu, rakibin eğilimlerini tehdit ile yönlendirmenin önemine dikkat çekmiştir (McNeilly, 2003; McNeilly ve McNeilly, 2012). Dolayısıyla caydırıcılık kavramı herhangi bir rakibin, saldırıyı düşünmesini ve gözden geçirmesini önleme, düşünse bile bunun kendisi açısından çok ağır sonuçları olacağına onu ikna etmesidir. Bu yönüyle caydırıcılık çoğunlukla askeri alanda gelişme göstermiştir (Du Pisani, 2006: 83-96). Ancak insanlık geliştikçe kendi medeniyetlerini koruma yöntemleri de gelişmiş ve değişime uğramıştır. Eski çağlarda kullanılan bu yöntemler bugün evrimleşerek yerini ekonomik

caydırıcılık, nükleer caydırıcılık, siber caydırıcılık gibi kavramlara bırakmıştır.

Teknoloji ve dijitalleşmenin gelişimiyle internet, siber alan gibi kavramların ortaya çıkması bir dizi sorunu da beraberinde getirmiştir. Bu sorunlardan biri siber alanda caydırıcılığın nasıl sağlanabileceğidir. Zira klasik caydırıcılıkta tehdit ve düşmanlar açıkça belliydi ve caydırıcılık sağlamak için nispeten daha az karmaşık bilgilere ihtiyaç vardı (Ermiş, 2015). Ancak siber alan birbirlerini göremeyen, tanımayan sonsuz düşmanla doludur.

Klasik caydırıcılık kavramı bir oyuncunun diğer bir oyuncuyu veya olası bir saldırganı, saldırısının bir bedeli olacağına, büyük bir ihtimalle bunun kabul edilemeyecek zarara yol açabileceğine ve bu zararın maddi veya siyasi kazanç beklentisinin üzerinde olacağına ikna etmesi durumu (Paulaukas, 2016; Ermiş, 2015), olarak tanımlanmaktadır. Aslında diğer caydırıcılık türlerinde temelde klasik caydırıcılık mantığına dayanmaktadır. Bu bağlamda siber caydırıcılık, siber alanda saldırgan veya saldırganların, saldırılarının bir bedeli olacağına ve bu bedelin maliyetinin saldırıdan yüksek olacağına ikna edilmesidir denebilir.

Siber alan suç işlemeye çok müsaittir. Bu suçlar genellikle siber casusluk, siber terörizmdir. Özellikle siber casusluk özel şirketlerde de endüstriyel casusluk olarak görülebilmektedir (van der Meer, 2016: 95). Peki devletler bu siber tehditler karşısında nasıl bir strateji geliştirmekte, hangi önlemleri almaktadırlar? bu soruları takiben devletlerin siber caydırıcılıktan ne anladıkları, dolayısıyla siber caydırıcılığı öğrenip öğrenemeyecekleri bu çalışmanın ana sorunsallarıdır. Bu bağlamda literatür taramasının ardından siber caydırıcılığın devletler tarafından hangi argümanla kullanıldığı veya kullanılmaya çalışıldığı tartışılacak ve çalışmanın ana sorusu olan “devletler siber caydırıcılığı öğrenebilir mi?” sorusu yanıtlanmaya çalışılacaktır.

1. Literatür Taraması

Literatürde siber caydırıcılığı anlamak için ilk önce caydırıcılık kavramının kendisine bakmak doğru olacaktır. Bu bağlamda caydırıcılığa ait bazı tanım ve bilgiler literatür taramasında da verilecektir. Jervis ve Stein (1989), etimolojik olarak caydırıcılık kavramının latice ‘terror’ (terör) kelimesine dayandığını ve yine latince ‘deterre’ (korkutup kaçırmak) kelimesi ile başladığını belirtmişlerdir (Jervis & Stein, 1989). Tehdit ve bu tehdidin karşı tarafta korku yaratma potansiyelinin caydırıcılık kavramı ile ilgili olması bu tanımı destekler niteliktedir. Bu durumda caydırıcılık bir kimseyi korkutarak bir eylemi yapmaktan alıkoymaktır. Uluslararası ilişkiler literatüründe ise caydırıcılık, devletlerin diğer

devletleri güç kullanma tehdidi ile istedikleri yönde hareket etmelerini sağlamak üzere güçlerini somut dış politika çıktılarına dönüştürmeleridir (Schelling, 1958: 203-264).

