TÜRKİYE'DE SİBER SALDIRILARA KARŞI CAYDIRICILIK

Mustafa ŞENOL
İstanbul Teknik Üniversitesi, Bilişim Enstitüsü Bilgi Güvenliği Mühendisliği ve Kriptografi Bölümü (Dr.),
Maslak 34469, İstanbul
senolm15@itu.edu.tr

ÖZET

Bu çalışmada, siber güvenliğin önemi, siber güç, siber saldırı, siber savaş ve siber caydırıcılık kavramlarıyla ilgili bilgiler verilmiş, siber saldırılara karşı caydırıcılık sağlayarak da karşı konulabileceği vurgulanmış, Türkiye'de bu güne kadar siber güvenlik strateji ve politikaları içerisinde siber caydırıcılık alanında yapılan çalışmaların neler olduğu konuları incelenmiştir. Bu kapsamda; siber caydırıcılığın, maliyet ve kullanım kolaylıkları yanında sağladığı üstünlükler nedeniyle üzerinde çalışılması, stratejiler geliştirilmesi ve gecikmeksizin uygulamaya konulması gereken çok önemli bir konu olduğuna dikkat çekilmiş ve bazı önerilerde bulunulmuştur.

Anahtar Kelimeler: Caydırıcılık, Siber Güç, Siber Caydırıcılık, Siber Saldırı, Siber Savaş, Siber Güvenlik.

DETERRENCE AGAINST CYBER ATTACKS IN TURKEY

ABSTRACT

In this study, information is given on the importance of cyber security, concepts of cyber power, cyber-attacks, cyber warfare and cyber deterrence while it is underlined that cyber-attacks can also be countered by providing deterrence. Additionally, actions carried out in the fields of cyber security strategies and politics in Turkey up until today were analysed. In this context, it is emphasized that due to the advantages it offers in addition to cost and ease of use, cyber deterrence is a crucial subject that must be studied, strategies and policies must be developed on and be implemented without delay.

Keywords: Deterrence, Cyber Power, Cyber Deterrence, Cyber Attacks, Cyber War, Cyber Security.

I. GİRİŞ (INTRODUCTION)

Teknolojinin, özellikle bilgisayar ve iletişim sistemlerinin hızla gelişmesi ve internetin de yaygınlaşmasıyla, bilişim sistemleri ve altyapılarının sağladığı kolaylıklar ve kazanımlar bilişim sistemlerini ve hizmetlerini hayatın vazgeçilmezleri yapmıştır. İnsanlık için tarihin başlangıcından bugüne en önemli varlık olan bilginin, elektronik ve bilişim sistemlerinin sağladığı imkânlarla, işlenmesinde, iletiminde, korunmasında ve kullanılmasında sağlanan etkinlik her geçen gün daha da artmış ve artmaya da devam etmektedir. Bu gelişmelere paralel olarak devletlerin özellikle ekonomik, politik ve askeri güçlerindeki kısa sürede meydana gelen olumlu yükselişler, kara, deniz, hava ve uzay ortamlarından sonra ortaya çıkan ve 5'inci Harekât Alanı olarak da adlandırılan Siber Ortamın önemini daha da artırmıştır.

Siber ortamın önemi artarken, bilgilere ve bilişim sistemlerine yönelik olarak başlayan kötü niyetli hareketler ve saldırılar günümüzde de artarak devam etmektedir. Teknoloji değerlendirmeleri ve geleceğe yönelik öngörüleriyle tanınan ABD'li yazar ve gelecek bilimci Alvin Toffler'ın "Teknolojik gücümüz artıyor ancak, yan etkileri ve olası tehlikeleri bundan çok daha hızlı büyüyor" [1] sözü bu durumu çok iyi açıklamaktadır.

Siber ortamda karşı tarafın bilgilerine ve bilgi sistemlerine yönelik zarar verme veya olumsuz etkileme istek ve ihtiyaçları 'Siber saldırı - Siber taarruz', bilgi ve bilişim sistemlerinin kötü niyetli hareketlere ve saldırılara karşı korunması ihtiyacı ise 'Siber güvenlik - Siber savunma' kavramlarını ortaya çıkarmıştır. Devletler siber savunma ve siber taarruz konularında strateji ve politikalar geliştirmeye ve bunları etkinlikle uygulamaya başlamışlar, bunlarla birlikte de 'siber savaş' kavramı ortaya çıkmıştır.

Siber savaşın başlatılması ve sürdürülmesi için gerekli olan, siber ortamda sahip olunan bilgi sistemleri ve alt yapıları ile bunların etkin olarak kullanılması yeteneği, 'Siber Güç' olarak tanımlanmaktadır [2]. Siber güç imkânları kullanılarak yapılan siber saldırıları ve siber saldırıların oluşturduğu savaşları önlemek, siber saldırıyı veya savaşı düşünenleri bu düşüncelerinden ve eylemlerinden vazgeçirmek, kısaca siber saldırganları caydırmak için siber güç imkânları tek başına kullanılabileceği gibi, yeterli olmadığında başka güçlerle birlikte kullanılmasına yönelik stratejiler geliştirilerek uygulanabilmektedir. Savaşlarda en mükemmeli hep kazanmak olmayabilir. M.Ö. 500'lü yıllarda yaşamış olan ünlü Çinli filozof ve savaş stratejisti Sun Tzu'nun dediği gibi "En iyisi savaşmadan baş eğdirmektir" [3]. Yani bir anlamda saldırganı isteğinden, saldırıdan veya savaştan caydırmak, söz konusu siber savaş olduğuna göre "Siber caydırıcılık" en iyisi olabilir.

Kişi, kurum, kuruluş, toplum veya devletlerin günümüzde en değerli varlıklarını oluşturan bilgi ve bilişim sistemleri ile altyapılarına yönelik kötü niyetli hareket ve tehlikeler olan tehditler ve saldırılar nelerdir? Bu saldırıların sonuçları veya oluşturabileceği hasar ve zararlar neler olabilir? Bunlara karşı korunmak için neler yapılmalı, hangi güvenlik veya savunma tedbirleri alınmalıdır? Saldırganları caydırarak kötü niyetli hareketlere ve saldırılara engel olmak, bu kapsamdaki risk ve tehditleri ortadan kaldırmak veya azaltmak mümkün olabilir mi? Bu kapsamda caydırıcılık nasıl sağlanabilir? Türkiye'nin resmi belgelerinde siber güvenlik ve caydırıcılık konusunda belirlenen ve uygulanması öngörülen tedbirler ve planlamalar ile yapılan çalışmalar nelerdir? Siber saldırılara karşı caydırıcılık sağlamak için nasıl bir strateji geliştirilerek uygulanmalıdır?

Bu çalışmada, yukarıda kısaca sıralanan soruların cevapları ortaya konulurken, siber saldırılara karşı siber güvenliğin öneminin vurgulanması ve caydırıcılık sağlayarak siber güvenliğin nasıl sağlanabileceği konusunun açıklanması, bu konuda dikkate alınmasının uygun olacağı düşünülen esas ve prensiplerin ortaya konulması hedeflenmiştir. Yöntem olarak; 2'nci bölümde 'Siber saldırılar ve güvenlik', 3'ncü bölümde 'Caydırıcılık ve siber caydırıcılık', 4'üncü bölümde 'Resmi belgelerde siber güvenlik ve caydırıcılık", 5'inci bölümde 'Siber saldırılara karşı caydırıcılık stratejisi' konularında araştırmalar sonucu derlenen bilgiler verilmeye çalışılmış ve 6'ncı ve son bölümde konuyla ilgili ulaşılan "Sonuç ve değerlendirmeler" sunulmuştur.

