# SİBER GÜÇLE CAYDIRICILIK AMA NASIL?

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

**ÖZET**

Bu çalışmada, bilgi ve iletişim sistemlerinin kazandırdığı siber güçle caydırıcılık sağlanabileceği vurgulanmış; siber güç, caydırıcılık, siber saldırı ve siber savaş kavramlarıyla ilgili bilgiler verilmiş; bilişim teknolojilerinin, özellikle internetin gelişmesi ve yaygınlaşması sonrasında dünyada ve Türkiye'de yaşanan bazı önemli siber saldırı olayları ve sonuçları gözden geçirilmiş; kazanılacak siber güçle karşı tarafa etkili hasar, zarar ve kayıplar verdirilebileceği gösterilerek yaptırım uygulanabileceği vurgulanmış; 2014 yılında Sony firmasına yapılan siber saldırıların içerik ve sonuçları değerlendirilmiştir. Sonuçta, 'siber güç' kullanılarak 'caydırıcılık' sağlamanın mümkün olduğuna, maliyet ve kullanım kolaylıkları yanında asimetrik savaş imkânı da sağlaması nedeniyle, siber caydırıcılığın ülkemiz için 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.

# DETERRENCE BY CYBER POWER BUT HOW?

**ABSTRACT**

This study emphasizes the cyber deterrence, which can be provided by the cyber power gained through the information and communication systems today. This is an important issue. Information is given on the concepts of cyber power, deterrence, cyber-attacks and the cyber warfare. Various significant cyber-attack events and their results in the world and in Turkey were evaluated. Also, sanctions can be imposed by demonstrating that the gained cyber power causing effective damage, harm and loss to the opponents by indicating the content and consequences of the cyber-attacks on Sony in 2014. Consequently, it is remarked that providing 'deterrence' by using 'cyber power' is possible; That since it provides opportunity of asymmetric warfare, besides cost and ease of use, cyber deterrence is a very important issue for Turkey. Some remarks were suggested and the results were concluded and summarised. It should be emphasized that strategies and policies should be developed on and implemented without delay.

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

## I. GİRİŞ (INTRODUCTION)

Her geçen gün gelişen bilgi sistemleri ve iletişim teknolojileri yardımıyla, kamu ve özel kurum ve kuruluşların özellikle haberleşme, finans, enerji ve güvenlik faaliyetlerini bilgi sistemleri üzerinden yürütmesi sonucu bilgi sistemleri ve altyapıları günlük yaşamın vaz geçilmez bir parçası olmuştur. Bilginin, elektronik ve bilişim sistemlerinin sağladığı imkânlarla, daha etkin işlenmesi, iletimi, muhafazası ve kullanılması sonucu, devletlerin özellikle ekonomik, politik ve askeri güçlerindeki kısa sürede olumlu yükseliş, kara, deniz, hava ve uzay ortamlarından sonra 5'inci Harekât Alanı olarak, ortaya çıkan siber ortamın önemini daha da artırmıştır.

Siber ortamda bilgilere ve bilişim sistemlerine yönelik kötü niyetli hareketlerin ve saldırıların başlaması ve bunların artarak devam etmesi 'Siber Güvenlik-Savunma' kavramlarını, karşı tarafın bilgilerine ve bilgi sistemlerine zarar verme veya olumsuz etkileme istek ve ihtiyaçları ise 'Siber Saldırı-Taarruz' kavramlarını ortaya çıkarmıştır. Devletler siber

savunma ve siber taarruz kavramlarıyla ilişkili olarak strateji ve politikalar geliştirmeye ve bunları etkinlikle uygulamaya başlamışlardır. Bunlarla birlikte de siber savaş konusu ortaya çıkmıştır.

Siber savaşın başlatılması ve sürdürülmesi için gerekli olan, siber ortamda sahip olunan bilgi sistemleri ve altyapıları ile bunların etkin olarak kullanılması yeteneği, 'Siber Güç' olarak tanımlanmaktadır [1]. Siber güç, kısaca 'Siber ortama hâkimiyet' demektir. Siber güçle, özellikle ekonomik, politik ve askeri güçlerin etkileri daha da artırılabilirken, siber güç tek başına da etkin olarak kullanılabilmektedir.

Türkçede genellikle "korkutarak cesaret kırmak ve vazgeçirmek" anlamlarında kullanılan 'caydırmak' sözcüğünden türetilen 'Caydırıcılık' kavramı Türk Dil Kurumu Sözlüğünde "Bir saldırganlığı önlemek ve engellemek için önlem alma işi" [2] olarak açıklanmaktadır.

Caydırıcılık hukuksal alanda "ceza veya hapis korkusuyla suç işlemekten alıkoyma" [3], uluslararası ilişkilerde yani diplomasi alanında "karşıdaki devleti emellerinden vazgeçirme davranışı veya belirli davranışlara yönlendirme" [4], askeri alanda ise "düşmanı çok yüksek bedel ödeyeceğine inandırarak bir hareketten vazgeçirmek için askeri güç, yaptırım ve tehditlerin kullanımı" [5] olarak ifade edilmektedir.

Geleneksel caydırıcılık teorisine göre caydırıcılık ise, geniş anlamıyla, "rakibin beklediği faydaların tahmini maliyetleri ve riskleri karşılamayacağı için, belirli bir eylemi başlatmamaya ikna edilmesi" anlamına gelmektedir [6].

Geçmişe veya 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.

Caydırıcılığı genel anlamda "karşı tarafa düşmanca eylemleri yapmama konusunda gözdağı verme" şeklinde tanımlayan 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 [7]. Siber caydırıcılık kapsamında misillemenin etkisinin de, nükleer ve konvansiyonel caydırıcılıktan sonra, diplomatik ve ekonomik yaptırımlarla sağlanan caydırıcılıktan ise önce geldiğinin kabul edilebileceğini belirtmektedir.

