Siber Güvenliğin Taarruzi Boyutu ve Uluslararası Hukuk Kurallarının Uygulanabilirliği

Hakan Şentürk, C.Zaim Çil, Şeref Sağıroğlu

***Özet*— Son on yılda, kaynağında bizzat devletlerin ya da devlet-destekli aktörlerin bulunduğu geniş çaplı siber saldırılar yaşandığı ve çok sayıda ülkenin alenen veya gizli olarak taarruzi siber yetenekler geliştirdiği açık olarak görülmektedir. Bu çalışmada; özellikle Ülke olarak siber güvenlik stratejimizin ve ilgili eylem planlarının belirlenmesi sürecinde; taarruzi siber güvenlik yetenekleri geliştirmenin öneminin vurgulanması maksadıyla; uluslararası hukuk kurallarının siber güvenliğe uygulanma durumu incelenmiş, ABD'nin bu alanda izlediği politika ve faaliyetleri ele alınmış, Türkiye'deki mevcut durum değerlendirilerek yapılması gerekenler sunulmuştur.**

***Anahtar Kelimeler*—Siber güvenlik, siber hukuk, siber savaş, taarruzi siber güvenlik**

***Abstract*— In the last decade, it has become evident that states or state-sponsored actors are involved in large scale cyber attacks and that many States have been developing offensive cyber security capabilities. In this study; in order to emphasize the criticality of developing offensive cyber capabilities, especially when the National Cyber Security Strategy and relevant action plans are being determined, the applicability of international law on to the cyber warfare has been researched, the United States's policy and activities are reviewed, current situation in Turkey is analyzed and some proposals are made.**

***Index Terms*—Cyber security, cyber law, cyber warfare, offensive cyber security**

I. GİRİŞ

Devletlerarası düzeyde ilk kez 2007 yılında gerçekleşen Estonya Siber Savaşından günümüze kadar olan dönemde, Rusya-Gürcistan (Güney Osetya Anlaşmazlığı), K.Kore-ABD, Çin-Hindistan, İsrail-Lübnan, Mısır gibi pek çok siber saldırı olayı gerçekleşmiştir. Özellikle son 3-4 yıl içerisinde yaşanan, İran nükleer tesislerinin hedef alındığı Stuxnet saldırısı ile başlayan ve onun türevleri olduğu iddia edilen, daha gelişmiş DuQu solucanı, Ortadoğu sistemleri hedef alınan Flame virüsü ve henüz ne olduğu öğrenilemeyen bir savaş başlığı taşıyan Gauss zararlı yazılımı, Suudi Arabistan'da bulunan AramCo şirketinde 30,000 iş istasyonuna zarar veren Shamoon virüsü gibi saldırılar, siber savaşların şiddetinin zamanla daha da artacağını, kullanılan saldırı teknolojilerinin daha da gelişmekte olduğunu göstermekte ve saldırıların kaynağında bizzat devletlerin ya da devlet-destekli aktörlerin bulunduğuna işaret etmektedir.

Özellikle Stuxnet, DuQu, Flame ve Gauss saldırılarının ABD açıklık veri tabanında kayıtlı bulunan ".lnk" isimli aynı açıklığı (CVE2010-2568) kullandığı, USB bulaşma, metin kodlama/çözme algoritması gibi pek çok ortak modülü paylaştığı, sonuç olarak aynı tesislerde, diğer deyişle aynı siber silah fabrikasında ve bir ya da birden fazla devlet desteğiyle üretildiği anlaşılmaktadır [1-6].

Son 10 yılda siber saldırıların gelişimi ele alındığında ilk yıllarda, basit tekniklerle organize olmayan test saldırıları, 2003 yılından itibaren ekonomik güdülerin öne çıktığı saldırılar, 2007 yılından itibaren ise botnet ve bunları kontrol eden komuta kontrol merkezleri aracılığıyla gerek saldırı sayıları ve bant genişlikleri, gerekse de gelişmiş saldırı teknikleriyle gerçekleştirilen siber saldırıların, siber savaşa doğru bir gelişim gösterdiği değerlendirilmiştir [7].

Buna paralel olarak başta ABD olmak üzere, Çin, K.Kore, İsrail, Fransa vb. çok sayıda ülkenin taarruzi siber yetenekler geliştirdiği bilinmektedir [8]. Siber güvenliğin sadece savunma stratejisi ile mümkün olamayacağı [9] bilinmekte olup ülke güvenliği adına, kara, deniz ve hava harekât alanlarında olduğu gibi siber uzayda da taarruzi yetenek geliştirmenin gerekli olduğu değerlendirilmektedir. Bu tür yeteneklerin kullanımı konusunda ise uluslararası hukuk kurallarının siber güvenliğe uygulanabilirliği konusu da üzerinde tartışılması ve çözüm bulunması gereken konuların başında gelmektedir.