II. SİBER SALDIRILAR VE GÜVENLİK (CYBER ATTACKS AND SECURITY)

A. Siber saldırılar (Cyber attacks)

Kazanç sağlamak veya zarar vermek maksatlarıyla siber ortamda belirlenecek hedef ya da hedeflere yönelik gerçekleştirilecek faaliyetler siber saldırıları oluşturmaktadır. ABD Ulusal Araştırma Konseyi tarafından, 2009 yılında yapılan bir çalışmada siber saldırılar; "Bilgisayar sistemleri, ağlar veya bilgiyi ve/veya bunlarda yerleşik olan ya da bunları taşıyan programları bozmak, aldatmak, küçük düşürmek veya yok etmek için yapılan kasıtlı hareketler" [4] olarak tanımlanmıştır.

Saldırganlar siber saldırılarla, siber ortamdaki fiziksel veya sanal yapıyı, yazılım, donanım ve alt yapı sistemlerini, genellikle de bu sistemler üzerindeki bilgiyi ve kullanıcıları hedef alarak eylemlerini gerçekleştirirken, temel olarak üç prensibe göre hareket etmektedirler. Bunlar, gizli bilgilerin elde edilmesi veya bilginin gizliliğinin açık edilmesi, bilgiye zarar verilerek değiştirilmesi yani bütünlüğünün bozulması ve bilgiye kullanıcıların erişiminin engellenmesi yani kullanılabilirliğinin önlenmesidir. Türkiye 2016-2019 Siber Güvenlik Stratejisi ve Eylem Planı belgesinde, bu üç prensipten hareketle siber saldırıların tanımı; "Ulusal siber uzayda bulunan bilişim sistemlerinin gizlilik, bütünlük veya erişilebilirliğini ortadan kaldırmak amacıyla, siber uzayın her hangi bir yerindeki kişi ve/veya bilişim sistemleri tarafından kasıtlı olarak yapılan işlemler" [5] şeklinde yapılmıştır.

Bilgisayar ve iletişim teknolojilerinde ve özellikle 1990'lar sonrası internette yaşanan hızlı gelişmeler siber gücün etkisini daha da artırmış, siber gücün sağladığı imkânlar hayatı kolaylaştırmanın yanında, aynı zamanda siber saldırılarla sonuç almaya çalışan birer tehdit ve yaptırım aracı olarak da kullanılmaya başlanmıştır.

Çeşitli niyet ve maksatlarla gerçekleştirilen çok çeşitli tip ve büyüklükteki siber saldırılarla siber savaşların başlayıp devam ettiği dünyada, internet medyası ile yazılı ve görsel basın gibi açık kaynaklara da yansıyan ve siber gücün etkisini de ortaya koyan önemli siber olaylar ve siber saldırıların bazıları aşağıda sunulmuştur [6].

- 2000'de Avustralya'da arıtma tesisi bilgi sistemlerine saldırı ve kanalizasyon sularının şehre bırakılması,
- 2003'te ABD'nin 8 eyaletinde 2 gün süren, ölümlere ve 6 milyar dolar zarara yol açan elektrik kesintisi,
- 2007'de Rus bilgisayar korsanlarının Estonya bilgi sistemlerine saldırısı ve ülke çapında faaliyetlerini durma noktasına getirmesi,
- 2007'de İsrail savaş uçaklarının Suriye topraklarına girmesi ve nükleer tesisini imha ederek zayiatsız dönmesi, bu sırada Suriye hava savunmasının hiçbir hedef görememesi,
- 2008'de Rusya-Gürcistan savaşında Gürcistan'a yapılan siber saldırılar sonucu finans, haberleşme ve elektrik sistemlerinde ciddi sıkıntılar yaşanması,

- 2010'da İran nükleer zenginleştirme programını hedefleyen ve ciddi sorunlara sebep olan 'Stuxnet' yazılımı saldırısı,
- 2010'da WikiLeaks'in yayınladığı belgeler ile diplomaside sanal bomba etkisi yaratması,
- 2011'de İran Silahlı Kuvvetlerinin ABD'ye ait insansız hava aracının kontrolünü ele geçirerek yere indirmesi,
- 2014'te Sony Şirketinin yoğun siber saldırılar sonucu Kuzey Kore Lideriyle ilgili 44 milyon dolara mal olan filmi gösterimden kaldırması.
- 2016'da ABD'nin doğu yakasına hizmet sunan sistem altyapılarına yönelik olarak başlayan siber saldırıların ülke geneline yayılarak internet bağlantısını engellemesi ve ciddi ekonomik zarara sebep olması.

Dünyada yaşanan bu siber olaylara benzer şekilde, Türkiye'de yaşanmış önemli siber saldırı ve olayların bazıları da aşağıda sıralanmıştır [6].

- 2008'de Bakü-Tiflis-Ceyhan boru hattına siber saldırı sonrası patlama meydana gelmesi,
- 2009'da zararlı bir yazılımın Atatürk Havalimanı bilgisayarlarını etkilemesi,
- 2011'de saldırılar sonrasında Telekomünikasyon İletişim Başkanlığı'nın sitesinin devre dışı kalması,
- 2015'te elektriğini İran'dan alan Van ve Hakkâri hariç 79 ili etkileyen elektrik kesintisi,
- 2015'te, 10 gün süreli saldırılar sonucu birçok banka, noter ve devlet kurumunun internet sitesine ve mobil uygulamalara erişim sağlanamaması,
- 2016'da Sağlık Bakanlığı hastanelerine yönelik siber saldırılar ile veri tabanındaki bilgilerin çalınması ve silinmesi.

Henüz farkına varılmayan veya gizlilik, saygınlık kaybı vb nedenlerle açıklanmayan ve açık kaynaklara yansımayanlarla birlikte, yaşanan binlerce önemli siber olay ve saldırının arasından sadece bunlara bakılarak, siber gücün sağladığı imkânlarla çeşitli teknik, taktik ve stratejilerin kullanılmasıyla gerçekleştirilecek siber saldırılarla ülke güvenliği için çok büyük tehlikeler, hasar ve zararlar yaratabileceği sonucuna kolaylıkla ulaşılabilir.

B. Siber güvenlik (Cyber security)

Hassas ve değerli varlıklara gelecek herhangi bir kötülüğe, hasar veya zarara karşı korunma veya karşı koyma derecesi anlamında kullanılan 'Güvenlik' kavramı; TDK sözlüğünde "Toplum yaşamında yasal düzenin aksamadan yürütülmesi, kişilerin korkusuzca yaşayabilmesi durumu, emniyet" [7] şeklinde açıklanmaktadır.

Saldırılarda hedefin merkezinde bilginin olması nedeniyle, başlangıçta 'Bilgi Güvenliği' olarak kullanılan kavramın siber güvenliği de kapsadığına dair yaklaşımların olmasına karşın, günümüzde siber ortamın hızlı değişimi dolayısıyla yaşanan olayların da etkisiyle bunun tersinin yaygınlaştığı, siber güvenliğin bilgi güvenliğini de içerir şekilde kullanılmaya başlandığı görülmektedir. Bu durum, "Konuyla ilgili farklı terimlerin ve tanımların ortak temalarından hareketle, siber güvenliğin devlet sırlarının korunması ve ulusal savunmanın sağlaması için temel esas olduğu…" [8] şeklinde NATO Siber Güvenlik Çerçeve Kılavuzunda da açıkça vurgulanmıştır.