Bu çalışmada; siber ortamda, son yılların bilgi ve iletişim teknolojileri kullanılarak sahip olunan gözde gücü 'Siber Güç'le Caydırıcılık; caydırıcılığın askeri ve diplomatik alanlarda uygulanması anlamlarının bütünleşmesi şeklinde ele alınmıştır. Yani siber güç kullanılarak, "karşıdaki devlet veya devlet benzeri oluşumların bir hareketten veya emellerinden vazgeçirilmesi ya da belirli davranışlara yönlendirilmesi" sağlanabilir mi ve nasıl sağlanabilir sorularının cevaplarının ortaya konması amaçlanmış ve siber güçle caydırıcılığın öneminin vurgulanması hedeflenmiştir.

Yöntem olarak; siber güç ile siber savaş bağlantısı, dünyada ve Türkiye'de yaşanan bazı önemli siber saldırıların ve olayların içerik ve sonuçları açıklanarak siber güçle devlet veya devlet benzeri oluşumlara karşı caydırıcılık maksadıyla kullanılabileceği ve caydırıcılık sağlanabileceği açıklanmaya çalışılmış, müteakiben özellikle caydırma maksatlı yapılan siber saldırı olaylarından bir tanesinin nasıl uygulandığı ve sonuçları ortaya konmuş, daha sonra konuyla ilgili stratejiler geliştirilmesine yönelik görüş ve değerlendirmelerde bulunulmuştur.

## II. SİBER GÜÇ, SİBER SAVAŞ VE SİBER SALDIRILAR (CYBER POWER, CYBER WAR AND CYBER ATTACKS)

İnternet, iletişim ağları, bilgisayar sistemleri, gömülü işlemci ve kontrol birimlerini içeren, bilgi teknolojileri altyapılarından meydana gelen, birbirine bağımlı ağların oluşturduğu bilgi ortamındaki küresel alan [8] olarak da ifade edilen siber alanda, bilgisayar ve iletişim teknolojilerinde ve özellikle 1990'lar sonrası internette yaşanan hızlı gelişmeler siber gücün etkisini artırarak ortaya çıkarmış, siber gücün hayatı kolaylaştırmanın yanında aynı zamanda bir tehdit ve yaptırım aracı da olduğunu göstermiştir.

Bilgi ve iletişim teknolojilerindeki gelişmelerle siber ortamın sağladığı imkân ve kolaylıklar yaşamı her geçen gün kendisine daha bağımlı hale getirirken, bu ortamın tehdit, saldırı, cana ve mala zarar verme vb amaçlarla kullanılması sonucunda kişilerin, toplumların ve ülkelerin uğradığı büyük zararlar güvenlik anlayışında büyük değişikliklere yol açmıştır. Bu kapsamda, bilgisayar ve iletişim teknolojilerinin sağladığı imkânlardan ve kolaylıklardan daha çok siber suçlar, siber saldırılar ve hatta siber savaş konuşulur olmuş, bunların sonucunda da bilgi ve iletişim sistemlerinin ve yapılarının siber saldırılara karşı korunmasının, yani siber güvenliğin sağlanmasının yolları aranır olmuştur.

Günümüzde işlenen siber suçların ve siber saldırıların çeşitliliği, miktarı ve şiddeti de her geçen gün daha da artarken, saldırganların bilgi ve yetkinlik seviyeleri ise düşmekte [9], siber savaş da sadece konuşulmakla kalmayıp, başlamış devam etmektedir. Dünyada siber savaşın başlayıp devam ettiği değerlendirmesinin doğruluğunu ve siber gücün etkisini ortaya koyan, yazılı ve görsel basın gibi açık kaynaklara da yansıyan önemli siber olaylar ve siber saldırıların bazıları aşağıda sunulmuştur. Bu saldırılar konuyla ilgilenenlerce bilindiği için ayrıntılarına girilmemiş, ancak siber güçle neler yapılabileceğine dikkat

çekmek amacıyla aşağıda başlıklar altında kısaca tanıtılmış ve değerlendirilmiştir.

• **2000'de Avustralya'da arıtma tesisi bilgi sistemlerine saldırı ve kanalizasyon sularının şehre bırakılması:** 28 Şubat - 23 Nisan 2000 tarihleri arasında, Avustralya'nın Moroochy eyaletinde, arıtma tesisi bilgi sistemlerine müdahale sonrasında pis kanalizasyon suları, en az 40 defa, parklara, nehirlere hatta turistik bir otelin zeminine bırakılmıştır [10].

• **2003'te ABD'nin sekiz eyaletinde 2 gün süren, ölümlere ve zarara yol açan elektrik kesintisi:** 14 Ağustos 2003'te ABD'nin sekiz eyaletinde 50 milyon kişiyi etkileyen, bazı şehirlerde 2 gün süren, 11 kişinin ölümüne ve 6 milyar dolar zarara yol açan ve tarihe 'Kuzey Doğu Kesintisi' olarak geçen ABD tarihinin en önemli elektrik kesintisinin nedenlerinden birisinin enerji yönetim sisteminde kullanılan bir yazılımdan kaynaklandığı saptanmıştır [10].

• **2007'de Rus bilgisayar korsanlarının Estonya bilgi sistemlerine saldırısı ve ülke çapında faaliyetlerini durma noktasına getirmesi:** 2007 yılı Nisan ve Mayıs aylarında, Rus bilgisayar korsanlarının Estonya bilgi sistemlerine sızması, özellikle internet ve bankacılık hizmetlerini durma noktasına getirmiş, ülke çapında ciddi ekonomik ve toplumsal zararlar yaşanmıştır [10].

• **Eylül 2007'de İsrail savaş uçaklarının Suriye topraklarına girmesi ve nükleer tesisini imha ederek zayiatsız dönmesi, bu sırada Suriye hava savunmasının hiçbir hedef görememesi:** 6 Eylül 2007'de İsrail savaş uçakları Türkiye-Suriye sınırını takip ederek hiçbir engelle karşılaşmadan Suriye topraklarına girmiş, nükleer tesisin yerle bir edilmiş harabesini bırakarak, en ufak bir zayiat vermeden evlerine dönmüşlerdir. İsrail uçaklarının saldırıları sırasında Suriye hava savunması siber saldırılar nedeniyle hiçbir hedef görememişlerdir [10].