Bu çalışmanın amacı; ulusal siber güvenlik stratejisinin ve ilgili eylem planlarının belirlendiği günümüzde, siber güvenliğin taarruzi boyutuna dikkat çekmek, konuya ilişkin literatürdeki uluslararası hukuk nezdinde yapılan yasal zemin tartışmalarını değerlendirmek ve barış zamanı taarruzi amaçlı yetenek geliştirmenin gerekliliği tartışmaktır.

Belirtilen amaçlarla hazırlanan bu çalışmada; uluslararası hukuk kurallarının siber güvenliğe uygulanıp uygulanamayacağı hususu incelenmiş, ABD'nin konuya ilişkin yaklaşımı ve faaliyetleri ele alınmış, Türkiye'deki mevcut durum değerlendirilerek yapılması gerekenler belirlenmiştir.

Manuscript received July 14, 2013.

Hakan ŞENTÜRK, Kara Harp Okulu Savunma Bilimleri Enstitüsü, Ankara. (Tlf: 312-414-2631; e-mail: hsenturk@hvkk.tsk.tr).

Celal Zaim ÇİL, Çankaya Üniversitesi Elektronik ve Haberleşme Mühendisliği, Ankara (e-mail: czaimcil@cankaya.edu.tr).

Şeref SAĞIROĞLU, Gazi Üniversitesi Bilgisayar Mühendisliği, Ankara (e-mail: ss@gazi.edu.tr)

II. ULUSLARARASI HUKUKUN SİBER GÜVENLİĞE UYGULANABİLİRLİĞİ

Uluslararası Hukuk'un iki ana kaynağı, örf ve adet hukuku ile yazılı kaynaklardır. Yazılı kaynaklar açısından, siber güvenlik alanında uluslararası tek sözleşme Avrupa Konseyi tarafından 2001 yılında hazırlanarak 2004 yılında yürürlüğe giren Avrupa Siber Suç Sözleşmesidir [10]. ABD'nin 2006 yılında imzaladığı, Rusya'nın ise imzaya yanaşmadığı Avrupa Siber Suç Sözleşmesinde 5 asli Siber Suç tanımlanmıştır:

- Yetkisiz erişim (illegal access)
- Yetkisiz müdahale (Illegal interception)
- Veri engelleme/karıştırması (Data interference)
- Sistem engelleme/karıştırması (System interference)
- Cihazların amacı dışında kullandırılması (Misuse of devices)

Asya Pasifik Ekonomik İşbirliği (APEC) 2002 tarihli Siber Güvenlik Stratejisi"nde, Avrupa Siber Suç Sözleşmesi, siber güvenlik alanındaki ilk çok taraflı yasal belge olarak tanınmaktadır [11].

Siber güvenliğin taarruzi boyutu ve bunun devletlerarasında kullanımı söz konusu olduğunda başvurulması gereken temel kaynak, Birleşmiş Milletler (BM) Sözleşmesidir. BM Sözleşmesi'ne göre ülkelerin kendi sınırları dışında kuvvet kullanımına dört istisna halinde izin verilmiştir. Bu istisnalardan ikisi BM'nin kuruluş yıllarına ait olduğundan günümüzde sadece iki istisnadan bahsetmek mümkündür:

a. Meşru müdafaa halinde kuvvet kullanımı (Madde 51)
b. Güvenlik Konseyi kararıyla kuvvet kullanımı (VII. Bölüm)

BM Şartı'nın 51. Maddesi meşru müdafaa hakkını şu şekilde tanımlamaktadır: "Bu Antlaşma'nın hiçbir hükmü, Birleşmiş Milletler üyelerinden birinin silahlı bir saldırıya hedef olması halinde, Güvenlik Konseyi uluslararası barış ve güvenliğin korunması için gerekli önlemleri alıncaya dek, bu üyenin doğal olan bireysel ya da ortak meşru savunma hakkına halel getirmez. Üyelerin bu meşru savunma hakkını kullanırken aldıkları önlemler hemen Güvenlik Konseyi'ne bildirilir ve Konsey'in işbu Antlaşma gereğince uluslararası barış ve güvenliğin korunması ya da yeniden kurulması için gerekli göreceği biçimde her an hareket etme yetki ve görevini hiçbir biçimde etkilemez" [12].

Görüldüğü üzere; meşru müdafaa halinde kuvvet kullanımı ancak bir ülkeye karşı "Silahlı Saldırı (Armed Attack)" söz konusu olması durumunda ortaya çıkmaktadır. Siber güvenlik alanındaki yasal zemin tartışmaları da bu alanda yapılmaktadır [13]. Geçmişte yaşanan, devlet destekli olduğu kuvvetle muhtemel siber saldırıların silahlı saldırı kapsamına girip girmeyeceği, bir saldırının silahlı saldırı sayılabilmesi için hangi şartta ve özellikte olması gerektiği üzerinde uzlaşılmış bir genel yargı bulunmamaktadır.