Türkiye Siber Güvenlik Stratejisi Belgesinde ise siber güvenliğin; "Siber uzayı oluşturan bilişim sistemlerinin saldırılardan korunmasını, bu ortamda işlenen bilgi/verinin gizlilik, bütünlük ve erişilebilirliğinin güvence altına alınmasını, saldırıların ve siber güvenlik olaylarının tespit edilmesini, bu tespitlere karşı tepki mekanizmalarının devreye alınmasını ve sonrasında ise sistemlerin yaşanan siber güvenlik olayı öncesi durumlarına geri döndürülmesini" [5] ifade ettiği belirtilmiştir.

Strateji belgesindeki bu tanımlamada görüldüğü üzere, temel amaç bilgiyi korumak ve sistemlerin devamlılığını sağlamaktır. Bilgiyi, bilişim sistemlerini ve kullanıcılarını hedef alarak gerçekleştirilen siber saldırılarda kullanılan üç prensip (bilginin gizliliğinin, bütünlüğünün ve erişilebilirliğinin korunması) siber güvenliğin de temelini teşkil etmektedir. Siber saldırı ve olayların tespit edilerek engel olunması ve bilişim sistemlerinin saldırı/olay öncesi duruma döndürülmesi de, siber güvenliğin amaç ve hedefleri arasında yer almaktadır.

Siber ortamın tehlikelerinin farkında olan ülkeler siber güvenliği önemsemekte, siber tehditleri ulusal güvenliğe karşı en önemli tehdit unsurlarından biri olarak kabul etmekte ve başta ülkenin elektronik haberleşme, enerji, su yönetimi, kritik kamu hizmetleri, ulaştırma, bankacılık ve finans sektörleri vb kritik altyapıları olmak üzere bireylerinin, kurum ve kuruluşlarının varlıklarını siber risklere, tehditlere ve saldırılara karşı korumak için çözümler üreterek uygulamaya koymaktadırlar. Bu konuda gerekli adımları atmayan ülkeler ise geç kalmış demektir. Çünkü başlangıçta küçük çapta ve bir kısmı zararsız denebilecek seviyedeki riskler, tehditler ve saldırılar, teknolojinin gelişmesi ve internetin yaygınlaşmasıyla birlikte büyüyerek siber savaş halini almıştır.

ABD eski Savunma Bakanı Leon Panetta, 2012 yılında yaptığı konuşmasında, "ABD'nin Siber-Pearl Harbor ihtimali ile karşı karşıya olduğu" [9] sözüyle, benzer hususları belirtmiş ve siber savaşın ulusal güvenlik için büyük bir tehdit olduğunu vurgulamıştır. Bilgisayar ve iletişim sistemlerinde, insanların internetinden nesnelerin internetine, akıllı cihazlardan akıllı evlere/şehirlere, siber uzayda sınır tanımayan ve insanın hayalinde canlandırma sınırlarını zorlayan gelişmeler yaşanmaktadır.

İşte böyle bir ortamda, siber saldırı risk ve tehditleri gerçeği ve tehlike boyutu ortadayken, çoğu ülke siber savaşın hem taarruz ve hem de savunma boyutu ile ilgili yasa, politika ve stratejiler üreterek uygulamaya

koyarken, siber savaşı küçümseyip bu konuda ciddi çalışmalar içerisinde olmayan ülkeleri çok zor bir gelecek beklemektedir. Çünkü siber savaş gerçektir ve saldırganlar şimdiye kadar gerçek yeteneklerini ortaya çıkmaması için en gelişmiş siber silahlarını yani bu konudaki gerçek yeteneklerini kullanmamışlardır. Tam ölçekli bir siber savaşın yani gerçek yeteneklerin kullanıldığı saldırıların yapıldığı bir savaşın sonuçlarının tahmin edilemeyeceği ve olabileceklerin modern bir ülkeyi mahvedebileceği [10] yorumları yapılmaktadır.

Bu kapsamda, bilgisayar ve iletişim teknolojilerinin sağladığı imkânlardan ve kolaylıklardan etkinlikle yararlanabilmek için bilgi ve iletişim sistemleri ile altyapılarının; her geçen gün artarak ve çeşitlenerek devam eden siber suçlara, siber saldırılara, hasar ve yıkım miktarı korkutucu seviyelere ulaşan veya belirsiz olan siber savaşa karşı korunmasının, yani siber güvenliğin sağlanmasının yolları aranmakta ve bu konuda stratejiler geliştirilmektedir.

Siber savaş stratejileri geliştirilirken dikkate alınması gereken en önemli hususların başında caydırıcılık gelmekle birlikte, sır gibi saklanmaları nedeniyle siber silahların caydırıcılık sağlanmasında etkilerinin olmadığı iddia edilmektedir [10]. Ancak, ayrı ve geniş kapsamlı bir konu olması nedeniyle bu çalışmada değinilmeyen, konuyla ilgili önde gelen ülkelerin siber güvenlik ve savaşla ilgili stratejileri incelendiğinde, genel olarak caydırıcılık sağlanması açıkça ifade edilmese de, siber caydırıcılık sağlanmasına katkı sağlayan esas ve prensiplerin sıkça yer aldığı görülmektedir. Bu esas ve prensiplerin başında ise; güçlü siber savunmayı sağlayacak teşkilat ve güçlü yapılanmaların oluşturulması, askeri kabiliyetleri bütünleyecek siber kabiliyetlerin geliştirilmesi, siber suçlarla mücadele ve bu kapsamda caydırıcı yasaların çıkarılması vb önemli konular gelmektedir [11].

III. CAYDIRICILIK VE SİBER CAYDIRICILIK (DETERRENCE AND CYBER DETERRENCE)

A. Caydırıcılık (Deterrence)

Türkçede genellikle "korkutarak cesaret kırmak ve vazgeçirmek" anlamlarında kullanılan 'caydırmak' sözcüğünden türetilen 'Caydırıcılık' kavramı, TDK Sözlüğünde "Bir saldırganlığı önlemek ve engellemek için önlem alma işi" [7] olarak açıklanmaktadır.

'Caydırıcılık'; hukuksal alanda "ceza veya hapis korkusuyla suç işlemekten alıkoyma" [12], uluslararası ilişkilerde yani diplomasi alanında "karşıdaki devleti emellerinden vazgeçirme davranışı veya belirli davranışlara yönlendirme" [13], askeri alanda ise "düşmanı çok yüksek bedel ödeyeceğine inandırarak bir hareketten vazgeçirmek için askeri güç, yaptırım ve tehditlerin kullanımı" [14] olarak tanımlanmaktadır.

Geçmişe ve günümüze bakarak, hukuk alanında bireylerin çeşitli cezalar ile suç işlemelerinin önlenmesine, diplomasi alanında devletlerin çeşitli yaptırımlarla ilişkilerinin yönlendirilmesine ve askeri alanda savaşmadan karşı tarafın farklı davranmasının sağlanmasına, yani bu alanlarda caydırıcılık uygulamasına yönelik, pek çok örnek sıralanabilir. Adli olaylarda para ya da mahkûmiyet cezaları, uluslararası ortamda devletlere çeşitli yaptırımların uygulanması, klasik savaşta güçlü ordularla karşı tarafa güç gösterisi, tatbikatlar vb.