Mehmetcik (2015: 31-60), caydırıcılık kavramının 21. Yüzyılda neyi ifade ettiğini ve geçmişten bugüne teoride ve pratikte nelerin değiştiğini analiz etmiştir. Bu bağlamda tarihte caydırıcılık kavramına atıfta bulunduğu görülen ünlü stratejist Sun Tzu'dan Clausewitz'e birçok önemli kişi bulunmakla birlikte, sistematik olarak caydırıcılık kavramı Soğuk Savaş döneminde çalışılmaya başlanmıştır. Yani caydırıcılık kavramı 21. Yüzyılın ürünüdür denebilir. Bunun yanında kavramın Soğuk Savaş yıllarında ifade ettiği anlam ve uygulamalar 21. Yüzyıla gelindiğinde değişime uğramıştır, uluslararası arenada meydana gelen olayların da etkisiyle caydırıcılık yeni boyutlar kazanmıştır. Özellikle nükleer silahların geliştirilmesiyle, daha çok Nükleer Caydırıcılık üzerinde durulmuştur.

Paulaukas (2016), NATO Dergisi'nde yayımladığı yazısında caydırıcılık kavramını çok basit bir şekilde bir oyuncunun diğer bir oyuncuyu veya olası bir saldırganı, saldırısının bir bedeli Olacağına, büyük bir ihtimalle bunun kabul edilemeyecek zarara yol açabileceğine ve bu zararın maddi veya siyasi kazanç beklentisinin üzerinde olacağına ikna etmesi durumu olarak açıklamıştır. Bu tanımlama, çok basit bir fikir olarak belirtilmesine rağmen uluslararası sistemdeki bazı olgular işin içine katıldığında kavramın karmaşıklığını göz önünde bulundurmaktadır. Öncelikle en az iki aktörün var olması gerekliliği, kavramı karmaşık bir sosyal ilişkiler ağına dönüştürmektedir. Burada kavramın kapsamı ise korku, cesaret, güven, güç arzusu, intikam gibi insan doğası, psikolojisi ve temel insani duygular ile ilişkili olmaktadır.

NATO Soğuk Savaş döneminde inkâr yoluyla caydırma ve cezalandırma yoluyla caydırma yöntemlerini kullanmıştır (NATO, 2022; Paulauskas, 2016). Cezalandırma yoluyla caydırma temelde "kabul edilemez" zararlar verme fikrini barındırmaktadır. Bu yöntem nükleer veya konvansiyonel fark etmeksizin olası bir Sovyet saldırısına karşı uygulanan caydırıcılık yöntemlerinden biriydi. İnkâr yoluyla caydırma ise saldırganın hedefine ulaşmasını fiziksel olarak zorlaştırmak anlamına gelmektedir (NATO, 2022; Paulauskas, 2016). Goodman (2010: 102-135), çıkar, caydırıcı beyan, inkâr tedbirleri, ceza tedbirleri, güvenilirlik, güvence, korku ve maliyet-fayda hesaplamasını caydırıcılığın sekiz unsuru olarak belirlemiştir. Caydırıcılık mantığında "bunu yapma yoksa bu olur" vurgusu yatmaktadır. Siber caydırıcılık, diğer tüm caydırıcılıklar gibi, bir düşman saldırgan davranmamaya karar verdiğinde başarılı olur (Davis, 2014: 327). Bu karar iki ayrı değerlendirmeyi takip eder: siber saldırganlığın

maliyetlerinin faydalarından daha fazla olup olmadığı ve siber uzayda kısıtlamanın faydalarının maliyetlerinden daha fazla olup olmadığıdır (Goodman, 2010: 102-135; Hoffman, 2019: 131-152).