Stratejik ve Uluslararası Çalışmalar Merkezi uzmanı J. Lewis, bir siber saldırının silahlı saldırı kabul edilebilmesi için sonuçlarına bakılması gerektiği, eğer siber saldırı sonucu oluşturulan etki, geleneksel saldırı sonucu oluşturulan etki ile aynı ise, siber saldırının da diğeriyle aynı kurallara tabi olması gerektiğini belirtmiştir. Örneğin, deniz ablukası ile oluşturulabilecek ticaret kaybı, bir siber saldırı sonucunda da oluşturuluyorsa, bu durumda siber saldırının, silahlı saldırı olarak kabul edilmesi gerektiği ve misilleme hakkı doğurması gerektiğini belirtmektedir [14]. Bu görüşe paralel olarak ABD Dışişleri Bakanlığı Hukuk Danışmanı Harold Koh, 18 Eylül 2012 tarihinde ABD Siber Komutanlığı tarafından düzenlenen bir konferansta ilk kez konu hakkındaki ABD pozisyonuna yönelik önemli açıklamalar yapmış, siber saldırının, silahlı saldırı olarak kabul edilebilmesi için siber harekatın sonuçlandıracağı fiziksel etkinin önemli olduğu, ölüm, yaralanma yada önemli derecede etki yaratacak tahriple sonuçlanan siber operasyonların kuvvet kullanımı olarak kabul edilebileceğini ifade etmiştir [15].

Alandaki yasal boşluğu doldurmaya hizmet amacıyla Tallinn/Estonya'da bulunan NATO İşbirliğine Dayalı Siber Savunma Mükemmeliyet Merkezi öncülüğünde oluşturulan uluslararası uzmanlar grubu tarafından "Uluslararası Hukukun Siber Savaşa Uygulanması Üzerine Tallinn El Kitabı" (Tallinn Manual on the International Law Applicable to Cyber Warfare) isimli doküman hazırlanarak 2013 yılında yayımlanmıştır [16]. Doküman, geçmişte uluslararası hukuk kurallarının deniz, hava ve füze savunmasına uygulanması üzerine hazırlanan San Remo El Kitabı ve Harvard dokümanlarının oluşturulmasında izlenen yöntem takip edilerek hazırlanmış olup kuvvet kullanımı ve silahlı çatışma hukukuna ilişkin uluslararası kuralların siber savaşa uygulanma durumunu incelemek suretiyle hükümetler için siber savaş hukuku alanında bağlayıcı olmayan, çalışmaya katılan uzmanların görüşlerini yansıtan bir referans kaynak niteliğindedir.

Tallinn El Kitabı [16], siber savaşı, uluslararası hukukun iki temel prensibi olan kuvvete başvurma hakkı (jus ad bellum) ile kuvvete başvurulduğunda uyulması gereken çatışma kuralları (jus in bello) normları [17] açısından değerlendirmekte, kuvvet kullanımı seviyesinin altında kalan siber suçlar vb. kavramları kapsam dışı tutmaktadır. Ayrıca El Kitabı, siber harekatlara karşı yapılan siber harekatları temel almış; örneğin bir devletin kritik altyapılarına ya da komuta kontrol merkezine karşı başlatılan siber harekatı uluslararası hukuk açısından incelemiş, ancak benzer bir hedefe yapılan hava taarruzunu kapsam dışında tutmuştur. Bu çerçevede, El Kitabı'nda, aşağıda listelenen 7 bölüm altında, çalışmaya katılan tüm uzmanların üzerinde uzlaştığı 95 adet kural belirlenmiştir. Ana bölümlerin başlığı aşağıda verilmiştir. Bunlar:

1. Devletler ve Siber Uzay
2. Kuvvet Kullanımı
3. Genel Silahlı Çatışma Hukuku
4. Düşmanca Davranma
5. Belirli Kişi, Nesne yada Faaliyetler
6. İşgal
7. Tarafsız Kalma

El Kitabının hazırlanmasında ABD; Kanada, İngiltere ve Almanya'nın askeri dokümanlarından faydalanıldığı belirtilmiştir. Dokümanın hazırlanması üç yıl sürmüş olup,

üzerinde uzlaşıya varılamayan hususlar da not edilmiştir. Örneğin, silahlı çatışma hukuku kapsamında orantılılık prensibinin uygulanmasına yönelik; askeri ve sivil amaçların ve hedeflerin ayrılması gerektiği ve örneğin askeri veri işleyen sivil bir sunucunun askeri hedef olabileceği üzerinde uzlaşılabilmişken, savaşı destekleyen unsurların askeri hedef olması hususundaki ABD yaklaşımı benimsenmemiş, uzmanlarca askeri avantaj kazandıracak hedefler savaşan ve savaşı destekleyen unsurlarla sınırlandırılmıştır. Bu kapsamda örneğin, savaşa mali kaynak için petrol tesislerine ihtiyacı olan bir ülkenin petrol tesisleri, ABD ve az sayıda uzmanın pozisyonuna göre askeri amaç olup silahlı çatışma hukukuna uygunken, çoğunluğun görüşü aksi yönde olmuştur [18]. Dolayısıyla görülmektedir ki, el kitabı temel hukuk prensipleri üzerinde yol gösterici olsa da belirlenen kuralların yorumlanması ve uygulanması ülkeden ülkeye farklılık gösterebilmektedir.

