Siber Caydırıcılık ve Türkiye'nin İmkân ve Kabiliyeti

Y. İduğ, F. Çalışkan, T. Güler

***Özet*— Bilgi teknolojilerinin günlük yaşamın vazgeçilmez bir parçası olması, kamu ve özel kurumların -özellikle finans, enerji ve güvenlik- faaliyetlerini bilgi sistemleri üzerinden yürütmesi, siber güvenlik kavramını hayati kılmaktadır. Tehdidin büyüklüğü ve gerçekleşme ihtimalinin yüksek oluşu devletleri kritik savunma, finans ve ulaşım altyapılarına yapılabilecek olası siber saldırılara karşı caydırıcı stratejiler geliştirmeye yöneltmektedir. Türkiye de diğer devletler gibi bilgi sistemlerinin güvenliğini sağlamak maksadıyla çalışmalar yapmaktadır. Bu çalışmada, siber caydırıcılık kavramı ile Türkiye'nin mevcut siber caydırıcılık kabiliyeti incelenmiş ve Türkiye'nin siber savunma ve taarruz alanında atması gereken adımlar ele alınmıştır.**

***Terimler* — Caydırıcılık, Nükleer Caydırıcılık, Siber Caydırıcılık.**

Abstract— Establishing cyber security is more important than ever because information technologies have become essential part of daily life, and public and private activities –particularly on finance, energy, and security- have been carried out via information systems. Since the threat is tremendous and most likely to occur, states are forced to develop deterrence strategies against any possible cyber attack to their crucial defense, finance, and transportation infrastructures. Considering the criticality of ensuring cyber security, Turkey has initiated a process of strengthening the security of its information systems. This work examines the concept of cyber deterrence, cyber deterrence capability of Turkey, and finally the necessary measures should be taken by Turkey to deter cyber threats.

***Keywords* — Deterrence, Nuclear Deterrence, Cyber Deterrence.**

I. GİRİŞ

BİLGİ teknolojilerinin günlük yaşantımızda yaygın olarak yer alması beraberinde bilgi sistemlerinin güvenliğini önemli hâle getirmiştir. Dünya genelinde bilgisayar kullanımı hızla artmaktadır. 2011 yılında 1,6 milyar bilgisayar kullanılırken bunun 2016'da 2,45 milyara ulaşması beklenmektedir [1]. Yedi milyar insanın yaşadığı dünyamızda altı milyar insan da cep telefonu kullanmaktadır [2].

Yavuz İduğ, Harp Akademileri Komutanlığı, Kara Harp Akademisi, Yeni Levent, 34330, Pbx: +90 212 398-0100, İstanbul-Türkiye, e-mail: yavuzidug@gmail.com.

Ferhat Çalışkan, Harp Akademileri Komutanlığı, Kara Harp Akademisi, Yeni Levent, 34330, Pbx: +90 212 398-0100, İstanbul-Türkiye, e-mail: fcaliskan10@gmail.com.

Talip Güler, Harp Akademileri Komutanlığı, Kara Harp Akademisi, Yeni Levent, 34330, Pbx: +90 212 398-0100, İstanbul-Türkiye, e-mail: talipguler99@gmail.com.

Devletlerin ve içinde yaşayan bireylerin bilgi sistemlerine olan bağımlılıkları onları siber saldırılara karşı hassas duruma getirmektedir. Bir devlete karşı yapılmış örgütlü ilk siber saldırının örneğini gördüğümüz 2007 yılında Estonya'ya karşı gerçekleştirilen botnet istilası, gerekli siber savunma tedbirlerinin alınmadığı ülkelerde kamu hizmetleri ile finans ve medya faaliyetlerinin bu tip saldırılara karşı ne kadar hassas olduğunu göstermekte ve devletleri siber savunma ve caydırıcılık stratejileri geliştirmeye teşvik etmektedir.