• **2008'de Rusya-Gürcistan savaşında Gürcistan'a yapılan siber saldırılar sonucu ciddi sıkıntılar yaşanması:** 2008 yılı Ağustos ayında, Rusya-Gürcistan savaşında, başta devlet başkanlığı internet sitesi olmak üzere Gürcistan'ın neredeyse tüm internet sayfaları bloke edilmiştir. Finans merkezleri, haberleşme sistemleri ve elektrik santralleri ciddi sıkıntılar yaşamıştır [10].

• **2010'da İran nükleer zenginleştirme programını hedefleyen ve ciddi sorunlara sebep olan 'Stuxnet' yazılımı saldırısı:** 2010 yılı Temmuz ayında keşfedilen, endüstriyel kontrol sistemlerini hedefleyen ve bilinen en tehlikeli zararlı yazılım olduğu düşünülen 'Stuxnet' yazılımı ile İran nükleer zenginleştirme programına saldırıldığı ve ciddi zararlar verildiği ortaya çıkmıştır. Bu saldırı, yazılım sistemlerine fiziksel zarar veriyor olması ile de bir ilk olmuştur [10].

• **Kasım 2010'da WikiLeaks'in yayınladığı belgeler ile diplomaside sanal bomba etkisi yaratması:** İsveç merkezli uluslararası bir oluşum olan WikiLeaks, yayınladığı diplomatik belgeler ile dünya çapında ses getirmiş ve şimdiye kadar açıkladığı toplam bir milyon civarında gizli yazışma ile diplomaside depreme yol açmıştır [11].

• **Aralık 2011'de İran Silahlı Kuvvetlerinin ABD'ye ait insansız hava aracının kontrolünü ele geçirerek yere indirmesi:** 2011 yılı Aralık ayında, İran Silahlı Kuvvetlerinin İran'ın doğusunda, ABD'ye ait insansız casus uçağının kontrolünü ele geçirip sapasağlam yere indirerek el koyması, bütün dünyanın ilgisini çeken ve siber harekât açısından incelenmeye değer bir olay olmuştur [10].

• **Aralık 2014'te Sony Şirketinin yoğun siber saldırılar sonucu Kuzey Kore Lideriyle ilgili filmi gösterimden kaldırması:** Aralık 2014'te, Kuzey Kore liderine suikast girişimini konu alan komedi filmi Kuzey Kore tarafından tepkiyle karşılanmış, yapımcı Sony Pictures Firması yoğun siber saldırılara maruz kalmış, şirket bilgisayarlarından çekimine başlanmamış film senaryoları ve personel bilgileri dâhil pek çok gizli bilgi/belge sızdırılmış, tehditler ve siber saldırılar sonucu film gösterimden kaldırılmıştır. Saldırılardan Kuzey Kore Cumhuriyeti sorumlu tutulmuş ancak kanıtlanamamıştır [12].

• **Ekim 2016'da ABD'de yapılan saldırılar sonucu internet bağlantısının yüzde 90'ının engellenmesi:** 21 Ekim 2016'da, ABD'nin doğu yakasına hizmet sunan DNS altyapılarına yönelik olarak başlayan saldırılar ülke geneline yayılarak internet bağlantısının yüzde 90'ını engellemiş ve Türkiye'nin de aralarında bulunduğu birçok ülkede etkisini göstermiştir. Özellikle sanal ticarete darbe vuran saldırıların, ABD ekonomisine maliyetinin 7 milyar doları bulduğu belirtilmiştir [13].

Yukarıda açıklanan ve dünyada yaşanan bu siber olayların benzerleri de Türkiye'de yaşanmış olup, yaşanan bu önemli siber saldırıların ve olayların bazıları aşağıda sıralanmıştır.

• **Ağustos 2008'de Bakü-Tiflis-Ceyhan boru hattına saldırı sonrası patlama meydana gelmesi:** 5 Ağustos 2008'de Bakü-Tiflis-Ceyhan boru hattındaki 1,768 kilometrelik hat üzerinde Erzincan'ın Refahiye ilçesi yakınlarında bir patlama meydana gelmiş, Türk makamların sabotajdan şüphelenmesi ile PKK terör örgütü saldırıyı üstlenmişti. Araştırma sonucunda ise patlamanın nedenin teknik arızadan kaynaklandığı belirtilmişti. Ancak sonradan elde edilen bilgilere göre, bu patlamanın bir siber saldırı sonucunda gerçekleştiği anlaşılmıştır [14].

• **Ocak 2009'da zararlı bir yazılımın Atatürk Havalimanı bilgisayarlarını etkilemesi:** 30 Ocak 2009 tarihinde birçok ülkenin bilgisayar sistemine yayılan ve önemli zararlar veren 'Conficker' virüsü İstanbul'da Atatürk Havalimanı'nın dış hatlar

terminalinde çalışan bilgisayarları ciddi şekilde etkilemiştir [10].

- **Haziran 2011'de saldırılar sonrasında TİB'in sitesinin devre dışı kalması:** 9 Haziran 2011'de 'İnternete Filtre Uygulamasının karşısında temel hak ve özgürlüklerin ihlal edileceğini savunan 'Anonymous' adlı Uluslararası Bilgisayar Korsanları Topluluğu akşam saatlerinde BTK Telekomünikasyon İletişim Başkanlığının internet sitesine saldırmış, devre dışı kalan site çalışmaya gece yarısından sonra ancak başlayabilmiştir [10].

- **Mart 2015'te 79 ili etkileyen elektrik kesintisi:** 31 Mart 2015 günü ülkemizde elektriğini İran'dan alan Van ve Hakkâri hariç 79 ilde elektrik kesintisi yaşanmıştır [15]. Nedeniyle ilgili uzmanların görüşü; "Yüklü bir hattın devre dışı kalmasının tüm sistem dinamiğini bozması, ardından diğer hatların bir arıza olduğunu düşünerek kademeli olarak kendilerini kapatması…" [16] şeklinde olmuştur. Kısa süre sonrasında ise, "TEİAŞ Siber Saldırıları Engellemek için Bilgisayar Ağları İhalesine Çıkıyor" [17] haberi basında yer almıştır.