İncelenen yayınların, literatürde uzun soluklu devam edecek çalışmaların ilk ürünleri olduğu görülmüştür. En genel anlamda; her ne kadar Greenberg "Uluslararası hukukta yasaklanmayan herhangi bir hususa, aynı hukuk kurallarına göre izin verildiğini söylemek yanlış olmaz" [19] şeklinde genel geçer bir kural olduğunu belirtse de özellikle ABD politikalarını yansıtan Koh konuşması ve Tallinn El Kitabı bu alandaki pek çok belirsizliği tartışmak suretiyle açıklığa kavuşturabilmiştir. Bundan sonra, yapılması gereken BM sözleşmesindeki "Kuvvet Kullanımı" ve "Silahlı Saldırı" normları temel alınarak uluslararası bir yasal rejim zemini oluşturabilmektir. Uluslararası bir anlaşma hazırlanarak [20], tanımlanacak kuralların uygulanmasını temin ve kontrol edecek politik organizasyonların oluşturulması da söz konusu olabilecektir [21]. Rusya'nın önderliğini yaptığı bir diğer düşünce akımı ise siber savaş silahlarının kısıtlanması hususu olup [21,22] siber silahların etkilerinin artarak hissedilmesi durumunda yakın gelecekte uluslararası anlaşmalarda gündem maddesi olabilecektir.

İncelenen çalışmalar göstermiştir ki, siber güvenlik alanında taarruzi yeteneklerin geliştirilmesine engel bir yasa, kanun ya da anlaşma bulunmamaktadır. Bu yeteneklerin uluslararası hukuk kuralları çerçevesinde nasıl kullanılacağına ilişkin kurallar da bağlayıcı olmamakla beraber üç yıllık süren bir çalışma sonucunda oluşturulan Tallinn El Kitabı'nda tanımlanmıştır. Bu doğrultuda da başta ABD olmak üzere pek çok ülkenin hem savunma hem de taarruzi amaçlarla insan gücü yetiştirdiği ve yetenek kazandığı görülmektedir. Siber silah üretimi konusunda henüz erken olduğunu düşünmenin yanlış olduğunu belirtmekte fayda vardır [23].

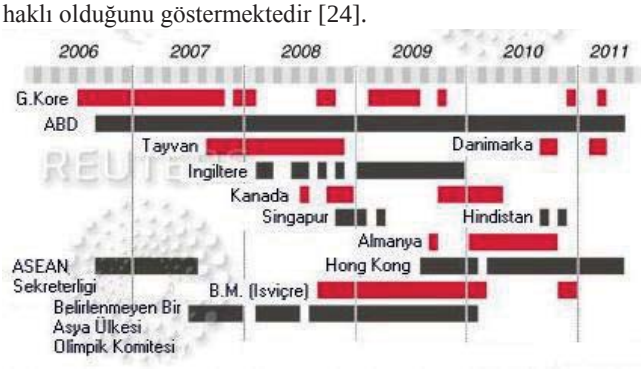
Sonraki bölümde açık kaynaklarda faaliyetlerine ilişkin diğer ülkelere nazaran daha fazla bilgi bulunabilen ABD'nin siber güvenliğin taarruzi boyutuna yaklaşımı ve bu alandaki gelişmeleri incelenecektir.

III. ABD'NIN YAKLAŞIMI ve ÖNEMLİ GELİŞMELER

ABD'de 11 Eylül 2001 saldırılarından sonra Bush yönetimi tarafından oluşturulan yeni ulusal güvenlik stratejisinin önemli ögesi önleyici saldırıdır. Uluslararası hukuka uygunluğu tartışmalı halde olan ve son yıllarda Obama yönetimi tarafından bırakılması tartışılan doktrine göre, ABD, kendisine tehdit teşkil ettiğini değerlendirdiği her unsura karşı kuvvet kullanımını "meşru müdafaa halinde kuvvet kullanımı" ile benzeştirmekte ve bu suretle yasallaştırmaktadır.

Özellikle son iki-üç yıl içerisinde ABD NSA Direktörü ve Savunma Sekreteri tarafından yapılan basın açıklamalarında, "siber 9/11", "siber pearl harbor", gibi ifadeler kullanılarak, siber uzayın kara, deniz, hava ve uzaydan sonra beşinci harekât alanı olduğu ve bu sebeple 2011 strateji belgesinde de ifade edildiği üzere diğer dört harekât alanındaki gibi, siber uzay üstünlüğünün sağlanması için gerekli yetenek geliştirme faaliyetlerinin icra edilmekte olduğu, açıkça dile getirilmektedir.

Şekil 1.de 2006-2011 yılları arasında ülkelerin maruz kaldığı önemli saldırılara ilişkin tarih çizelgesinde ABD'nin tüm zamanlarda saldırı altında olduğu görülmektedir. Bu durum, ABD üst yönetimi tarafından yapılan açıklamaların haklı olduğunu göstermektedir [24].