Caydırıcılığın yaygın olarak kullanılan genel tanımı ise, bir düşmanın, belirli bir eylemi gerçekleştirmek için maliyet/fayda hesaplamasına yönelik tahmini üzerinde yönlendirilmesidir [15]. Diğer bir ifadeyle, potansiyel faydaları azaltarak ya da olası masrafları arttırarak (ya da her ikisini de birden), düşmanı eylemi yapmaktan kaçınmaya ikna etmektir. Bu maksatla varlık ve çıkarların korunması için gerekli bütün olanak ve yeteneklerin kullanılacağına yönelik niyet ve kararlılık gösterilir. Caydırıcılığın sağlanması için 'Saldırganın eylemini boşa çıkarma' ve 'Cezalandırma (misilleme tehdidi)' yoluyla saldırıdan vazgeçirilmesine dayanan iki yöntem uygulanır.

Bu yöntemlerden özellikle soğuk savaş döneminde ön planda kullanılan ve nükleer caydırıcılığın esasını teşkil eden cezalandırma yoluyla caydırıcılığın başarıyla sağlanması için üç temel koşul bulunmaktadır [16]. Bunlar caydırıcının yetenekleri, misilleme tehdidinin güvenilirliği ve tehdidin saldırgana iletilmesidir. Nükleer caydırıcılıkta başarıyı olumlu yönde etkileyen bu temel koşullar, siber caydırıcılığın sağlanmasında da dikkate alınmalıdır.

B. Siber caydırıcılık (Cyber Deterrence)

Caydırıcılık ile ilgili yukarıdaki açıklamalardan hareketle 'Siber caydırıcılık' nasıl tanımlanabilir?

Sun Tzu'nun "En iyisi savaşmadan baş eğdirmektir" [3] özdeyişinden de hareketle siber caydırıcılık; 'siber ortamda bilişim sistem ve altyapılarına saldırı başlatacak saldırganı saldırıdan vazgeçirmektir' şeklinde de tanımlanabilir.

Caydırıcılığı genel anlamda "karşı tarafa düşmanca eylemleri yapmama konusunda gözdağı verme" şeklinde açıklayan ABD'li siber savaş araştırmalarıyla ünlü bilim adamı Martin C. Libicki siber caydırıcılığı, siber ortamda saldırganın eylemini boşa çıkarma veya cezalandırma (misilleme tehdidi) yoluyla saldırıdan vaz geçirme olarak tanımlamaktadır. Bu kapsamda misillemenin etkisini de, nükleer ve konvansiyonel caydırıcılıktan sonra, diplomatik ve ekonomik yaptırımlarla sağlanan caydırıcılıktan ise önce geldiğinin kabul edilebileceğini belirtmektedir [17],

ABD eski Genelkurmay Başkan Yardımcılarından olan Orgeneral James Cartwright siber caydırıcılığı; "Siber ortamda başkalarının bize yapmak istediklerinin aynısını onlara yapma yeteneği" [17] olarak tanımlamıştır. Bu tanımlamanın nükleer veya

konvansiyonel caydırıcılık için karşılık bulduğu kabul edilmekle birlikte, siber gücün ve kullanılmasının özellikleri dolayısıyla, siber caydırıcılık için yeterli olup olmayacağı tartışılmaktadır.

Siber saldırılara ve savaşa karşı caydırıcılık stratejisini analiz eden çalışmaların çoğu soğuk savaş teorilerine dayanmaktadır. Bu kapsamda başarılı bir caydırıcılık için yerine getirilmesi gereken tarafların yetenekleri, misilleme tehdidinin güvenilirliği ve tehdidin saldırgana iletilmesi koşullarının, siber saldırıların yarattığı tehditlere uygulandığında başarısız olunmasının beklendiği iddia edilmektedir [16].

İstihbarat yetenekleri bu sorunun çözümünü kolaylaştırsa da, genelde saldırıya karşılık verileceği zaman daha geniş bir potansiyel tehdidi kapsayacak şekilde değerlendirilmelidir. Soğuk savaş döneminde her iki tarafın da yetenekleri açıkça bilinirken, bilgi çağında olası saldırganların sayısının artması ve güçlerinin de belirsizliği, caydırıcılık mesajının kime ve nasıl ileteceğinin zorlukları istikrarlı ve inanılır caydırıcılık sunma olasılığını düşürmüştür.

Siber saldırılara karşı caydırıcılığın zorlukları nedeniyle; nükleer savaşı önlemenin olmazsa olmazı olan caydırıcılık kuramının, günümüzde siber savaşı durdurmakta önemli bir rol oynayamadığı ve ABD'nin nükleer ve konvansiyonel anlamda sağladığı caydırıcılığı, tüm çabasına rağmen siber alanda sağlayamayacağı ileri sürülmektedir [10]. Bu tez, 2011 yılında ABD Savunma Bakanlığınca hazırlanan raporlardan sızan bilgilerden, 'siber saldırıların savaş sebebi sayılacağının ve askeri operasyonlarla karşılık verilebileceğinin açıklanması' [18] ile desteklenmektedir.

Libicki'ye göre ise, siber caydırıcılık işe yarayabilir. Ancak bunun için, siber caydırıcılığı nükleer ve klasik askeri caydırıcılıktan ayıran, siber caydırıcılığın aleyhinde olan ve problemli yanlarını ortaya koyan üçü asıl, altısı yardımcı olmak üzere dokuz soruyu cevaplamak gerekmektedir [17].

Asıl sorular:

- Kimin yaptığı biliniyor mu?
- Onların değerli varlıkları risk altında tutulabilir mi?
- Aynı şey art arda tekrarlanabilir mi?

Yardımcı sorular:

- Eğer misilleme caydırıcılığı sağlamazsa, en azından silahsızlandırmayı sağlayabilir mi?
- Üçüncü gruplar mücadeleye katılır mı?
- Misilleme kendi tarafımıza doğru mesajı verir mi?
- Saldırıya karşılık vermek için bir eşik var mıdır?
- Tırmanmadan kaçınılabilir mi?
- Saldırgan tarafa vurmaya değmediği durumda ne olur?

Nükleer caydırıcılıkta cevaplanması kolay olan bu soruların, siber caydırıcılık söz konusu olduğunda cevaplanması zorlaşmakta ve bazen de imkânsızlaştığı görülmektedir. Ancak siber ortamda siber güç kullanılarak caydırıcılık sağlanması düşünülüyorsa bu soruların cevaplanması ve bu cevaplar doğrultusunda planlamaların yapılması ve eyleme dönüştürülmesi gerekmektedir.

IV. RESMİ BELGELERDE SİBER GÜVENLİK VE CAYDIRICILIK (CYBER SECURITY AND DETERRENCE IN OFFICIAL DOCUMENTS)

Türkiye'de siber güvenlikle ilgili faaliyet ve çalışmalar 17 Şubat 2003 tarihinde yayımlanan '2003/10 Sayılı Başbakanlık Genelgesi' ile başlamıştır. Söz konusu genelgede, Güvenlik Kültürünü oluşturmayı amaçlayan ve OECD üyesi ülkelerin ortak tutumunu yansıtan rehber ilkelerin bilgi sistem ve ağlarına yönelik tehditler karşısında, her düzeydeki kullanıcılar tarafından benimsenip uygulanmasının yararlı olacağı belirtilerek, öncelikle ve başta kamu kurum ve kuruluşları olmak üzere, bilgi sistem ve ağlarının korunması için yürütülen çalışmalarda göz önünde bulundurulması istenmiştir.