II. CAYDIRICILIK

Caydırıcılık; bir devlet veya topluluğun, başka bir devlet veya topluluğun aleyhine olabilecek hareketlerden sakınması için gerekli tedbirleri alması olarak tanımlanabilir. Caydırıcılığın; belirli bir menfaati koruma niyetinin belirtilmesi ve bu menfaati savunmak için gerekli imkân ve kabiliyetin gösterilmesi olmak üzere iki temel unsuru bulunmaktadır [3]. Bu kapsamda caydırıcılık, bir bakıma anlaşmazlığın tırmanarak askeri kuvvet kullanımını gerektirmesine engel olur.

Uluslararası güvenlik literatüründe caydırıcılığın esirgeme (deterrence by denial) ve misilleme (deterrence by retaliation) olmak üzere iki yönü bulunmaktadır. Sağlam kalelerin inşa edildiği ve topun muharebe sahasında henüz yerini almadığı ortaçağda hasmın saldırılarını boşa çıkarmasından dolayı caydırıcılığın esirgeme yönü ağır basmaktayken, nükleer silahların hüküm sürdüğü ve bunlara karşı savunmanın imkânsızlaştığı Soğuk Savaş boyunca caydırıcılığın misilleme yönü ön planda olmuştur [3]. Ancak, hem Soğuk Savaş'ın hatıralarımızda yer alması hem de bu dönemde caydırıcılık ile ilgili üretilen politikaların fazlalığı nedeniyle caydırıcılık kavramı daha çok literatürde nükleer caydırıcılık olarak yer almaktadır.

III. SİBER CAYDIRICILIK

Siber caydırıcılığın önemi konusunda uzmanlar arasında bir fikir birliği bulunmamaktadır. Clarke'ın da başını çektiği kimi ulusal güvenlik uzmanları siber caydırıcılığın siber savaşları önleyemeyeceğini belirtmektedir. Bu uzmanlara göre; nükleer savaşta her iki tarafın da taarruz kabiliyeti bilindiğinden ve savaşın sonucunda büyük olasılıkla dünyadaki yaşamın yok olacağı düşünüldüğünden uluslararası ilişkilerde nükleer caydırıcılık etkilidir. Ancak, siber savaşta saldırının gücü bir sır olarak kalmaya devam edeceğinden ve etkin bir savunma kurma olasılığı bulunmasından dolayı nükleer savaşı engelleyen güç olan caydırıcılık bu uzmanlara göre siber savaşta bulunmamaktadır [4].

Siber silahların nükleer silahlar gibi kullanılamayacağı bir gerçektir. Nükleer silahların teşhiri bir caydırıcılık etkisine sahipken siber silahların teşhiri potansiyel hasımların bu teknolojiyi çalmalarına ve/veya siber savunmalarını bu silahlara karşı sağlamlaştırmalarına neden olacağından siber taarruz yeteneğini işe yaramaz kılmaktadır [5]. Ancak, siber

caydırıcılığı nükleer caydırıcılık ile mukayese eden uzmanlar konuyu Soğuk Savaş teorileri ile ele alarak caydırıcılığın misilleme dışında esirgeme yönünün de olduğunu göz ardı etmektedirler. Nükleer caydırıcılık misilleme odaklıyken siber caydırıcılık daha çok esirgeme odaklıdır. Siber caydırıcılıkta, potansiyel saldırganların hedeflerine ulaşmada başarısız olacaklarına ikna edilerek harekete geçmekten vazgeçmeleri esas alınır [6].

Siber kabiliyet yalnız başına bir caydırıcılık etkisi oluşturabileceği gibi ekonomik ve diplomatik güç, konvansiyonel ve nükleer kabiliyetler ile de beraber bir etki oluşturabilir. Şekil 1'de belirtildiği üzere siber etki yalnız kullanıldığında şiddet olarak ekonomik ve diplomatik yaptırımlardan daha yüksek seviyede olacakken, konvansiyonel ve nükleer etkiden daha düşük olacaktır [3]. Bir devlet beliren bir tehdidi yok etmek maksadıyla diplomatik yaptırımlardan nükleer güç kullanımına kadar şiddeti değişen geniş bir yelpazede karşılık verecektir.

Şekil 1. Güç ve Kabiliyetlerin Şiddet Hiyerarşisi.