Şekil 1. 2006-2011 Yılları Arasında Ülkelerin Maruz Kaldığı Siber Saldırılar [24].

Ulusal Savunma Yetkilendirme Yasası'nın 2012 yılı için onaylanmış metninde ABD'nin taarruzi siber harekâtlarının dayandırıldığı yasal zemin şu şekilde belirtilmiştir [25]:

"Kongre, Ülkemizi, Müttefiklerimizi ve milli çıkarlarımızı korumak amacıyla Savunma Bakanlığı'nın siber uzayda taarruzi harekât icra etmek için gerekli yeteneklere sahip olduğunu ve ABD Başkanı'nın aşağıda belirtilen iki hususa bağlı olarak vereceği direktif üzerine gerekli taarruzi harekâtları icra edebileceğini teyit etmektedir:

(1) Savunma Bakanlığı'nın kinetik yetenekler için silahlı çatışma hukuku da dahil olmak üzere izlediği politika prensipleri ve yasal rejimler,

(2) Savaş Üst Kararı (War Powers Resolution) (ABD Başkanı'nın Kongre onayı olmadan savaş ilan edememe yetkisi).

Birinci maddede bahse geçen politika prensipleri ve yasal rejimler ABD Dışişleri Bakanlığı Hukuk Danışmanı Harold Koh'un, 18 Eylül 2012 tarihinde ABD Siber K.lığı tarafından düzenlenen bir konferansta yaptığı yazılı konuşma metninde açıklanmıştır [15]. Ulusal Savunma Yetkilendirme Yasası'nın 2013 yılı için onaylanmış metninde ise her üç aylık dönemde icra edilen taarruzi siber harekatlar için Senato'ya brifing verilmesi hususu belirtilmiştir [26].

ABD Başkanı tarafından açıklanan 2010 tarihli Ulusal Güvenlik Stratejisinde, siber güvenlik tehditlerinin ülke

olarak karşı karşıya olunan en ciddi milli güvenlik, kamu güvenliği ve ekonomik zorluk olduğu belirtilmiştir [27].

Mayıs 2011 tarihli "Siber Uzay için Uluslararası Strateji" isimli strateji belgesinde askeri açıdan 21.yüzyılın tehditlerine hazırlanma, internetin yönetimi ve yetenek geliştirme belirlenen politika öncelikleri arasındadır. Ayrıca, dokümanda Birleşmiş Milletler Sözleşmesi'ne uygun olarak siber uzayda saldırgan davranışlara karşı ABD'nin meşru müdafaa hakkı bulunduğu belirtilmiştir [28].

ABD Savunma Bakanlığı (Department of Defense- DoD) tarafından hazırlanan, "Siber Uzayın İşletilmesi için Savunma Bakanlığı Stratejisi" isimli 2011 Temmuz tarihli belgede ise beş stratejik inisiyatif tanımlanmış olup ilkinin, siber uzayın harekât alanı kabul edilmesi, bu kapsamda DoD tarafından siber uzayın tüm avantajlarından faydalanabilmek maksadıyla kara, hava, deniz ve uzay harekat alanlarında yapılan faaliyetlere paralel olarak siber uzayda da gerekli düzenlemelerin, eğitimlerin ve teçhizatlanmanın yapılması gerektiği belirtilmiştir [29].

Bir diğer strateji dokümanı olan "Kapsamlı Ulusal Siber Güvenlik İnisiyatifi" (Comprehensive National Cybersecurity Initiative-CNCI) dokümanı, 2008 yılında Bush yönetimince "GİZLİ" gizlilik derecesinde hazırlanmış ancak; 2010 Mart ayında bir bölümünün gizlilik derecesi indirgenerek kamuya açılmıştır. Dokümanda; askeri, sivil ve hükümet bilgisayar ağları ve sistemlerinin ve kritik altyapıların korunması ile siber savaşa karşı izlenilecek saldırgan stratejilere ilişkin hükümetin kapsamlı stratejisini kapsayan 12 adet direktif yer almaktadır. Planın kamuya açılan kısmında hükümete bağlı bilgisayar ağlarının korunmasına ilişkin kullanılan Einstein 2 ve Einstein 3 programları altında kurulması planlanan saldırı tespit sistemleri sensörleri ve çoğunluğu özel sektör tarafından işletilen ve kontrol edilen ülke kritik altyapılarının korunmasına ilişkin hükümetin rolü yer almaktadır. Einstein 2 programı, federal ağlara giren ve çıkan tüm ağ paketlerinde tehdit içeren imzaların tespiti amacıyla araştırma yapılmasını; tespit edilen tehdit emarelerinin ABD Bilgisayar Olaylarına Müdahale Ekibi (BOME) merkezine (US-CERT) gerçek zamanlı olarak iletilmesi suretiyle bir siber savaş erken uyarı sisteminin kurulmasını; Einstein 3 ise USCERT'e ilave olarak Ulusal Güvenlik Ajansı (NSA) gibi çeşitli federal başkanlık ve ilgili birimlerle gerçek zamanlı olarak veri paylaşımını da kapsayan bir sistemin kurulmasını öngörmektedir [30].