Bu genelgeyi, Devlet Planlama Teşkilatı tarafından 'E-Dönüşüm Türkiye Projesi (2003)', Kalkınma Bakanlığı koordinasyonunda 'Bilgi Toplumu Stratejisi ve Eylem Planı (2006)', TÜBİTAK koordinasyonunda hazırlanan 'Ulusal Sanal Ortam Güvenlik Politikası (2009)' takip etmiştir. Bu çalışmaların içeriğinde, siber güvenlikle ilgili tespitler ve yol haritaları ortaya konmakla birlikte siber caydırıcılıkla ilgili dikkat çekici hususların bulunmadığı görülmektedir.

Daha sonra, 27 Ekim 2010 tarihli MGK Bildirisinde; "Siber tehdidin küresel düzeyde ulaştığı boyut ve bu tehdidin ulusal güvenliğe etkileri kapsamlı surette ele alınmıştır. Bu bağlamda, siber tehdidin engellenebilmesi için milli düzeyde yürütülen çalışmalar değerlendirilmiştir. Siber tehditlere karşı önlem almaya yönelik kararlılık ve irade ortaya konmuştur" [19] ifadeleri yer almıştır. Ülkenin en üst ulusal güvenlik kurulunun bildirisinde yer alan bu ifadeler, siber tehditlere karşı önlem alınmasına yönelik kararlılık ve iradenin ortaya konduğunun vurgulanması ve bunun duyurulması, caydırıcılık açısından önemlidir.

Bilgi toplumu politika, hedef ve stratejileri çerçevesinde, 26 Eylül 2011'de '655 Sayılı KHK' ile Ulaştırma Denizcilik ve Haberleşme Bakanlığı (UDHB)'nın teşkilat ve görevleri yeniden düzenlenmiş, 'Siber güvenlik faaliyetleri ve hizmetlerine ilişkin kamu kurum ve kuruluşlarıyla gerekli işbirliği ve koordinasyonun sağlanmasına ilişkin usul ve esasları belirlemek ve gerekli düzenlemelerin yapılması' görevi UDHB'ye verilmiştir [20]. Siber güvenlikten sorumlu bir makamın belirlenmesinin, bu konularda eksikliklerin

giderileceğine yönelik umut vermesi açısından caydırıcılık özelliği taşıdığı söylenebilir. Müteakiben siber güvenlik konusunda çalıştay ve tatbikatların yapılması, kamu kurumlarında yapılanmaya gidilmesi ve 2012 yılında siber güvenlik yol haritasının ortaya konması bu tespiti destekler niteliktedir.

Bakanlar Kurulunun 'Ulusal Siber Güvenlik Çalışmalarının Yürütülmesi, Yönetilmesi ve Koordinasyonuna İlişkin' 20 Ekim 2012 tarihli kararı ile UDHB başkanlığında 'Siber Güvenlik Koordinasyon Kurulu' kurulmuş, siber güvenliğe yönelik ilkeler, teşkilat, görev ve sorumluluklar resmi olarak belirlenmiştir. Siber güvenliğe yönelik en önemli stratejik adımlardan birisi olan bu adımla ilgili bakanlık ve kamu kurumlarının üst düzey yöneticilerinden 12 kişilik Siber Güvenlik Kurulu oluşturulmuştur. Siber Güvenlik Kurulu tarafından 'Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı' [21] kabul edilerek yayımlanmıştır.

Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planının amacı;

- Kamu kurum ve kuruluşlarınca bilgi teknolojileri üzerinden sağlanan her türlü hizmet, işlem ve veri ile bunların sunumunda kullanılan sistemlerin güvenliğinin sağlanmasına,
- Kamu ya da özel sektör tarafından işletilen kritik altyapılara ait bilişim sistemlerinin güvenliğinin sağlanmasına,
- Siber güvenlik olaylarının etkilerinin en düşük düzeyde kalmasına, olayların ardından sistemlerin en kısa sürede normal çalışmalarına dönmesine yönelik stratejik siber güvenlik eylemlerinin belirlenmesine ve oluşan suçun adli makam ve kollukça daha etkin araştırılmasının ve soruşturulmasının sağlanmasına yönelik bir altyapı oluşturmaktır.

Plan içeriğinde ve eylemlerde siber caydırıcılık açıkça yer almamakla birlikte, eylemlerden güdülen niyet ve maksatlarla ulaşılması öngörülen hedeflerin kısmen de olsa siber caydırıcılık sağlama sonucuna götürebileceği açıktır.

- Siber güvenlik konusunda yasal düzenlemelerin yapılması ve adli süreçlere yardımcı olacak çalışmaların yürütülmesi siber saldırganların siber ortamda işledikleri suçlar nedeniyle cezalandırılacak olmaları,
- Ulusal Siber Olaylara Müdahale Merkezi (USOM)'nin oluşturulması ile Siber Olaylara Müdahale Ekipleri (SOME)'nin faaliyete başlaması, siber olayların tespitini, duyurulmasını, gerekli tedbirlerin alınarak saldırganlarla ilgili gerekli yasal işlemlerin de kısa sürede başlatılmasın sağlanabilecek olması,
- Ulusal siber güvenlik altyapısının güçlendirilmesinin siber saldırıların başarılı olmasını zorlaştırması ve daha masraflı hale getirmesi,
- Siber güvenlik alanında insan kaynağının yetiştirilmesi ile başta kullanıcıları siber güvenlik farkındalığının artırılmasıyla güvenlikte ihmallerin ve yanlışların azalması, bu konuda strateji ve politikaların geliştirilmesi,
- Siber güvenlikte yerli teknolojilerin geliştirilmesi ile daha güvenli donanım ve yazılımların kullanılmaya başlanması,
- Ulusal güvenlik mekanizmalarının kapsamının genişletilmesi ile koordinasyon ve işbirliğin artırılması siber caydırıcılık sağlanmasında temel yapı taşlarını oluşturan çok önemli eylem ve faaliyetlerdir.

Ülkemizin 2015-2018 döneminde takip edeceği ve Kalkınma Bakanlığının koordinasyonunda hayata geçirilecek olan 6 Mart 2015 tarihli 'Bilgi Toplumu Stratejisi ve Eylem Planı' [22] bilişim teknolojileri alt yapılarının geliştirilmesi, kullanıcıların eğitimlerinin artırılması, sektörlerin desteklenmesi vb nedenlerle siber caydırıcılığa önemli katkılar sağlayacaktır.

Türkiye '2016 - 2019 Ulusal Siber Güvelik Strateji ve Eylem Planı' 09 Eylül 2016'da açıklanmıştır. Türkiye'nin siber güvenlik konusunda izleyeceği yolu belirleyen Strateji ve Eylem Planında, siber güvenliğin, ulusal güvenliğin ayrılmaz bir parçası olduğu anlayışının tüm kesimlerde yerleşmesi, ulusal siber uzayda bulunan sistem ve paydaşların tamamının güvenliğini sağlamak üzere idari ve teknolojik önlemlerin alınmasını sağlayacak yetkinliğin eksiksiz bir şekilde kazanılması amacıyla, 5 ana eylem ve 41 alt eylemin gerçekleştirilmesi öngörülmektedir. Dört yıllık siber güvenlik yol haritasını oluşturan ana eylem maddeleri aşağıda sunulmuştur [5].