Nükleer bir saldırının çok büyük yıkımlara sebep olacağı muhakkaktır. Nükleer tesisleri kontrol eden sistemlere yönelik bir siber saldırı da benzer bir etki gösterecek ve hedeflenen devlete büyük bir darbe vuracaktır. Bu açıdan siber yeteneği nükleer bir saldırıyı tamamlayıcı bir unsur olarak görmekteyiz.

Bunun yanında siber kabiliyet diğer kabiliyetleri de destekleyici bir unsur olarak kullanılabilir. Nükleer bir saldırı ile eş zamanlı olarak yapılacak etkili bir siber saldırı hazırlıksız yakalanan hedefin bilgi sistemlerini sekteye uğratacak ve misilleme yapmasına engel olabilecektir.

Kritik altyapı sistemlerinin imhasına yönelik yeterli büyüklükteki siber saldırıya uğrayacak bir devletin siber misilleme yapabilmesi için on yıla varabilecek uzun bir zaman gerekecektir [7]. İran nükleer tesislerinde fiziksel hasar meydana getiren Stuxnet virüsü belki de bu tür saldırıların başlangıcını oluşturmaktadır. Bundan dolayı, siber savunma yeteneği olmaksızın siber taarruz kabiliyetleri işe yaramayacaktır.

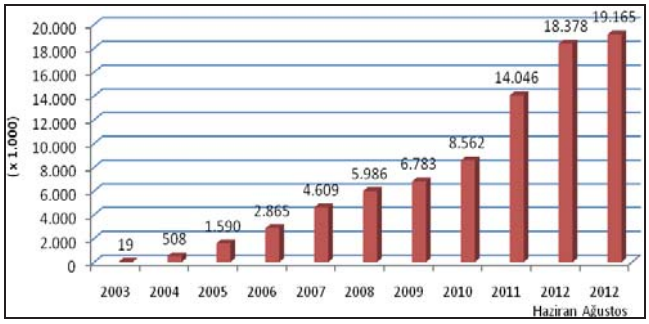
Siber caydırıcılığa yapılan en büyük eleştiri, bir siber saldırının nereden gerçekleştiğini bulmanın güç oluşudur. Siber savunma kabiliyeti yüksek olduğu müddetçe siber saldırılar boş çaba olarak görülecek ve bu yola başvurulmayacaktır. Böylece siber savunma kendi başına bir caydırıcılık sağlayacaktır. Yine Stuxnet örneği göstermiştir ki, hedefte büyük tahribata yol açmayan siber saldırılar hedefin güvenlik açıklarını görmesini sağlayarak bu açıklıkları gidermesine olanak verecek ve bir sonraki benzer saldırıyı boşa çıkaracaktır.

IV. TÜRKİYE'NİN SİBER CAYDIRICILIK KABİLİYETİ

"Enerji üretim ve dağıtım sistemleri, telekomünikasyon altyapısı, finansal servisler, su ve kanalizasyon sistemleri, güvenlik servisleri, sağlık servisleri ve ulaştırma servisleri en başta gelen kritik altyapılardır, bunların üzerinde çalıştıkları bilgi sistemleri de kritik bilgi sistem altyapılarıdır" [8]. Örgütlü olarak yönlendirilen siber saldırıların öncelikli hedefi kritik altyapılar olacağından Türkiye'nin de kritik altyapıları siber tehdit altındadır.

Artan şekilde teknolojiye olan bağımlılık, kamu ve özel sektörün yaygın olarak internet üzerinden hizmet vermeleri Türkiye'nin siber saldırılara olan hassasiyetini artırmaktadır.

Türkiye'de 2002 yılında geniş bant erişim abone sayısı 100 binin altındayken, 2012'de bu rakam 19 milyon kişiyi geçmiştir (Bakınız Şekil 2). Bunun yaklaşık 11 milyonu mobil internet kullanan abonelerdir. Bu da toplamda Türkiye'de 50 milyon internet kullanıcısı olduğuna göstermektedir. Mobil internet abone sayısı da son bir yılda yüzde 80'in üzerinde artmıştır. Türkiye'de cep telefonu abone sayısı da 67 milyona ulaşmıştır. Yaklaşık 39 milyon 3G abonesi bulunmaktadır. Cep telefonu kullananların içinde yüzde 58 olan bu oran, yüzde 30 olan Avrupa ortalamasının çok üzerindedir [9].