Çift şapkalı olarak Ulusal Güvenlik Ajansı (National Security Agency-NSA) ve ABD Siber Komutanlığı (USCYBERCOM) direktörü olan General Keith Alexander tarafından ABD'nin siber taarruz gücüne ihtiyacı olduğu basına da açıklanmıştır [31]. Nitekim, Savunma Sekreteri Mr. Leon Panetta tarafından basına yapılan açıklamada da, sadece gelişmiş korunma yöntemleri ile ülkeye yapılması muhtemel saldırıların önlenemeyeceği, ülke topraklarına veya vatandaşlarına zarar verecek saldırıların gerçekleşmesi durumunda, ABD'nin de ülkesini korumaya yönelik farklı seçeneklerinin bulunması gerektiği açıklanmıştır [32].

Aralık 2011'de ABD'de imzalanan Ulusal Savunma Yetki Kanunu ile siber saldırı amaçlı operasyonlara yetki tanınmış, bu kapsamda ABD'nin taarruz amaçlı siber yetenek geliştirmesinin onaylandığı açıklanmıştır [33]. Basına ayrıntıları açıklanmayan Pentagon tarafından başlatılan ve DARPA tarafından icra edilecek olan Plan X projesi kapsamında, ABD tarafından taarruzi amaçlı siber yetenek geliştirildiği medyada yer alan haberler arasındadır [32]. Plan X projesinin amacı, siber uzayın anlaşılması, yönetilmesi ve planlanması için yeni, devrimsel teknolojiler geliştirmek olarak tanımlanmıştır. Ağustos 2012 tarihinde yapılan bir basın açıklamasında da ABD Hava Kuvvetleri Siber K.lığı tarafından hasmın siber uzayı kendi avantajına kullanamaması için, siber uzay yeteneklerinin imhası, azaltılması, caydırılması, aldatılması, bozulması ya da el konulması amacıyla yeni fikirler arandığı açıklanmıştır. Nitekim, ABD Hava K.K.lığı, siber uzayda üstünlüğün kazanılması amacıyla 2013 yılı bütçesi için 4 milyar ABD doları talep etmiştir [34].

ABD Kara K.K.lığının İstihbarat ve Bilgi Harbi Direktörlüğü tarafından hazırlanan bir proje kapsamında elektronik harp ve siber savaş teknolojilerinin entegrasyonu sayesinde kapalı şebekelere sızma amacıyla bir demo programı yürütüldüğü açıklanmıştır. İki yıl sürmesi planlanan projenin ayrıntıları açıklanmamakla beraber adının Taktik Elektromanyetik Siber Savaş Demo Programı olduğu açıklanmıştır [35].

Ekim 2012 ayı içerisinde Pentagon tarafından, ABD'ye yapılan siber saldırılara ABD tarafından aynı şekilde siber saldırılarla cevap verileceği açıklanmıştır. Bu açıklama daha önce yapılan siber saldırıların savaş sebebi kabul edileceği ve karşılığında ABD'nin siber uzayda ya da diğer şekilde askeri operasyonlarla cevap verme hakkının bulunduğuna [36] yönelik açıklamalarla örtüşmektedir. 2013 yılı için hazırlanan ve Başkan Obama tarafından 02 Ocak 2013 tarihinde imzalanarak yasalaşan Ulusal Savunma Yetkilendirme Yasası metninde, Savunma Sekreterliği tarafından, üç ayda bir, siber uzayda icra edilen tüm taarruzi ve önemli savunma harekâtları hakkında bilgilendirme yapılması gerektiği ifadesi bulunmaktadır [37].

Sonuç olarak, ABD'de gerek insan gücü yetiştirme gerekse diğer taarruzi yetenek geliştirme faaliyetlerinin [3] artık kamuoyunda da açıkça dile getirildiği, dolayısıyla siber taarruzların askeri plan, program ve doktrinlerde yer almaya başladığı değerlendirilmektedir.

Sonraki bölümde Türkiye'de son dönemde siber güvenlik ve özellikle siber güvenliğin taarruzi boyutuna ilişkin gelişmeler ele alınmıştır.