- Siber Savunmanın Güçlendirilmesi ve Kritik Altyapıların Korunması,
- Siber Suçlarla Mücadele,
- Farkındalık ve İnsan Kaynağı Geliştirme,
- Siber Güvenlik Ekosisteminin Geliştirilmesi,
- Siber Güvenliğin Milli Güvenliğe Entegrasyonu.

Bu strateji ve eylem planının ana metin ve ana eylem maddelerinde siber caydırıcılık konusunda açık ifadeler bulunmamakla birlikte, ana eylem maddelerinde planlanmakta olduğu belirtilen hususların doğru planlanarak zamanında da uygulamaya konulmasının siber caydırıcılık konusunda ciddi ilerlemeler sağlayabileceği ortadadır. Caydırıcılık konusundaki bu öngörü ve beklentinin 'Siber suçlarla mücadele' eyleminin alt maddelerinde siber saldırganların tespiti ve suçlarının kanıtlanması sağlanarak caydırıcılık sağlanmasının hedeflenen kazanımlar arasında yer aldığının vurgulandığı görülmektedir.

V. SİBER SALDIRILARA KARŞI CAYDIRICILIK STRATEJİSİ (CYBER STRATEGY AGAINST CYBER ATTACKS)

Türkiye'de siber güvenlik strateji ve politikalarıyla ilgili bu güne kadar hazırlanan ve uygulamaya konulan belgeler incelendiğinde siber caydırıcılık

konusuna, siber suçlarla yasal olarak mücadele edilerek caydırıcılık sağlanması konusu hariç, yer verilmediği görülmektedir. Siber güvenliğin sağlanarak saldırıların engellenmesi ve saldırıların boşa çıkarılması açısından bakıldığında dolaylı olarak kısmen caydırıcılık sağlanabilecek olsa da, yeterli olmadıkları düşünülmektedir. Yapılması gereken siber caydırıcılık stratejisinin, siber güvenlik stratejisi ile birlikte ele alınarak açık ve ayrıntılı olarak oluşturulmasıdır.

Siber saldırılara karşı başarılı olacak ve siber güvenliğin artırılmasına da katkı sağlayacak caydırıcılık stratejisinin temel bileşenleri neler olmalıdır? Bu bileşenlerin, başarılı bir caydırıcılık için asgari koşulları karşılamasının ve Libicki tarafından ortaya konulan (III'üncü bölümde değinilen) dokuz soruya cevap verecek şekilde belirlenmesinin uygun olacağı düşünülmektedir. Bu tespit çerçevesinde başarılı bir siber caydırıcılık stratejisinin temel unsurları aşağıda sunularak kısaca açıklanmaya çalışılmıştır.

- Ülkenin öncelikle kritik altyapılarını koruyan etkin bir siber savunma:

Siber saldırılara karşı korunmak için her türlü saldırıya karşı koymada temel esas olan değerli varlıkların savunmasının güçlendirilmesi, saldırıyı boşa çıkartmak veya etkisini azaltarak karşı saldırıyı başlatmak için en öncelikli kural olmalıdır. Bu maksatla karşı tarafın saldırı yeteneklerini dikkate alarak ülkenin öncelikle kritik altyapıları olmak üzere bilgi ve bilişim sistemlerinin güvenliğinin sağlanması maliyeti yüksek olmakla birlikte caydırıcılık da sağlayacaktır. Çünkü bu durumda saldırgan tarafın saldırıları zorlaşacak ve maliyetleri de artacaktır.

- Siber saldırı yapması olası hedeflere yönelik etkin siber istihbarat:

Siber ortamda siber tehditlerin ortaya konması ve gelecekte saldırıları yapması mümkün görülen hedeflerin belirlenerek bunların yeteneklerinin öğrenilmesi siber savunma tedbirlerinin alınması yanında saldırı durumunda saldırganın kimliğinin tespiti, caydırıcılık tehdidinin duyurulması, başarılı misillemenin yapılarak hedeflenen sonuca ulaşılması vb pek çok eylem için çok önemli bir unsurdur.

- Olası siber saldırılara karşı etkin misilleme sağlayacak siber taarruz yeteneği:

Gerekli savunma tedbirlerinin alınmış olduğu bir siber ortamda, mutlak güvenlik mümkün olmadığı için savunmanın mutlaka aşılabileceği düşünülmeli ve karşı saldırılarla misilleme yapılması mutlaka planlanmalıdır. Bunun için da siber saldırı/taarruz yetenekleri olası hedeflerin durumları da dikkate alınarak kazanılmalı ve kullanılmaya hazır olunmalıdır. Bu kapsamdaki yeteneklerin maliyeti siber savunmadan daha düşük ve daha kullanılmadan bile karşı tarafta misilleme korkusu yaratarak siber savunmaya da katkı sağlayacaktır

- Siber güvenlik konusunda ulusal ve uluslararası alanda etkin koordinasyon ve işbirliği:

Ülkede bilişim sitem ve altyapılarını kullanan kişi, kurum ve kuruluş bütün kademelerin koordinasyon ve işbirliği içerisinde olması siber gücün etkisini artıracaktır. Siber ortamda saldırıların tespiti ve karşı konulmasında uluslararası işbirliğine ve koordineli hareket edilmesine de büyük ihtiyaç duyulmaktadır. Bu konudaki planlama ve uygulamalar siber savunmayı güçlendirirken siber caydırıcılığın etkinliğini de her bakımdan artıracaktır.

- Siber tehditlere ve saldırılara karşı bütün yeteneklerin kullanılması, koordinasyon ve işbirliğinin sağlanması için etkili komuta ve kontrol:

Siber ortamda bilişim sistemleri ve alt yapıları ile bunların etkin olarak kullanılması yeteneği olan siber güç unsurlarının kendi içerisinde birlikteliği yanında, diğer ulusal güç unsurları (insan, coğrafi, ekonomik, politik, psiko sosyal, bilimsel ve teknolojik ve askeri güç) ile de koordinasyon ve işbirliği içerisinde kullanımı planlanmalıdır. Siber ortamda savunma, taarruz ve istihbarat yeteneklerinin koordinesi ve işbirliğinde başarı içinse şüphesiz etkili bir komuta kontrol sitemi kurulmalıdır.

- Siber tehditlere ve saldırılara karşı caydırıcılık niyet ve kararlılığının karşı tarafa bildirilmesi için etkin duyuru ve açıklama politikası:

Karşı taraf tarafından bilinmeyen gücün ve yeteneğin, karşı tarafa etkisi ancak kullanıldığında anlaşılabilir. Fakat önemli olan ve istenilen, bunun önceden bilinmesi ve caydırıcılığından yararlanılmasıdır. Gücün ve yeteneğin baskın etkisi yaratması için gizli kalmasının da faydaları bulunmaktadır. Saldırı öncesinde olası hedeflere gücün ve yeteneklerin duyurulması, saldırı girişimine karşı veya saldırı sırasında caydırıcılık sağlayacak tehditle ilgili niyet ve kararlılığın içeriği ve duyurulma şekli ile vasıtalarının önceden belirlenmesi gerekir. Bu konudaki eksik ve yetersizliklerin başka sorunlara ve istenmeyen etkilere sebep olabileceği unutulmamalıdır.