Literatürde siber caydırıcılığa ait birçok çalışma bulunmakla birlikte bu çalışmada daha çok ayırt edici çalışmalar göz önünde bulundurulmaya çalışılmıştır. Literatüre bakıldığında siber caydırıcılığın sağlanmasındaki en önemli engellerden biri olarak saldırganın kimliğinin belirlenememesi olduğu görülmektedir. Bu da misilleme problemini ortaya çıkarmaktadır. Van der Meer, (2016: 95), savunma, caydırıcılık ve diplomasi olgularının siber güvenlikte dış politika enstrümanı olarak kullanılmasını incelediği çalışmasında siber caydırıcılıkta aktif caydırıcılık seçeneğini tartışmıştır. Bu bağlamda aktif caydırıcılığı "misilleme olasılığı ile potansiyel siber saldırganların caydırılması" olarak tanımlamıştır (Van der Meer, 2016: 95; Lupovici, 2016: 322-342; Meer, 2017: 85-135).

Buna göre siber güvenlikte misillemenin gerçekleştirilmesi için saldırganın kimliğinin bilinmesi gerekir. Ancak bahsedildiği gibi siber alanda kimliklerin tespitinin zor olması işleri zorlaştırmaktadır. Bazı devletlerde siber saldırılarda kendilerini hacker grupları gibi oluşumlarla gizleyebilmektedir. Saldırıya uğrayan devlet, saldırganın başka bir devlet olduğunu çoğu zaman ispatlayamaz. Böyle bir argümanı öne sürdüğünde ise karşı taraf iddiaları reddeder ise masum bir tarafın suçlanma riski ortaya çıkar. Bu durumda çok az devlet bunun riskini alabilir (van der Meer, 2016: 95).

Bu bağlamda van der Meer, siber alandaki güçlü hukuki yetkinlikler saldırgan tarafın belirlenmesi açısından çok önemli olduğunu belirtmekte, daha yüksek bir kimlik tespit edebilme olasılığının potansiyel saldırganlar üzerinde caydırıcı bir etki yaratacağını savunmaktadır. Dolayısıyla siber alan ve bu alandaki zafiyetler konusunda uluslararası iş birliğinin elzem olduğunu vurgulamıştır (van der Meer, 2016: 95).

Stevens (2012: 148-170), ABD'nin 1990'lardan beri siber caydırıcılığı stratejik bir araç olarak nasıl geliştirmeye çalıştığını incelemiştir. Bu bağlamda Stevens, siber caydırıcılık teorisinin vücudunun 2007 Estonya ve 2008 Gürcistan saldırıları ile birlikte geliştiğini ancak bunun somut olarak bir politika veya stratejiye dönüşme konusunda büyük ölçüde başarısız olunduğunu savunmaktadır. Ayrıca Stevens, devletlerin amacının siber uzayda güç kullanımının normalleştirilmek olduğunu, ancak bu konuda izlenecek yollar arasında farklılıklar olduğunu belirtmektedir (Stevens,

2012: 148-170).

Burton (2018), da misilleme ve anonimlik sorununa dikkat çekerek eğer bir düşmanın kimliği bilinemezse cezalandırılamayacağını belirtmiştir. Bununla birlikte Burton, siber caydırıcılığın imkânsız olmadığını ancak birçok faktörün siber caydırıcılığı sınırlandırdığını vurgulamıştır. Burton (2018), soğuk savaş caydırıcılığı ve siber caydırıcılığı karşılaştırdığında ise nükleer caydırıcılığın görülebilir dehşeti ve verdikleri zarar olduğunu, ancak siber caydırıcılıkta etkilerin görünmez ve aynı şok değerini oluşturamadığını belirtmişti. Bununla birlikte Burton'a (2018) göre, siber caydırıcılıkta soğuk savaştan kalma caydırıcılık kavramlarına güvenmek etkisiz olacaktır. Bunun yenine caydırıcılığa yönelik yasal, sosyal, normatif ve teknolojik yaklaşımları içeren özel bir yaklaşımın daha çok işe yarayabileceğini iddia etmektedir (Burton, 2018).