IV. TÜRKİYE'DEKİ DURUM

Ülkemizde siber güvenlik yapılanma faaliyetleri kapsamında;

- Temmuz 2012'de TÜBİTAK BİLGEM'e bağlı Siber Güvenlik Enstitüsü kurulmuş,
- Eylül 2012'de TSK Siber Savunma Merkezi Başkanlığı,
- 20 Ekim 2012 tarihinde Ulusal Siber Güvenlik Çalışmalarının Yürütülmesi, Yönetilmesi ve Koordinasyonuna İlişkin 2012/3842 sayılı Bakanlar Kurulu kararı Resmi Gazete'de yayımlanmış,

- Ekim 2012'de ise Siber Güvenlik Kurulu kurulmuş ve ilk toplantısını 20 Aralık 2012'de icra etmiş,
- Mayıs 2013 tarihinde Siber Güvenlik Kurulu ikinci toplantısını yapmış, Telekomünikasyon İletişim Başkanlığı (TİB)'na bağlı Ulusal Siber Olaylara Müdahale Merkezi (USOM) faaliyete başlamış,
- 20 Haziran 2013 tarihinde Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı resmi gazetede yayımlanmıştır [38-41].

2012/3842 sayılı Bakanlar Kurulu kararı ile; Ulusal Siber Güvenliğin sağlanması için politika, strateji ve eylem planlarını hazırlamak başta olmak üzere ana koordinasyon ve sorumluluk Ulaştırma, Denizcilik ve Haberleşme Bakanlığı'na (UDHB) verilmiştir. Ayrıca, bahse konu karar ile, siber güvenlikle ilgili olarak alınacak önlemleri belirlemek, hazırlanan plan, program, rapor, usul, esas ve standartları onaylamak ve bunların uygulanmasını ve koordinasyonunu sağlamak amacıyla; Ulaştırma, Denizcilik ve Haberleşme Bakanı'nın başkanlığında Dışişleri, İçişleri, Milli Savunma, Ulaştırma, Denizcilik ve Haberleşme Bakanlıkları müsteşarları, Kamu Düzeni ve Güvenliği Müsteşarı, Milli İstihbarat Teşkilatı Müsteşarı, Gnkur.Bşk.lığı MEBS Başkanı, Bilgi Teknolojileri ve İletişim Kurumu Başkanı, Mali Suçları Araştırma Kurulu Başkanı, Telekomünikasyon İletişim Başkanı ile sorumlu bakanlıkça belirlenecek bakanlık ve kamu kurumlarının üst düzey yöneticilerinden oluşan Siber Güvenlik Kurulu kurulmuştur [40].

Ülkemizi etkileyebilecek tehditlere karşı, 7 gün 24 saat müdahale esasına göre çalışan Ulusal Siber Olaylara Müdahale Merkezi (USOM), kendisine bağlı Sektörel Siber Olaylara Müdahale Ekiplerini (SOME) eğitmekte ve UDHB ve ilgili kuruluşlara ait 34 web sitesini siber saldırılara karşı izlemektedir [39].

Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı'nda 29 eylem maddesi belirlenmiş [41], belirlenen 29 eylem maddesinde taarruzi yeteneklerin geliştirilmesine yönelik açık bir ifade bulunmamaktadır.

Siber savunmaya yönelik balküpü kurulması, çeşitli eğitim ve Ar-Ge projeleri bulunmakta olup SSM Müsteşarlığı ile STM A.Ş. arasında 23 Temmuz 2012 tarihinde Bilgi Güvencesi ve Siber Savunma yeteneklerinin kazanılması amacıyla "Bütünleşik Siber Güvenlik Sistemi" Fizibilite Çalışması Sözleşmesi imzalanmıştır. Fizibilite çalışması kapsamında konsept doğrulama amacı ile, sınama ortamı üzerinde çalışan prototip bir ürün geliştirilecek ve Ağ Destekli Yetenek kapsamında kullanılabilecek siber savunma sistemleri, yazılımları ve süreçlerini kapsayan bir fizibilite raporu hazırlanacaktır [42].

Meclis İnternet Komisyonu'nun Aralık 2012 ayında açıklanan bin on bir sayfalık raporunda, TSK bünyesinde siber ordu kurulması önerilmiştir. Komisyonun Meclis Başkanlığı'na sunduğu raporda, acilen ulusal siber güvenlik, ulusal bilgi güvenliği stratejileri ve eylem planları oluşturulmasının yanı sıra, "savaş halinde düşman ülke bilgi sistemlerini hedef alacak siber saldırıların Silahlı Kuvvetler bünyesinde teşkil edilecek siber komutanlık birimlerince yapılması ve bu amaçla gereken altyapının kurulması" da önerilmiştir [43].

25 Aralık 2012-11 Ocak 2013 tarihleri arasında gerçekleştirilen 2'nci Siber Güvenlik Tatbikatı sonrasında Ulaştırma, Denizcilik ve Haberleşme Bakanı, savaşların artık topla tüfekle değil, bilişim teknolojileriyle yapıldığını bildirerek, Türkiye'de, hem askeri anlamda hem sivil anlamda bu tehditle ilgili gerekli adımlar atılmaya başlandığını, siber tehlikenin gelecekte daha da önemli hale geleceğini ve siber saldırı konusunda devletlerin farkındalık bakımından aralarında uçurum olduğunu ifade etmiştir [44].