Şekil 2. Genişbant İnternet Abone Sayısındaki Gelişim [10].

Türkiye'nin bilgi teknolojilerine olan bağımlılığı onu siber saldırılara karşı hassas duruma getirmektedir. Bu hassasiyeti gidermek maksadıyla 20 Ekim 2012 tarihinde yürürlüğe giren Ulusal Siber Güvenlik Çalışmalarının Yürütülmesi, Yönetilmesi ve Koordinasyonuna İlişkin Bakanlar Kurulu Kararıyla Genelkurmay MEBS Başkanı ve MSB müsteşarının da üyesi olduğu, Ulaştırma Denizcilik ve Haberleşme Bakanının başkanlık ettiği Ulusal Siber Güvenlik Kurulu oluşturulmuştur [11].

Kara, deniz, hava ve uzay harekât alanlarının yanında, yeni bir harekât alanı olarak ortaya çıkan siber ortama ilişkin yetenekleri geliştirmek maksadıyla 2012 yılında TSK Siber Savunma Merkezi Başkanlığı kurulmuştur [12].

Bu kapsamda siber tehditleri önleyerek, gelişmiş siber savunma ikaz ve tepki sistemlerine sahip güçlü bir merkezi siber savunma yeteneği kazanmak hedeflenmektedir. TSK Siber Savunma Merkezi Başkanlığı; Ulaştırma, Denizcilik ve Haberleşme Bakanlığı, TÜBİTAK ve diğer kamu kurumları ile koordineli olarak faaliyetlerini icra etmektedir. Ayrıca, NATO ile eşgüdüm içerisinde görevlerini ulusal ve uluslararası alanda yürütmektedir [13].

Mevcut duruma bakıldığında siber taarruz ile ilgili olarak herhangi bir yetenek geliştirme çalışmasının olmadığını görmekteyiz. Siber savunma konusunda ise devlet bünyesinde çalışmalar ancak 2012 yılında başladığından tecrübe eksikliği bulunmaktadır. Siber savunma alanında uzman personelin yetişmesi için en az beş yıl gerektiği [13] değerlendirildiğinde Türkiye'nin siber savunma konusunda daha yolun başında olduğu söylenebilir.

Siber güç siber savunma ve siber taarruzun birleşiminden oluşmakta ve siber caydırıcılık da siber güç ile doğru orantılı olarak ele alınmaktadır. Siber konusunda tecrübeli devletlere baktığımızda siber savunma ve taarruzun ayrı ayrı ele alındığını görmekteyiz. Savunma yapan personel ile taarruz yapacak personelin profillerinde de farklılık bulunmaktadır. Siber savunma yapan personel belli kurallar çerçevesinde çalışan bir özellik gösterirken, siber taarruz yapan personelin kuralların sınırı zorlayan kişilik özellikleri gösterdikleri kabul edilmektedir [13]. Bundan dolayı siber savunma ve taarruz için gerekli insan gücünün temininde siber savunma ve taarruz ayrı ele alınmalıdır.

Türkiye'nin siber hassasiyetleri yüksektir, fakat siber savunma konusunda ise daha yolun başındadır. Siber caydırıcılık kabiliyetini artırması için Türkiye'nin siber savunma kabiliyetini geliştirmesi, hassasiyetlerini gidermesi ve siber taarruz kabiliyeti elde etmesi gerekmektedir.

V. SONUÇ

Bilgi teknolojilerinin günlük hayatın vazgeçilmez bir parçası olduğu ve siber uzayın muharebe sahasının yeni bir boyutunu oluşturduğu bu çağda devletlerin ulusal güvenliklerini sağlayabilmeleri için siber caydırıcılık kabiliyetine sahip olmaları elzemdir.

Siber caydırıcılığın esirgeme ve misilleme olmak üzere ilki savunmaya, diğeri taarruza yönelik olmak üzere iki yönü bulunmaktadır.