- **Aralık 2015'te, 10 gün süreli saldırılar sonucu birçok internet sitesine ve mobil uygulamalara erişim sağlanamaması:** 14 Aralık 2015 tarihinde başlayan ve yaklaşık 10 gün süreli, özellikle 'tr' uzantılı alan adlarının yönetildiği sunucuları hedef alan saldırılar sonucu birçok banka, noter ve devlet kurumunun internet sitesine ve mobil uygulamalarına erişim sağlanamamıştır. İnternet trafiğini büyük ölçüde etkileyen bu toplu saldırıların, bugüne değin dünya üzerinde yaşanmış en yoğun siber saldırılardan biri olduğu ifade edilmiştir [18].

- **Mayıs 2016'da Sağlık Bakanlığı hastanelerine yönelik siber saldırılar ile veri tabanındaki bilgilerin çalınması ve silinmesi:** 18 Mayıs 2016 günü sabah saatlerinde, 33 devlet hastanesinin veri tabanlarında bulunan bilgilerin kopyalandıktan sonra silindiği, saldırıları 'Anonymous' adlı grubun üstlendiği belirtilmiştir. Sağlık Bakanlığı sistemin kısmen etkilendiğini ve yedekleme mekanizması sayesinde olası veri kayıplarının önüne geçildiğini duyurmuştur [19].

Tüm bu yaşanan olaylar ve siber saldırılar; siber gücün tek başına veya başka güç unsurlarıyla birlikte kullanılmasının sonucudur. Bu sonuçlardan, siber gücün çeşitli strateji, taktik, teknik ve usullerle kullanılmasıyla gerçekleştirilecek siber saldırılarla;

- Askeri haberleşme dâhil girilip yanıltıcı bilgilerin sistemlere bırakılabileceği,
- Hava kontrol sistemlerine sızılabileceği,
- Stratejik sistemlerin ve projelerin devre dışı bırakılabileceği,
- Kritik altyapıların her zaman tehdit altında kalabileceği,
- İletişim ağlarının devre dışı bırakılarak haberleşmenin sekteye uğratılabileceği,
- Ulaşım ve su sistemlerinin bozulabileceği, bankacılık ve finans sektörünün çökertilebileceği,
- Elektrik ve doğal gaz sisteminin kapatılabileceği ve doğalgaz boruları basıncının artırılarak tahrip edilebileceği,
- Baraj kapaklarının açılarak şehirlerin sular altında bırakılabileceği,
- Enerji santrallerin kontrolünün ele geçirilerek potansiyel birer atom bombasına dönüştürülebileceği,
- Ülkelerde, karma (hibrit) savaş tekniklerinin kullanılabileceği,
- Toplumsal olayların çıkarılabileceği veya yönlendirilebileceği,
- Halka verilen haberleşme, elektrik, doğalgaz, e-devlet, ulaşım, vb hizmetler engellenerek ülkede kargaşa ve karışıklık yaratılabileceği,
- Kişi, toplum, devlet ve ülke güvenliği için çok büyük endişeler yaratılabileceği

gibi önemli sonuçlara ulaşmak yanlış olmayacaktır.

## III. SİBER GÜÇ VE CAYDIRICILIK (CYBER POWER AND DETERRENCE)

Saygınlık kaybı, gizlilik, kamu yararı, ulusal ve uluslararası güvenlik vb nedenlerle açıklanmayanlar yanında, yazılı ve görsel basın, medya gibi açık kaynaklarda da yer alan siber saldırı olaylarına ve bunların olumsuz sonuçlarına rağmen, siber savaşın bir savaş olup olmadığı tartışmaları ile birlikte, siber alanda siber güçle bir caydırıcılığın mümkün olup olmadığı konusunda da tartışmaların başlamış ve devam etmekte olduğu görülmektedir.

Siber caydırıcılığın, bugünün teknolojik yetersizlikleri ve uluslararası hukuktaki eksiklikler nedeniyle çoğu ülke için uygulanabilir olmadığı [6] iddia edilmekte, nükleer savaşı önlemenin olmazsa olmazı olan caydırıcılık kuramının, günümüzde siber savaşı durdurmakta önemli bir rol oynayamadığı [20] ve ABD'nin nükleer ve konvansiyonel anlamda sağladığı caydırıcılığı, tüm çabasına rağmen siber alanda sağlayamayacağı [21] ileri sürülmektedir. Nitekim 2011 yılında ABD Savunma Bakanlığınca, "ABD'ye yapılan siber saldırıların savaş sebebi kabul edileceği ve karşılığında siber uzayda ya da askeri operasyonlarla cevap verme hakkının bulunduğu" [22] açıklanmıştır.

Ancak, siber silahlar nükleer silahlara benzemez ve bireyler, küçük gruplar ve devletler tarafından kolayca geliştirilir ve konuşlandırılırlar. Kolayca çoğaltılır ve ağlar arasında dağıtılır [23]. Siber alanda bilgisayar ve iletişim teknolojileri kullanarak elde edilen imkân ve kolaylıkların bir güç (siber güç) olduğu, bu gücün hem saldırı aracı, hem de saldırı hedefi olabileceği, tarafların birbirine zarar vermek, siber güçlerini zayıflatmak veya bazı unsurlarını devre dışı bırakmak maksadıyla karşılıklı siber güçlerini kullanabilecekleri tereddüde meydan bırakmayacak şekilde ortadadır. Bu

arada, güçlü ülkelerin en gelişmiş siber silahlarını kullandığı türden bir siber savaşın henüz gerçekleşmediği [20] öne sürülmektedir. Bu nedenle gelişmiş ve kullanılmayı bekleyen siber silahların kullanılacağı bir savaşı kimin kazanacağı, bu savaşın sonuçlarının ne olacağı şu anda tahmin edilse de tam olarak bilinmemektedir.