2. Siber Caydırıcılığın Değerlendirilmesi

Siber caydırıcılık, savunan bir devletin, daha büyük bir misilleme yapma korkusuyla yıkıcı siber faaliyetlerde bulunmaktan kaçınmak için bir rakibin karar alma aygıtını hedef alarak ve etkileyerek düşmanca siber faaliyetleri caydırma niyetlerini işaret ederek statükoyu korumaya çalıştığı bir stratejidir (Huang vd., 2018: 1-36; Brantly, 2018: 31-54).

Siber caydırıcılığın başarılı olabilmesi için tıpkı diğer caydırıcılık türlerinde olduğu gibi düşmanın saldırgan davranmamaya karar vermesi gerekir. Bu kararın arkasındaki değerlendirmeler; saldırganlığın maliyetinin faydalarından daha fazla olup olmadığı ve siber uzaydaki kısıtlamaların faydalarının maliyetinden daha fazla olup olmadığıdır (Goodman, 2010: 102-135). Dolayısıyla bir saldırgan saldırı yapmadan önce kar-zarar hesabı yapar.

Şüphesiz ki siber alanda caydırıcılık diğer caydırıcılık türlerine oranla daha karmaşık ve zordur. Bu zorluğun büyük bir bölümünü anonimlik kaplamaktadır. Ancak maliyet açısından düşünüldüğünde siber alanda caydırıcılık diğer alanlardaki caydırıcılık türlerinden daha ucuzdur. Burada özellikle siber alanda yaşanabilecek muhtemel bir çatışmanın vereceği zararların daha hafif kalması belirtilmelidir. Bu nedenle siber uzayda caydırıcılığın sağlanabilmesi için üç önemli faktörden söz etmek gerekmektedir. Bunlar gelecekte yaşanması muhtemel siber savaş tehdidinin hızla artması, diğer dört boyutta (kara, hava, deniz, uzay) başarıyla uygulanan caydırıcılığın beşinci boyutta, yani siber alanda etkili olma ihtimalinin düşünülmesi ve caydırıcılığı sağlamak için yapılacak bütün yatırımların maliyetinin, yaşanacak

çatışmada ortaya çıkacak zararlardan nispeten daha az olmasıdır (Ermiş, 2015; Goodman, 2010: 102-135).

Goodman, genel olarak caydırıcılığın sağlanabilmesi için sekiz temel unsur ortaya atmıştır (Goodman, 2010: 102-135). Bunlar: menfaat, caydırıcı deklarasyon, esirgeyici/engelleyici önlemler, cezalandırıcı önlemler, inanırlık, güven verme, korku ve kar-zarar hesabıdır. Bu bahsedilen caydırıcılığın sekiz temel unsurunu açmak gerekirse, menfaat devletlerin menfaatleri doğrultusunda hareket ettiğini ifade eder. Dolayısıyla devletler kendi menfaatlerini korumak için caydırıcılığı kullanmaktadırlar. Bunun için menfaatlerine zarar verecek devletlerin cezalandırılacağına dair bir deklarasyonda bulunurlar (Ermiş, 2015). Devletler bu deklarasyon doğrultusunda menfaatlerine saldırılması halinde onları korumak için defansif ve ofansif önlemler almalıdırlar (Goodman, 2010: 102-135; Ermiş, 2015). Burada defansif önlemler menfaatlere karşı yapılacak saldırının korunması içinken ofansif önlemler ise saldırıyı yapan aktöre bedel ödetmek içindir (Goodman, 2010: 102-135; Iasiello, 2014: 54-67; Iasiello, 2018: 35-52). İnanırlık konusuna gelindiğinde ise, caydırıcılığı asıl işlevsel kılan özellik devreye girmektedir. Burada dikkat edilmesi gereken nokta kapasite ile tehdit (deklarasyon) arasındaki tutarlılıktır. Menfaatlere zarar gelmesi halinde ise belirtilen kapasitenin kullanılacağına dair bir inanırlık söz konusudur. Diğer bir unsur olan güven verme, menfaatlere zarar verilmediği müddetçe rakip devlete zarar verilmeyeceğine dair oluşturulan güveni ifade eder. Korku, ödetilecek bedelden kaynaklanan korkuyu, kar- zarar hesabı ise rakip devletin rasyonel davranacağı düşüncesiyle kar- zarar hesabı yapacağıdır. Bu da caydırıcılıkta etkin rol oynamaktadır (Goodman, 2010: 102-135).