- Siber güvenlik ve caydırıcılık stratejilerinin uygulanmasına yönelik ortaya çıkabilecek olası durumlara ve koşullara da uyarlı yüksek durumsal farkındalık:

Siber güvenlik ve caydırıcılık stratejilerinin uygulanmasının başarısı, bu stratejilerin uygulanmasında veya uygulanması sonrasında beklenen hedeflere ulaşılmaması durumunda, bilişim sistem ve altyapılarının bütün seviyelerindeki kullanıcıların bilgi ve eğitim seviyeleri ile farkındalıkları çok önemlidir. Bu konuda analizler, eğitimler, tatbikatlar vb çalışmaların yapılmasına yönelik planlamalar uygulamaya konmalıdır.

- Siber güvenlik ve caydırıcılık stratejilerinin güncellenmesi ve geliştirilmesi:

Bilişim sistemleri ve altyapılarında çok hızlı yaşanan gelişmelere paralel olarak çeşitleri ve şiddeti de artan siber tehdit ve saldırıların takip edilmesi, her geçen gün değişik kimliklere bürünen saldırganların (kişi, grup, kurum, ülke vb) yeteneklerinin tespit, analiz ve değerlendirme sonuçlarına göre siber güvenlik ve caydırıcılık stratejileri güncellenmeli ve geliştirilmelidir. Bu kapsamda araştırma, seminer, çalıştay, tatbikat vb faaliyetler düzenlenerek sonuçları stratejilere yansıtılmalıdır.

- Siber güvenlik ve caydırıcılık stratejilerinin güçlü ve merkezi bir otorite tarafından oluşturulması ve uygulanması:

Siber güvenlik ve caydırıcılıkta başarı sağlanmasında en önemli faktörlerden birisi şüphesiz bu konuda doğru ve ayrıntılı strateji ve politikaların hazırlanması ve kararlılıkla uygulanmasıdır. Tarihsel gelişim ve dünya üzerinde yaşananlardan öğrenilen en önemli koşul ise bu strateji ve politikaların güçlü ve merkezi bir otorite tarafından oluşturulması ve uygulanmasıdır.

VI. SONUÇ VE DEĞERLENDİRME (CONCLUSION AND EVALUATION)

Bilişim teknolojilerinin geliştiği ve hızla gelişmeye de devam ettiği günümüzde, bilgisayar ve iletişim teknolojilerinin sağladığı imkân ve kolaylıklardan etkin şekilde yararlanmak için siber güvenliğin önemi her geçen gün daha iyi anlaşılmakta, siber güvenlik ve savunmanın daha etkin şekilde sağlanması için de çalışmalar aralıksız sürdürülmektedir.

Siber saldırı olayları analiz edildiğinde, başarılarının, etkilerinin ve verilen zararların yüksek olmasında temel nedenlerinin başında savunmaya yönelik ulusal veya yerel strateji ve politikaların bulunmaması ya da bulunsa bile bunların yeterli olmaması veya etkin uygulanmaması gelmektedir.

Herşeyden önce, ülkenin haberleşme, enerji, su yönetimi, kritik kamu hizmetleri, ulaştırma, bankacılık ve finans gibi kritik altyapı sektörlerine yönelik siber saldırılara karşı korunması için siber gücün öncelikle savunma maksatlı olarak artırılması ve kritik altyapılar başta olmak üzere, ülkenin bilişim varlıklarının etkinlikle savunulması gerekmektedir.

Tarihte sadece savunmayla hiçbir zafer kazanılmamış, karşı saldırı ve taarruz yeteneğinin de kazanılmasının ve kullanılmasının gerekli ve kaçınılmaz bir zorunluluk olduğu anlaşılmıştır. Siber ortamda savunma veya taarruz şeklinde icra edilecek mücadele ve savaşlarda, maksat istek veya istekleri karşı tarafa zorla kabul ettirmek ve temel amaç kazanmak olsa da, Sun Tzu'nun "En iyisi savaşmadan baş eğdirmektir" özdeyişinden de hareketle, siber savaşta saldırganı saldırıdan veya savaştan caydırmak, yani 'siber caydırıcılık' en iyisi olabilir.

Türkiye'de geçmişten bugüne siber güvenlik strateji ve politikaları incelendiğinde, siber caydırıcılık konusuna gereken önemin verilmediği ve siber saldırılara karşı doğrudan veya dolaylı olarak caydırıcılık sağlanması için yapılan çalışmaların da yetersizliği de ortadır.

09 Kasım 2016 tarihli ve 6757 numaralı Kanun Hükmünde Kararname ile 5 Kasım 2008 tarihli ve 5809 sayılı Elektronik Haberleşme Kanununun 60'ıncı maddesinde değişiklik yapılarak Bilgi Teknolojileri ve İletişim Kurumuna; "Kamu kurum ve kuruluşları ile gerçek ve tüzel kişilerin siber saldırılara karşı korunması ve bu saldırılara karşı caydırıcılık sağlamak için her türlü tedbiri alma veya aldırma" [23] görevi verilmiştir.

Türkiye Cumhuriyeti Başbakanının, 22 Kasım 2016 günü Bilişim Zirvesi'nde, siber güvenlikle ilgili yaptığı ve basına da yansıyan açıklamasında "Siber saldırılarda caydırıcılığın arttırılacağını, saldırılardan sadece korunulmayacağını ayrıca caydırıcılık için ek önlemler alınacağını…" [24] ifade etmesi Türkiye'de siber güvenlik yanında siber caydırıcılık konusunda da umut verici çalışmaların başladığını göstermektedir.

Siber saldırılarda caydırıcılığı sağlamak için; saldırılara karşı önceden etkili bir siber savunmaya hazır olarak karşı konulmalı, etkin bir karşı saldırı ve taarruzla hedefe ulaşma gücüne, ancak savunma için de, taarruz için de, kısaca savaşta başarının vazgeçilmezi olan etkin siber istihbarat yeteneğine sahip olunmalıdır.

Siber ortamda savunma, taarruz, caydırıcılık ve istihbarat yetenekleri bilgi, bilgisayar ve iletişim konularında milli teknolojilere sahip olunarak desteklenmeli, milli teknolojilere sahip olunamayan alanlarda sahip olunan teknolojilere hâkim olunmalıdır.

Siber gücün geliştirilerek artırılması ve her maksatla etkin şekilde kullanılması için uygulayıcıların yetiştirilmesi ve farkındalıklarını artıracak eğitimler verilmesi, bu maksatla özellikle siber güvenlik konularında uzman kadroların oluşturulması, her seviyede eğitim ve öğretimin planlanması ve yaygınlaştırılması gerekmektedir.

Siber gücün artırılması ve siber saldırılara karşı caydırıcılık da sağlayarak etkin güvenlik ve korunma için her alanda koordinasyon ve işbirliği gerekir. Bunun için bütün devlet kurum ve kuruluşları ile özel sektör arasında etkin iş birliği ve koordinasyon sağlanmalıdır.

Siber güvenliği hukuki, teknik, idari, ekonomik, politik ve sosyal boyutları ile ele alan bütüncül bir yaklaşımın benimsenmesi, gerekli yasal mevzuatın mutlaka oluşturulması ve etkinlikle uygulanması gerekmektedir. Bilişim teknolojileri ve özellikle internet sayesinde ülkelerarası etkileşimin boyutunun

da derinleşmesi nedeniyle, diğer ülkelerle siber saldırılara karşı işbirliği yapılması, suçluların yakalanması ve haklarında gecikmeksizin yasal işlem yapılarak cezalandırılması, aynı zamanda caydırıcılık sağlaması yanında saldırıların azalmasını da sağlayacaktır.