Saldırıların bir kısmının devlet destekli olduğu bilinse de bazılarının küçük saldırı gruplarınca gerçekleştirildiği ve siber saldırıların ve olayların, daha önce açıklandığı üzere, sadece bilinen sonuçlarına bakmak bile, "siber alanda siber güç kullanılarak caydırıcılık (siber caydırıcılık) sağlanabilir" sonucuna ulaşmak için yeterli olmaktadır.

Siber caydırıcılıkta, askeri yeteneklerin ve güç gösterilerinin aksine, bir ülkenin büyüklüğü pek önemli değildir. Bir siber savaşın savaş alanı tüm dünya olup, nitelik, girişim ve konum özellikleri genellikle nicelikten daha önemlidir [24]. Bunun daha iyi anlaşılmasını sağlamak için, siber saldırılarla caydırıcılığın nasıl sağlandığı ve hedeflenen sonuçlara nasıl ulaşıldığı açıkça görülen ve açık kaynaklarda da geniş yer tutan, "Aralık 2014'te Kuzey Kore Lideriyle ilgili film nedeniyle Sony Şirketinin yoğun siber saldırılara maruz kalması ve filmin gösterimden kaldırılması" olayı örnek alınmış ve açık kaynaklara yansıyan bazı ayrıntıları aşağıda sunulmuştur.

ABD'de Sony Pictures firmasının yapımcısı olduğu, 'Röportaj (The Interview)' isimli filmde, Kuzey Kore Lideri Kim Jong-Un ile röportaj yapmaya hazırlanan bir muhabirin ABD Merkezi İstihbarat Teşkilatı (CIA) tarafından Kim'e suikast düzenlemek için eğitilmesi ve ardından Kuzey Kore'de yaşadıkları anlatmaktadır [12].

Film, Kuzey Kore'de büyük öfkeyle karşılanmış ve "Yüce lideri aşağılıyorlar" yorumları yapılmıştır. Bu yorumların ardından, Sony kendilerini 'Barışın Savunucuları' olarak tanımlayan kimliği belirsiz bir grup bilgisayar korsanı tarafından başlatılan yoğun siber saldırılara maruz kalmış ve düzenlenen siber saldırılar sonrasında, Sony firmasına ait, aralarında çekimine başlanmamış film senaryoları dâhil, pek çok film çalınarak internet ortamında yayımlanmıştır. Şirket içindeki pek çok gizli bilgi ve belgeler ile tüm özel elektronik posta ve yazışmalar da bu arada yayımlanmıştır. Sony, bu saldırı nedeniyle milyonlarca dolar zarara uğratılmıştır.

Filme tepki olarak gönderilen ve Sony çalışanlarının ekranlarına "11 Eylül 2001'de neler olduğunu hatırlayın. Size tavsiyemiz bu filmi gösterime sokan sinemalardan uzak durmanız!" denilen mesajlar düşmüştür.. Gönderilen e-postalarla filmi göstermeyi planlayan sinema salonları da açıkça tehdit edilmiştir [25].

ABD Federal Soruşturma Bürosu (FBI), bu saldırılardan Kuzey Kore'yi sorumlu tutmuştur. FBI'nın, "Siber saldırıların ardındaki yazılımların Kuzey Kore ile bağlantılı olduğunu ve filmle bağlantılı şirketlerin risk altında olabileceğini…" duyuran açıklamasının ardından, ülkenin en büyük sinema zincirleri filmi göstermekten vazgeçtiklerini açıklamıştır. Gelişmeler üzerine Sony firması, 44 milyon dolara mal olan filmi geri çektiklerini belirten açıklamasında "Ortaklarımızın kararını anlıyor ve saygı duyuyoruz ve tabii çalışanların ve sinemaseverlerin güvenliğine verdikleri değeri paylaşıyoruz." denilmiştir. Filmin sadece ilk hafta sonu 30 milyon dolar gişe yapması ve Sony'nin filmden toplam 120 milyon dolar kazanabileceğinin beklendiği de raporlanmıştır [12].

ABD yönetimi, Sony'ye yapılan saldırıların 'ulusal güvenlik meselesi' olarak değerlendirildiğini duyurmuştur. ABD Başkanı Barack Obama, söz konusu filmin vizyona çıkmasının engellenmesine neden olan siber saldırıların ardında Kuzey Kore'nin olduğuna inandıklarını belirtmiştir. Kuzey Kore tarafından yapılan açıklamalarda, siber saldırılardan sorumlu oldukları iddiaları yalanlamış ve bunun 'terbiyesizce yapılan dedikodular' olduğunu belirtmişlerdir.

"Kuzey Kore liderine yönelik saldırıyı konu alan 44 milyon dolarlık filmin, 'siber korku' nedeniyle geri çekildiği, Sony Pictures'ın, kendi halkını öldüren zalim bir diktatörün baskılarına boyun eğdiği, bu olayın ifade özgürlüğüne bir tehdit olduğu…" haber ve yorumları yapılmıştır. ABD Temsilciler Meclisi'nin eski başkanı Newt Gindrich, "Sony'nin kararı ile ABD'nin ilk siber savaş yenilgisini aldığını" belirtmiştir [25].

Sonuçta; Kuzey Kore lideriyle ilgili komedi filminin gösterimden kaldırılmasının arkasında bu ülke tarafından devlet destekli (direk/dolaylı) siber saldırıların hedefe ulaştığını, bir ülke veya devlete karşı olmasa da Sony gibi uluslararası, küresel dev bir firmaya karşı, yapılan siber saldırılar ile caydırıcılık sağlanmış ve geri adım attırılmıştır.