Yukarıda bahsedilenlerden hareketle, siber alanda caydırıcılığın sağlanabilmesi için beş önemli faktörün olduğunu söylemek mümkündür. İlk olarak devletler, siber çatışma esnasında caydırıcı mesajın oluşturulmasını, iletilmesini ve saldırgan veya saldırganlar tarafından anlaşılmasını sağlamalıdırlar. Devletler ofansif ve defansif kapasitelerinin etkinliğini korumalı ve karşı saldırı yapılmadan önce saldırganın kimliğini tespit etmelidir. Ayrıca devletlerin, ilk saldırı sonrasında karşı saldırı kapasitelerinin varlığının ve bunun devamının garanti altına almaları önemlidir. Son olarak güven verme siber caydırıcılığın sağlanmasında elzemdir. Güven vermenin yokluğu siber caydırıcılığın sağlayacağı ilişkiye zarar verebilir (Goodman, 2010: 102-135). Bu bağlamda saldırgan hedefinin karşılık verme kapasitesinin güvenilir olduğuna ikna olmazsa caydırıcılığın etkili olma ihtimali çok zordur.

Teknolojinin gelişmesi ve siber güvenlik kavramının ortaya çıkmasıyla sadece devletler değil, devlet dışı aktörler de siber caydırıcılığa önem vermişlerdir. Bu bağlamda devletlerin çoğu siber alanı "beşinci muharebe alanı" olarak tanımlamaktadır (Korhan, 2016: 147-161). Örneğin NATO 5. Maddesini siber alana taşımıştır. Yani müttefik devletlerden herhangi birine siber saldırı yapıldığında diğer NATO ülkeleri o devlete destek verecektir (van der Meer, 2016: 95). Diğer yandan devletler karşılaşılabilecek herhangi bir siber saldırıya karşı Acil Müdahale Ekipleri (CERTs) kurmuşlardır. ABD ve İngiltere bu alanda daha çok öne çıkan devletler olmak üzere Brezilya da 2009 yılında Bilgi ve İletişim Güvenliği Departmanı Altında Kritik Altyapı Koruması Bilgi Güvenliği Çalışma Grubu kurmuştur (Korhan, 2016: 147-161).

Siber alanda caydırıcılığın sağlanabilmesi için devletler ve devlet dışı aktörlerin birlikte çalışması gerekmektedir. Bu şekilde geliştirilecek bir siber caydırıcılık stratejisinin toplumsal, devlet ve uluslararası düzeyde iyi kaynaklara sahip olması gerekmektedir. Ayrıca siber caydırıcılığı arttıracak tedbirler ekonomik kıtlık ve kaynaklara ulaşmak için siyasi ve bürokratik rekabet ortamında yürütülecektir. Ayrıca caydırıcılık kavramının siber güvenliğin askeri olmayan yönlerini içerecek şekilde genişletilmesi de kavramı sulandırabilir (Bruton, 2018).

Uluslararası alanda bazı siber saldırılara bakmak gerekirse özellikle Goodman tarafından siber caydırıcılığın pratikte teoriden daha karmaşık bir olgu olduğunu vurgulanmış ve bazı siber saldırıları incelemiştir. İncelenen saldırılar 2007 Estonya saldırısı ve 2008 Gürcistan saldırısıdır. Estonya saldırısında, siber ataklara aslında oldukça etkili bir biçimde karşılık verilmesine rağmen caydırıcılık konusunda başarılı sayılmamaktadır. Diğer yandan 2008 Gürcistan savaşında Rusya tarafından yapılan siber saldırılar, siber caydırıcılığın birkaç sorununu daha ortaya çıkarmıştır. Bunlar, ölçülebilirlik ve zamansallık sorunlarıdır (Goodman, 2010: 102-135; Geers, 2011).