Siber güvenlik başta olmak üzere, siber gücün artırılması, etkin bir yönetim ve denetim sağlanması için teşkilatlanmaya gidilmesi, 2016-2019 Ulusal Siber Güvenlik Stratejisinde belirtildiği gibi "Siber güvenlik alanında koordinasyonu sağlayacak güçlü bir merkezi kamu otoritesi oluşturulması" [5] ve siber gücü kullanma yetkilerinin tek bir merkezde toplanması kısa sürede olumsuzlukların en aza indirilerek başarının artırılmasını da sağlayacaktır. Siber güvenlik stratejisini oluşturarak uygulayacak teşkilatın, dünyadaki örneklerinden de yararlanılarak, bir ordu yapılanması gibi düşünülerek hayata geçirilmesi teşkilatın etkinliğini ve başarısını daha da artıracaktır.

Siyasi, askeri, ekonomik, coğrafik, demografik, bilimsel, teknolojik, sosyal ve kültürel güçten oluşan Milli Güç unsurlarının her biri uluslararası ortamda ve ilişkilerde aynı zamanda birer caydırıcılık unsuru oluşturmaktadır. Bilimsel ve Teknolojik Güç içerisinde kabul edilen 'Siber Güç (siber savunma, taarruz ve caydırıcılık gücü)' ile de, tek başına veya diğer milli güç unsurlarıyla birlikte siber alanda, uluslararası hukuk ilkelerine bağlı kalarak, kendine özgü kural, esas ve stratejiler doğrultusunda yaptırım uygulamak ve belirlenecek amaçlar doğrultusunda tespit edilecek talep ve isteklerin gerçekleştirilmesi için strateji ve politikalar geliştirerek daha güçlü ve etkin 'caydırıcılık' sağlamak mümkündür. Bu amacın başarısı ise ulusal ve yerli üretim sektörüne gereken önem verilerek caydırıcılık sağlayacak şekilde yönlendirilmesi ve desteklenmesinden geçmektedir.

Siber caydırıcılıkta temel esas ve önemli olan siber saldırıların/savaşın doğru zamanda, doğru hedefe yönelik, doğru teknik ve yöntemlerle yapılmasıdır. Bu kapsamda, 'Siber Güçle Caydırıcılık'; üzerinde düşünülmesi, daha fazla önem verilmesi, diğer alanlardaki caydırıcı gücün bu alanda da oluşturulması için ciddi ve ayrıntılı olarak çalışılması, konuyla ilgili doktrinler üretilmesi, mevcut stratejilerin bu yönde güncellenmesi, yeni stratejiler geliştirilmesi ve geleceğe dönük planlamalar yapılarak gecikmeksizin uygulamaya konulması gereken çok önemli bir konu olduğu değerlendirilmektedir.

TEŞEKKÜR (ACKNOWLEDGEMENT)

Makalenin hazırlanması aşamasında destek ve katkıları dolayısıyla, Prof. Dr. Şeref SAĞIROĞLU'na teşekkür ederim.

KAYNAKLAR (REFERENCES)

[1] Goodman, M., Geleceğin Suçları Dijital Dünyanın Karanlık Yüzü, TİMAŞ Yayınları, İstanbul, 2016.
[2] Nye, J. S., Cyber Power, http://belfercenter. ksg.harvard.edu /files/ cyber-power.pdf, (Erişim: 18 Şubat 2017).
[3] Tzu, Sun, Savaş Sanatı, Türkiye İş Bankası Kültür Yayınları, İstanbul, 2014.
[4] Singer, P.W. ve Friedman, A., Siber Güvenlik ve Savaş, Buzdağı Yayınları, Ankara, 2015.
[5] T.C. UDHB , 2016-2019 Ulusal Siber Güvenlik Stratejisi ve Eylem Planı, T.C. UDHB Yay. Ankara, 2016.
[6] Şenol, M., Siber Güçle Caydırıcılık Ama Nasıl? Uluslararası Bilgi Güvenliği Mühendisliği Dergisi, Cilt:2, No:2, Ankara, 2016.
[7] TDK, Büyük Türkçe Sözlük, http://www.tdk.gov.tr/index. php?option=com_bts, (Erişim: 25 Şubat 2017).
[8] Klimburg, A., National Cyber Security Framework Manual, NATO Yayını, Talinn, 2012.
[9] Yayla, M., Hukuki Bir Terim Olarak Siber Savaş, Türkiye Barolar Birliği Dergisi, Sayı 104, Ankara, 2013.
[10] Clarke, R.A.ve Knake, R.K., Siber Savaş, İKÜ Yayınları, İstanbul, 2010.
[11] NATO Cooperative Cyber Defence Centre of Excellence, https://ccdcoe.org/cyber-security-strategy-documents.html, (Erişim: 18 Şubat 2017).
[12] Kızmaz, Z., Ceza veya Kriminal Yaptırımın Suç Oranları Üzerindeki Caydırıcı Etkisi, Afyon Kocatepe Üniversitesi Sosyal Bilimler Dergisi, Cilt:7, Afyonkarahisar, 2005.
[13] Özdemir, H., Uluslararası İlişkilerde Güç-Çok Boyutlu Bir Değerlendirme, Cilt:63, Sayı:3, Ankara Üniversitesi SBF Dergisi, Ankara, 2008.
[14] Akad, M. T., Modern savaşın Temel Kavramları, Kitap Yayınevi, Ankara, 2011.
[15] Long, A., Deterrence From Cold War to Long War, RAND Corporation, ABD, 2008.
[16] Lupovici, A, Cyber warfare and deterrence. Military and Strategic Affairs, Volume:3, No:3, İsrail, 2011.
[17] Libicki, M. C., Cyberdeterrence and Cyberwar, RAND Corporation, ABD, 2009.
[18] Gorman, S. ve Barnes, J. E., Cyber Combat: Act of War, http://www.wsj.com/articles/SB10001424052702304563104 5763556 23135782718, (Erişim: 25 Şubat 2017).
[19] T.C. MGK Sekreterliği, 27 Ekim 2010 Tarihli Toplantı, http://www.mgk.gov.tr/index.php/27-ekim-2010-tarihli-toplanti, (Erişim: 25 Şubat 2017).
[20] Resmi Gazete, UDHB'nin Teşkilat ve Görevleri Hakkında Kanun Hükmünde Kararname, http://www.resmigazete. gov.tr/eskiler /2011/11/20111101M1-1.htm, (Erişim: 01 Şubat 2017).
[21] T.C. UDHB, Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı, T.C. UDHB Yay. Ankara, 2016.
[22] T.C. Kalkınma Bakanlığı, 2015-2018 Bilgi Toplumu Stratejisi ve Eylem Planı, Bilgi Toplumu D.Yay., 2015.
[23] Resmi Gazete, Olağanüstü Hal Kapsamında Bazı Kurum ve Kuruluşlara İlişkin Düzenleme Yapılması Hakkında KHK Değiştirilerek Kabul Edilmesine Dair Kanun, http://www. resmigazete.gov.tr/eskiler/2016/11/20161124-4..htm, (Erişim: 01 Şubat 2017).
[24] Bilgi Teknolojileri ve İletişim Kurumu, Bilişim Zirvesi'16 "No Way Out!" Dedi, https://www.btk.gov.tr/tr-TR/Ulusal-Etkinlik/BILISIM-ZIRVESI16-NO-WAY-OUT-DEDI, (Erişim: 01 Şubat 2017).