Saldırıların başarılı olmasında;

- Siber istihbarat,
- Teknolojik güç,
- Medyanın ve psikolojik harekâtın etkin kullanılması,
- Saldırıların çok iyi düşünülüp hedef odaklı olarak yönlendirilmesi ve organizasyonu,
- Devlet desteğinin gizliliği,
- Diplomatik destek ve
- Misillemeye karşı hazırlık

gibi faktörler önemli rol oynamıştır. Bu olayda, nükleer güce ve caydırıcılığa sahip bir ülke olan Kuzey Kore'nin, sahip olduğu kısıtlı siber güç yeteneklerini caydırıcılık maksadıyla etkinlikle kullanarak hedefine ulaştığı anlaşılmaktadır.

Elbette ki siber caydırıcılık, klasik askeri caydırıcılık veya nükleer caydırıcılık kadar kolay ve kesin kural veya esaslarla açıklanamaz. En basit açıklama olarak, nükleer caydırıcılık, 'nükleer silahlara sahip taraflar arasında, hedeflerin ve saldırı etkileriyle sonucunun belli olduğu' bir durumda söz konusudur. Buna karşın siber caydırıcılıkta; güvenlik ve savunmanın yüksek maliyeti yanında, saldırı ve taarruz yetenekli siber güce sahip olmak kolay ve maliyeti düşük olmakla birlikte, günümüz şartlarında hedefin belirlenmesinin çok büyük zorluklarının bulunduğu, misilleme saldırısının başarısızlıkla sonuçlanmasının ve aynı saldırı eyleminin tekrarlanmasının zorlukları gibi olumsuzluklar [7] yadsınamaz gerçeklerdir.

Yine siber caydırıcılıkta saldıranın gerçek gücü bilinememekte, karşı tarafın değerli varlıklarının risk altında tutulup tutulamayacağı yani saldırı sonrası verilebilecek hasar ve zararlar konusunda da önceden belirgin tespitlerde bulunmak günümüz şartlarında mümkün görülememektedir. Bu ve benzeri konularda belirsizliklerin olması, siber caydırıcılığa asimetrik saldırı/savaş (zayıf tarafın daha güçlü tarafa karşı onun zayıf taraflarından da istifade ederek farklı taktik veya rastgele/belirsiz yöntemlerle yürüttüğü mücadele) [5] özelliği ve imkânları sağlamakta ve etkisini daha da artırmaktadır.

## IV. SONUÇ VE DEĞERLENDİRME (CONCLUSION AND EVALUATION)

Bilgisayar ve iletişim teknolojilerinin geliştiği ve hızla gelişmeye de devam ettiği günümüzde, bilgisayar ve iletişim teknolojilerinin kazandırdığı siber gücün sağladığı imkân ve kolaylıklardan etkin şekilde yararlanmak için siber güvenliğin önemi anlaşılmış, siber güvenlik ve savunmanın etkin şekilde sağlanması için de çalışmalar aralıksız sürdürülmektedir.

Siber saldırı olayları analiz edildiğinde, başarılarının, etkilerinin ve verilen zararların yüksek olmasında temel nedenlerinin;

- Savunmaya yönelik ulusal veya yerel strateji ve politikaların bulunmaması, olsa bile yeterli olmaması veya etkin uygulanmaması,
- Teknoloji ve altyapı yetersizlikleri,
- Uluslararası boyut içerdikleri için karşılaşılabilecek olumsuzluklardan dolayı uzak durulması veya buna hazır bir yapı kurulamaması,
- Saldırılara karşı bilgi sahibi ve hazırlıklı olmama,
- Yetenek ve yeterliliği yüksek personel veya ekip azlığı,
- Kullanıcıların eğitim ve farkındalık eksikleri,
- Kurum ve kuruluşlar arasında koordinasyon ve işbirliğin olmaması

şeklinde sıralanabilir.

Etkin bir siber caydırıcılık için değerlendirmeler ve öneriler aşağıda maddeler halinde verilmiştir.

1. Her şeyden 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.

2. Tarihte sadece savunmayla hiçbir zafer kazanılmamış, karşı saldırı ve taarruz yeteneği de kazanılmasının ve kullanılmasının gerekli ve kaçınılmaz bir zorunluluk olduğu anlaşılmıştır. Yine tarihte en iyi savunmanın taarruz olduğunu vurgulayan özdeyişi kanıtlayan çok sayıda muharebe yaşanmıştır. Bunu siber güvenlik ve siber savaşa da uygulamak mümkündür.

3. Savaşın maksatlarından birisi, istek veya istekleri karşı tarafa zorla kabul ettirmektir ve M.Ö. 500'lü yıllarda yaşamış olan Sun Tzu'ya göre savaşta amaç kazanmak olsa da, en mükemmeli hep kazanmak olmayabilir. "En iyisi savaşmadan baş eğdirmektir!."[26] Bu özdeyişten de hareketle, söz konusu siber savaş olduğunda, saldırganı siber saldırıdan veya savaştan caydırmak, yani 'siber caydırıcılık' en iyisi olabilir.

4. Siber caydırıcılığı sağlamak için; saldırılara karşı önceden etkili bir siber savunmayla hazır olarak karşı koymak, etkin bir saldırı ve taarruzla hedefe ulaşma gücünde olmak gerekir. Uygulamada siber savunma eylemi için önleyici bir yaklaşım izlenmelidir; çünkü rakip ilk saldırıyı yaparsa, daha güçlü savunma veya karşı saldırı yeteneği devre dışı bırakılabilir [24].

5. Ancak savunma için de, taarruz için de, kısaca savaşta başarı için vazgeçilmez olan konu ise istihbarattır. Sun Tzu bunun önemini "Düşmanı ve kendinizi iyi biliyorsanız, yüzlerce savaşa bile girseniz sonuçtan emin olabilirsiniz."[26] özdeyişi ile açıklamıştır. Siber güvenlik, savaş ve caydırıcılık için siber istihbarata önem verilmelidir.

6. Siber saldırılara karşı konulacağını ve bir saldırı durumunda bunun saldırgana misliyle ödetileceğini göstererek onu saldırıdan caydırmak, bütün bunlar için de etkin bir siber istihbarat yeteneğine sahip olmak, etkili bir siber istihbarata dayanan siber savunma, taarruz ve caydırıcılık yetenekleri toplamı siber güçle bunu desteklemek şarttır.