Estonya'nın siber saldırılara karşı verdiği tepki etkiliydi ve başlangıçta bazı bölümlerini uluslararası trafiğe kapatmıştı (Mansfield-Devine, 2012: 12-20). Saldırılar özellikle Estonya siber toplumunun kritik olan sektörlerini hedef almıştı. Bununla birlikte Estonya Bilgisayar Acil Müdahale ekibinin başarılarıyla saldırılar ciddi bir hasara yol açmamıştı. Ancak bu, Estonya'nın siber caydırıcılık konusunda başarı sağladığı anlamına gelmemektedir. Aynı şekilde 2008 Gürcistan savaşında Rusya'nın başlattığı siber saldırılarda hackerler hükümet sitelerini çökertmişti. Ancak bu durum hafif hasarlara yol açarak uzun vadeli bir bozulma yaratmamıştı. Ya da bir süre öyle sanılmıştı. Çünkü Ruslar gizli ve zamana

dayalı virüsleri hükümet sistemlerine bırakmış ve müdahale bittikten sonra Gürcü şebekelerinde tahribat yaratmışlardı (Goodman, 2010: 102-135; Geers, 2011).

Siber caydırıcılığı bir kavram ve strateji olarak sürdürmek ve caydırıcılık kuramını ve uygulamasını askeri ve stratejik alan dışındaki daha az ikili ve daha kapsamlı tehditler ve aktörler yelpazesine genişletmek için çeşitli başka zorlayıcı argümanlar vardır. Bunlardan ilki ve en belirgin olanı, siber güvenlik açıklarının toplum çapında olması ve kritik altyapıya, genellikle özel ellerde yapılan saldırıların, ani ve sonuç olarak ulusal güvenlik etkileri olabileceğidir. Bankacılık ve finans kuruluşlarına, enerji tesislerine, ulaşım altyapısına ve diğer hayati kamu hizmetlerine yönelik saldırıların caydırılması, askeri-stratejik hedeflere yönelik devlet kaynaklı saldırıların caydırılması kadar önemli hale gelmiştir (Moteff, 2010). Saldırıların hedefleri daha genişse, caydırıcılık stratejilerinin de olması mantıklıdır (Burton, 2018).

Devletler siber caydırıcılığı sağlamak için çeşitli çalışmalar, stratejiler üretmektedir (McKenzie, 2017). Bu noktada özellikle acil müdahale ekipleri dikkat çekerken, NATO gibi bir savunma örgütünün de kendi bünyesinde bu konuyla ilgilenmesi önem arz etmektedir. Literatürde birçok akademisyenin de bahsettiği gibi devletler siber caydırıcılığın sağlanması için kendi aralarında bir birlik kurmalıdırlar. Bu birlik siber alan ile ilgili bilgi alışverişi, kuralların ve kırmızı çizgilerin ne olacağının belirlenip bildirilmesi ve saldırılara karşı birlikte hareket etme gibi koordinasyonlar olabilir. Bu bağlamda devletlerin siber caydırıcılığı öğrenmeleri gerekir. Peki devletler siber caydırıcılığı öğrenebilir mi?

Çalışmada görüldüğü üzere devletler her geçen gün gelişen yeni tehditlere karşı yeni stratejiler geliştirme eğilimindedir. Nasıl ki devletler Soğuk Savaş döneminde gerekli olan caydırıcılık tedbirlerine adapte olmaya çalışmışsa teknoloji çağında da siber caydırıcılığın sağlanması için gerekli olan bilgiyi geliştirmek için çalışacaklardır. Dolayısıyla devletler şu an siber caydırıcılığı öğrenme aşamasındadırlar. Buna örnek olarak NATO'nun siber caydırıcılığa verdiği önemi ve acil müdahale ekiplerinin kurulması verilebilir.