Türkiye siber kabiliyetlerinin bir devlet çatısı altında koordineli olarak yönetilmesi için 2012 yılından itibaren çalışmalara başlamış ve siber hassasiyetlerin belirlenerek giderilmesi konusuna odaklanmıştır. Türkiye'nin siber gücü bir bütün olarak ele alması ve siber savunmanın yanında siber taarruz kabiliyetini de geliştirmesi siber caydırıcılık kabiliyeti elde edebilmesi bakımından önemlidir.

KAYNAKLAR

[1] Computer Industry Almanac Inc. http://www.c-i-a.com/pr02012012.htm. Erişim Tarihi: 08 Temmuz 2013.

[2] UN News Centre. http://www.un.org/apps/news/story.asp?NewsID=44452. Erişim Tarihi: 08 Temmuz 2013.

[3] M.L.Libicki, Cyberdeterrence and cyberwar. RAND Corporation, 2009.

[4] R. Clarke, R. Knake, Siber savaş: Ulusal güvenliğe yönelik yeni tehdit. İKÜ Yayınevi, 2011, s. x, 99.

[5] S. Weiner, Searching for cyber-deterrence. Center for Strategic and International Studies, 26 Kasım 2012.

[6] A. Lupovici, Cyber warfare and deterrence. Military and Strategic Affairs, 3Aralık 2011, s. 51.

[7] C. Wilson, Botnets, Cybercrime, and Cyberterrorism: Vulnerabilities and Policy Issues for Congress. CRS Report for Congress. 2008, s.18.

[8] H. Bahşi, B. Karabacak, Ü. Tatar, Sayısal Ortamda Savunma ve Bilgi Güvenliği Yol Haritası, Bilişim Kurultayı, Ankara, 2009.

[9] Türkiye Avrupa birincisi oldu. http://www.sabah.com.tr/Teknoloji/Haber/2012/08/21/turkiye-avrupa-birincisi-oldu. Erişim tarihi:11Temmuz 2013.

[10] Genişbant Hizmetlerinde Şeffaflık Düzenlemeleri ve Hizmet Kalitesi Uygulamaları. http://www.tk.gov.tr/kutuphane_ve_veribankasi/raporlar/arastirma_raporlari/dosyalar/genisbant_hizmetlerde_seffaflik_ve_hizmet%20kalitesi-05_10_2012.pdf. Erişim Tarihi: 10 Temmuz 2013.

[11] Bilgi ve Teknoloji Yüksek Kurulu 25. Toplantısı Hazırlık Dosyası. http://www.tubitak.gov.tr/sites/default/files/btyk25_gelismeler.pdf Erişim Tarihi: 09 Temmuz 2013.

[12] C.Çatal, TSK'dan siber savunma merkezi. http://www.hurriyet.com.tr/teknoloji/22405874.asp Erişim tarihi:11Temmuz 2013.

[13] Ü. Tatar, Geleceğin muharebelerinde siber savaş boyutu. HAK Geleceğin Harekât Ortamı ve Harp Teknolojileri Paneli. 2013, s.65.

Yavuz İduğ lisans eğitimini 2003 yılında Uluslararası İlişkiler ve Liderlik & Yönetim dallarında ABD Kara Harp Okulu, West Point'te tamamlamıştır. Yüksek lisans eğitimini 2011 yılında ABD Deniz Kuvvetleri Yüksek Lisans Okulu (Naval Postgraduate School)'nda Mali Yönetim dalında yapmıştır. Hâlihazırda İstanbul'da Kara Harp Akademisi'nde öğrenim görmektedir. Uluslararası ilişkiler, liderlik & yönetim ve siber savaş konularına ilgi duymaktadır.

Ferhat Çalışkan lisans eğitimini 2003 yılında Sistem Mühendisliği dalında Kara Harp Okulu'nda tamamlamıştır. Yüksek Lisans Eğitimini 2011 yılında ABD Deniz Kuvvetleri Yüksek Lisans Okulu (Naval Postgraduate School)'nda Güvenlik İncelemeleri-Orta Doğu dalında yapmıştır. Hâlihazırda İstanbul'da Kara Harp Akademisi'nde öğrenim görmektedir. Uluslararası ilişkiler, oyun teorisi, Orta Doğu çalışmaları ve siber savaş konularına ilgi duymaktadır.