7. Etkili bir siber güç için özellikle bilgi, bilgisayar ve iletişim konularında milli teknolojilere sahip olmak, milli teknolojilere sahip olunamayan alanlarda sahip olunan teknolojilere hâkim olmak gerekmektedir. Askeri alanda bir silah

milli olmasa da satın aldığınız da ona hâkim olmanız kolay ve başkasının etkisi olmadan o silahı kullanmak sizin elinizdedir. Ancak bilişim teknolojileri milli değilse bunu söylemek zordur. Bu maksatla araştırma ve geliştirme çalışmaları başta olmak üzere teknolojik altyapı geliştirmeleri büyük önem arz etmektedir.

8. Siber gücün geliştirilerek artırılması ve etkin şekilde kullanılması için kullanıcıların yetiştirilmesi ve farkındalıklarını artıracak eğitimler verilmesi çok önemlidir. Bu maksatla özellikle siber güvenlik konularında uzman kadroların oluşturulması, her seviyede eğitim ve öğretimin planlanması ve yaygınlaştırılması gerekmektedir. Kullanıcıların eğitimleri, siber güvenlik ve savunma için önemli olduğu kadar, gerektiğinde saldırı ve taarruz için de kolaylıkla yönlendirilmeleri ve bazı görevlerin etkinlikle yerine getirilmesi için de önemlidir.

9. Siber gücün artırılması ve siber saldırılara karşı etkin güvenlik ve korunma için her alanda koordinasyon ve işbirliği gerekir. Siber tehditlere devlet kurumlarının, özel sektörün veya bireylerin tek başlarına karşı koyması mümkün değildir. Bunun için bütün devlet kurum ve kuruluşları ile özel sektör arasında etkin iş birliği ve koordinasyon sağlanmalıdır. Kamu veya özel, bütün kurum ve kuruluşlar da siber güvenliği önemseyip üzerlerine düşen görev sorumlulukları tam olarak yerine getirmelidir.

10. 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.

11. Siber suçlulara müdahale edilmesi, siber saldırılara karşı konulması ve aktif bir siber savunma gerçekleştirilebilmesi için, tüm kamu kurum ve kuruluşları ile özel girişimcilerin görev ve sorumlulukları ile birbirleriyle olan koordinasyon ve ilişkileri açık ve belirgin bir şekilde, yasalarla ortaya konmalı ve bu yasalar kararlılıkla uygulanmalıdır.

12. Bilgi ve iletişim teknolojileri ve özellikle internet sayesinde ülkeler arası etkileşimin boyutu da derinleşmiştir. Aynı zamanda, bir ülkede ortaya çıkan zararlı bir yazılım da anında tüm dünyayı etkisi altına alabilmektedir. Bu nedenle, ülkelerin siber saldırılara karşı işbirliği yapmaları ve bu ilişkileri geliştirmeleri suçluların yakalanması ve haklarında gecikmeksizin yasal işlem yapılarak cezalandırılması, aynı zamanda caydırıcılık sağlaması yanında saldırıların azalmasını da sağlayacaktır.

13. 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"[27] ve siber gücü kullanma yetkilerinin tek bir merkezde toplanması kısa sürede olumsuzlukların en aza indirilerek başarının artırılmasını da sağlayacaktır. Bu kapsamda siber savunma ve taarruz yetenekli bir siber ordu teşkilatlanmasına gidilmesi, bütün bilgi, bilgisayar ve iletişim sistemi kullanıcısı olan vatandaşların bilinçlendirilmesi ve farkındalıklarının artırılarak gerektiğinde topyekûn mücadelede kolaylıkla yönlendirilebilmeleri için örgütlenmesi, siber güç olmak ve siber güçle caydırıcılık sağlayabilmek için en önemli faktörlerden birisidir.

14. Türkiye Cumhuriyeti Başbakanının 22 Kasım 2016 günü Bilişim Zirvesi'nde, siber güvenlikle ilgili yaptığı ve basına da yansıyan açıklamada "Siber saldırılarda caydırıcılığın arttırılacağını, saldırılardan sadece korunulmayacağını ayrıca caydırıcılık için ek önlemler alınacağını…"[28] ifade etmesi Türkiye'de siber güvenlik yanında siber caydırıcılık konusunda da çalışmaların başladığını göstermektedir. Bu hedefin, kısa sürede hayata geçirilmesi gerekmektedir.

15. 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 [29]. 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.

16. Siber caydırıcılıkta temel esas ve önemli olan siber saldırıların/savaşın doğru zamanda, doğru hedefe yönelik, doğru teknik ve yöntemlerle yapılmasıdır. Uygulanması zor olmakla birlikte, ülkemizin siber güvenliği ve savunmasına daha fazla katkı sağlaması yanında, maliyet ve kullanım kolaylıkları yanında asimetrik saldırı/savaş imkânı da sağlaması nedeniyle, '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, stratejiler geliştirilmesi ve geleceğe dönük planlamalar yapılarak gecikmeksizin

uygulamaya konulması gereken çok önemli bir konu olduğu düşünülmektedir.

Sonuç olarak; Türkiye'de her alanda yeni başarılı çalışmalar yapılsa da, bu alanda da yeni çalışmalar yapılması, konunun farklı boyutlarıyla ele alınması, bu konuda tezler üretilmesi, caydırıcı ürün ve teknolojilerin geliştirilmesi, bu konuya gerekli yatırımların yapılması ve en önemlisi insan kaynağı olarak siber alanda caydırıcı güçlerin oluşturularak geliştirilmesinin ülke siber savunması ve güvenliğine büyük katkı sağlayacağı değerlendirilmektedir.