Sonuç

Siber caydırıcılık, bilgi iletişim teknolojilerin gelişmesiyle ortaya çıkan bir dizi güvenlik sorununun ürünüdür. Devletler siber uzay kavramıyla ve burada güvenliğin nasıl sağlanacağına dair hala bir dizi çalışmalar yürütmektedirler. Bu çalışmada devletlerin siber alanda caydırıcılığı sağlamak için kendi aralarında bir konsensüs kurmaları gerektiği savunulmaktadır. Klasik caydırıcılığa nazaran daha karmaşık ve sonsuz bir alanı içeren siber alanın devletler tarafından iyi

öğrenilmesi de caydırıcılığın sağlanması açısından önemlidir. Literatürdeki birçok çalışma siber caydırıcılığın önündeki en büyük engelin anonimlik olduğunu savunmaktadır. Ancak burada sorun sadece anonimlik değil, siber alanı tanıma sorunudur. Devletler siber caydırıcılığı öğrenmek için siber alanı iyi tanımalıdırlar. Ancak bugünkü haliyle siber alanın iyi tanınması biraz zordur. Bununla birlikte teknoloji geliştikçe yeni yöntemler, yeni bilgilerin ortaya çıkışı ile siber saldırıları yapanların yeni yöntemlerle saldırılarına devam etmeleri bir sorundur. Devletler siber caydırıcılığı anlama ve öğrenme sürecinde bunu iyi bir şekilde hesaba katmalıdırlar. Devletler sadece askeri güvenlik alanlarında değil, toplumsal alanda da siber güvenliği sağlamakla yükümlüdürler. Bu yüzden siber caydırıcılığın öğrenilmesi devletler açısından hayati önem taşımaktadır.

Kaynakça

Brantly, A. F. (2018). The cyber deterrence problem. In *2018 10th International Conference on Cyber Conflict (CyCon)*, 31-54. https://doi.org/10.23919/CYCON.2018.8405009

Burton, J. (2018). Cyber deterrence: A comprehensive approach?. *NATO Cooperative Cyber Defence Centre of Excellence*. http://195.222.11.251/uploads/2018/10/BURTON_Cyber_Deterrence_paper_April2018.pdf

Davis, P. K. (2014). Deterrence, influence, cyber attack, and cyberwar. *NYUJ Int'l L. & Pol.*, *47*, 327.

Du Pisani, J. A. (2006). Sustainable development–historical roots of the concept. *Environmental sciences*, *3*(2), 83-96. https://doi.org/10.1080/15693430600688831

Ermiş, U. (2015). Siber caydırıcılık kavramının nükleer caydırıcılık olgusu ile karşılaştırmalı analizi (Doctoral dissertation, Bursa Uludag University).

Ermiş, U. (2015, Kasım, 2). Geleneksel caydırıcılığın siber alana uygulanabilirliği üzerine bir inceleme. Siber Bülten. https://siberbulten.com/makale-analiz/geleneksel-caydiricilik-kavramlarinin-siber- alanda-uygulanabilirligi-uzerine-bir-inceleme/

Geers, K. (2011). Strategic cyber security. Kenneth Geers.

Goodman, W. (2010). Cyber deterrence: Tougher in theory than in practice?. *Strategic Studies Quarterly*, *4*(3), 102-135.

Hoffman, W. (2019). Is Cyber Strategy Possible?. *The Washington Quarterly*, *42*(1), 131-152. https://doi.org/10.1080/0163660X.2019.1593665

Huang, K., Siegel, M., & Madnick, S. (2018). Systematically understanding the cyber attack business: A survey. *ACM Computing Surveys (CSUR)*, *51*(4), 1-36. https://doi.org/10.1145/3199674

Iasiello, E. (2014). Is cyber deterrence an illusory course of action?. *Journal of Strategic Security*, *7*(1), 54-67.

Iasiello, E. (2018). Is Cyber Deterrence an Illusory Course of Action?. *Air & Space Power Journal-Africa and Francophonie*, *9*(1), 35-52.

Jervis, R., & Stein, J. G. (1989). *Psychology and Deterrence*. Baltimore: Johns Hopkins University Press.

Korhan, S. (2016). Uluslararası İlişkilerde Siber Caydırıcılık. *Cyberpolitik Journal*, *1*(1), 147- 161.

Lupovici, A. (2016). The "Attribution Problem" and the social construction of "Violence": taking cyber deterrence literatüre a step forward. *International Studies Perspectives*, *17*(3), 322-342. https://doi.org/10.1111/insp.12082

Mansfield-Devine, S. (2012). Estonia: what doesn't kill you makes you stronger. *Network security*, *2012*(7), 12-20. https://doi.org/10.1016/S1353-4858(12)70065-X

McKenzie, T. M. (2017). *Is Cyber Deterrence Possible?*. Air University Press.

McNeilly, M. (2003). *Sun Tzu and the art of modern warfare*. Oxford University Press on Demand.

McNeilly, M., & McNeilly, M. R. (2012). *Sun Tzu and the art of business: Six strategic principles for managers*. OUP USA.

Meer, S. (2017). Deterrence of Cyber-Attacks in International Relations: Denial, Retaliation and Signaling. In *International Affairs Forum* (pp. 85-135). https://bit.ly/3wCzFhH

Mehmetcik, H. (2015). 21. Yüzyıl için caydırıcılık: teori ve pratikte neler değişti. *Güvenlik Stratejileri Dergisi*, 31-60.

Moteff, J. D. (2010). *Critical infrastructures: Background, policy, and implementation*. DIANE Publishing.

Schelling, T. C. (1958). The strategy of conflict. Prospectus for a reorientation of game theory. *Journal of Conflict Resolution*, *2*(3), 203-264. https://doi.org/10.1177/002200275800200301

Stevens, T. (2012). A cyberwar of ideas? Deterrence and norms in cyberspace. *Contemporary Security Policy*, *33*(1), 148-170. https://doi.org/10.1080/13523260.2012.659597

NATO. (2022, July, 06). Deterrence and defence. NATO.int. https://www.nato.int/cps/en/natohq/topics_133127.htm

Paulauskas, K. (2016, Ağustos, 05). Caydırıcılık Hakkında. NATO.int. https://www.nato.int/docu/review/tr/articles/2016/08/05/caydiricilik-hakkinda/index.html

Van der Meer, S. (2016). Defence, deterrence, and diplomacy: foreign policy instruments to increase future cybersecurıty. *Securing Cyberspace*, 95.

Protokol Dergisi

Çağrı Metni

Protokol dergisi, Karadeniz Teknik Üniversitesi Stratejik Araştırma Merkezi bünyesinde yayımlanmaktadır. Uluslararası İlişkiler, Sosyoloji, Ekonomi, Kent, Çevre ve Yönetim konuları başta olmak üzere sosyal bilimler alanına dair kısa makalelere yer veren dergi, Şubat ve Ağustos olmak üzere yılda iki kez yayımlanmaktadır.

Kısa makalelerin yanı sıra derginin her sayısında rapor, derleme, konferans notları, örnek olay, kitap tanıtımı vb. makale dışı yazılara da yer verilmektedir.

Dergi, öncelikli olarak ilgili alanlardaki güncel strateji temelli konulara dair tartışmaları okuyucu ile buluşturmayı hedeflemektedir.

Bu bağlamda hazırladığınız çalışmalarınızı bekliyoruz…

Genel yayım ilkeleri ve yazım kuralları için:

www.ktu.edu.tr/sam/protokol

Dergiye yazı göndermek için:

suna.ersavaskavanoz@ktu.edu.tr

KARADENİZ
TEKNİK ÜNİVERSİTESİ
Stratejik Araştırma Merkezi
SAM

KARADENİZ
TEKNİK ÜNİVERSİTESİ
Stratejik Araştırma Merkezi

SAM

PROTOKOL