**TEŞEKKÜR (ACKNOWLEDGEMENT)**

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

**KAYNAKLAR (REFERENCES)**

**[1]** J. S. Nye, Cyber Power, http://belfercenter.ksg.harvard.edu/files/cyber-power.pdf, (Erişim: 18 Şubat 2016).

**[2]** TDK Büyük Türkçe Sözlük, Caydırıcılık, http://www.tdk.gov.tr/index.php?option=com_bts, (Erişim:13 Şubat 2016).

**[3]** Z. Kızmaz, Ceza veya Kriminal Yaptırımın Suç Oranları Üzerindeki Caydırıcı Etkisi, Afyon Kocatepe Üniversitesi Sosyal Bilimler Dergisi, Cilt:7, Afyonkarahisar, 2005.

**[4]** H. Özdemir, Uluslararası İlişkilerde Güç-Çok Boyutlu Bir Değerlendirme, Cilt:63, Sayı:3, Ankara Üniversitesi SBF Dergisi, Ankara, 2008.

**[5]** M. T. Akad, Modern savaşın Temel Kavramları, Kitap Yayınevi, Ankara, 2011.

**[6]** L.H. Wei, The Challenges of Cyber Deterrence, Pointer, Journal of The Singapore Armed Forces Vol.41 No.1, Singapur, 2015.

**[7]** M. C. Libicki, Cyberdeterrence and Cyberwar, RAND Corporation, ABD, 2009.

**[8]** H. Çiftçi, Her Yönüyle Siber Savaş, TÜBİTAK Yayınları. Ankara, 2013.

**[9]** G. Canbek, Ş. Sağıroğlu, Bilgi, Bilgi Güvenliği ve Süreçleri Üzerine Bir İnceleme, Politeknik Dergisi, Cilt: 9 Sayı: 3, Ankara, 2006.

**[10]** M. Şenol, Siber Savaş, Silahlı Kuvvetler Dergisi, Gnkur. ATASE Yayınları. Sayı:413, Ankara, 2012.

**[11]** P. W. Singer, A. Friedman, Siber Güvenlik ve Siber Savaş, Buzdağı Yay. Ankara, 2015.

**[12]** Milliyet Gazetesi, Kuzey Kore'yi kızdıran Sony filmi geri çekildi, http://www.milliyet.com.tr/kuzey-kore-yi-kizdiran-sony-filmi/dunya/detay/1986604/default.htm, (Erişim: 15 Şubat 2016).

**[13]** Anadolu Ajansı, ABD'deki siber saldırı 7 milyar dolarlık zarara yol açtı, http://xn--anadoluajans-d5b.gov.tr/tr/dunya/abd-deki-siber-saldiri-7-milyar-dolarlik-zarara-yol-acti/672549, [Erişim: 01Şubat 2017).

**[14]** Vatan Gazetesi, Hackerların En Büyük Darbesi Erzincan'da olmuş, http://www.gazetevatan.com/hackerlar-in-en-buyuk-darbesi-erzincan-da-olmus-705841-teknoloji/, (Erişim: 20 Şubat 2016).

**[15]** Kaynak Elektrik Dergisi, Elektriğin Mumla Arandığı Gün, http://issuu.com/elekrikdergisi/docs/mart, (Erişim: 18 Şubat 2016).

**[16]** E. Başaran, Elektrik Kesintisi Gerçekten Siber Saldırı İşi mi, http://www.radikal.com.tr/yazarlar/ezgi-basaran/elektrik-kesintisi-gercekten-siber-saldiri-isi-mi-1326537/, (Erişim: 19 Şubat 2016).

**[17]** Hürriyet Gazetesi, TEİAS Elektrik Kesintilerini Engellemek İçin İhaleye Çıkıyor, http://www.hurriyet.com.tr/teias-elektrik-kesintilerini-engellemek-icin-ihaleye-cikiyor-30001794, (Erişim: 20 Şubat 2016).

**[18]** Hürriyet Gazetesi, Onlar Saldırdı Biz Fişi Çektik, http://www.hurriyet.com.tr/onlar-saldirdi-biz-fisi-cektik-40030151 (Erişim: 13 Şubat 2016).

**[19]** HaberTürk Tv. haberturk.com/saglik/haber/1241415-anonymous-turkiyedeki-saglik-kayitlarini-caldi-mi, (Erişim: 20 Mayıs 2016).

**[20]** R. A. Clarke, R. K. Knake, Siber Savaş, İKÜ Yayınları, İstanbul, 2010.

**[21]** U. Ermiş, B. Özdal, Martin C. Libicki'nin 'Siber Caydırıcılık' Kavramının Nükleer Caydırıcılık Olgusu İle Karşılaştırılmalı Analizi, 6.Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansı-2013, http://www.iscturkey.Org/s/2226/i/2013-paper51.pdf, (Erişim: 20 Şubat 2016).

**[22]** S. Gorman, J.E. Barnes, Cyber Combat: Act of War,http://www.wsj.com/articles/SB10001424052702304563104576355623135782718.

**[23]** D. Denning, Cybersecurity's next phase: Cyber-deterrence, https://theconversation.com/ cyber securitys-next-phase-cyber-deterrence-67090, ((Erişim: 25 Mart 2017).

**[24]** V. Veebel, Baltic States and Cyber Deterrence: Taking or Losing Initiative against Russia?, http://www.fpri.org/article/2017/01/baltic-states-cyber-deterrence-taking-losing-initiative-russia/, (Erişim: 26 Mart 2017).

**[25]** BBC Türkçe Servisi, Kuzey Kore-ABD arasında siber saldırı gerilimi, http://www.bbc.com/turkce/haberler/2014/12/141219_kuzey_kore_obama, (Erişim: 15 Şubat 2016).

**[26]** Sun Tzu, Savaş Sanatı, Türkiye İş Bankası Kültür Yayınları, İstanbul, 2014.

**[27]** 2016-2019 Ulusal Siber Güvenlik Stratejisi ve Eylem Planı, T.C. UDHB, Ankara, 2016.

**[28]** 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).

**[29]** E. Mütercimler, Geleceği Yönetmek ve Kazanmak için Stratejik Düşünme, Alfa Yayınları, İstanbul, 2016.