V. SONUÇ

Siber savaş her geçen gün önemini daha da artırmaktadır. Haziran 2013'de icra edilen NATO Savunma Bakanları toplantısı kapsamında İttifak, tarihinde ilk kez siber savunmayı, ayrı bir oturumda ele almıştır. Önemini her geçen gün artıran siber savaşta kullanılan teknolojiler, nükleer teknoloji gibi birkaç ülkenin tekelinde bulunmamaktadır. Bütün ülkeler veya belli gruplar tarafından bu teknoloji kullanılarak siber saldırılar icra edilebilmektedir.

Türkiye'nin siber savaşlara hazırlanması kapsamında, yazarların 5'nci Bilgi Güvenliği ve Kriptoloji Konferansı'nda sunduğu önerilere [8] ilave olarak aşağıdaki somut önerilerin dikkate alınmasının uygun olacağı değerlendirilmektedir:

- Siber uzayın bir harekât alanı olduğunun kabul edilmesi ve bunun Milli Güvenlik Siyaset Belgesi'ne dahil edilmesi (bu sayede TSK'ya hem savunma hem de taarruzi yetenek geliştirme direktifi verilmesi),
- Bu doğrultuda başta TSK olmak üzere gerek savunma gerek taarruzi siber yetenekler konusunda uzmanlaşmış insan gücü yetiştirmesi,
- Harekât ihtiyacı analizi yapılarak gerekli yetenek boşluklarının çıkarılması ve ilgili projelerin başlatılması,
- Ulusal çapta gerçekleştirilebilecek bir teknoloji yol haritası uygulaması sonucunda savunma ve saldırı amaçlı kullanılabilecek kritik siber teknolojilerin belirlenerek milli olarak geliştirilmesinin sağlanması
- Ulusal Kritik Altyapıların korunması amacıyla müşterek (kamu-özel sektör) SOME'lerin kurulması, başta bünyesinde kritik altyapı barındıran Bakanlıklar olmak üzere tüm Bakanlıkların Siber Güvenlik Stratejik Planlarını oluşturmaları,
- Ulusal ve uluslararası siber güvenlik tatbikatlarına aktif olarak katılınması,
- Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı'ndaki 29 numaralı "Siber Güvenliğin Milli Güvenliğe Entegrasyonu" eylem maddesinin revize edilerek milli güvenliği sağlayan kara, deniz ve hava gücüne yönelik izlenen milli güvenlik stratejisinin siber uzay ve siber güvenlik alanında da aynı şekilde izlenmesinin sağlanması,
- Bu konuda yetişmiş insan gücüne duyulan ihtiyacın karşılanması için gerek akademilerde ve gerekse üniversitelerde çalışmalar yapılması.

Sonuç olarak, siber güvenlik alanında taarruzi yeteneklerin geliştirilmesine engel bir yasa, kanun ya da anlaşma bulunmadığı açıktır. Siber uzayın, ABD'de olduğu gibi, harbin beşinci boyutu olarak tanımlanması durumunda, diğer dört boyutun kurallarının siber uzaya da uygulanması gerektiği, bu durumda barış zamanında taarruzi yetenek geliştirmenin siber uzayda üstünlüğün elde edilmesi için kritik öneme sahip olduğu değerlendirilmektedir.

Ulusal Siber Güvenlik Stratejisi kapsamında, siber güvenliğin sağlanması için savunma stratejisinin uygulanmasının, saldırı tekniklerinin her geçen gün gelişmekte olduğu, gerek işletim sistemi gerekse kullanılan uygulama yazılımları ve donanımlarda ortaya çıkarılan sıfır gün açıklıklarının hedefli saldırılarda kullanıldığı düşünüldüğünde, hiçbir zaman yüzde yüz başarı getirmeyeceği bilinmelidir.

Meydansız muharebe olarak tanımlanan siber savaşların kazanılmasının yolunun bu ortamlarda bilgi birikimi, deneyim, yetişmiş insan gücü ve yeteneklerin geliştirilmesi, uzmanlaşma ve önceden hazırlanma ile kazanılacağının farkında olunmalıdır.

Bu bildirinin ihtiva ettiği hususlar, yazarların şahsi görüşleri olup, kurumlarının resmi görüşlerini yansıtmamaktadır.

KAYNAKLAR

[1] Zetter, K., "State-Sponsored Malware 'Flame' Has Smaller, More Devious Cousin", 15 Ekim 2012, erişilme tarihi 12 Temmuz 2013, <http://www.wired.com/threatlevel/2012/10/miniflame-espionage-tool/>

[2] Raiu, Costin., Emm, David., "Kaspersky Security Bulletin 2012. Malware Evolution", 5 Aralık 2012, erişilme tarihi 12 Temmuz 2013, <http://www.securelist.com/en/analysis/204792254/>

[3] Mulrine, A., "Pentagon's Plan X: How it could change cyberwarfare" , 12 Ekim 2012, erişilme tarihi 6 Temmuz 2013, <http://www.csmonitor.com/USA/Military/2012/1012/Pentagon-s-Plan-X-how-it-could-change-cyberwarfare/>

[4] Zetter, K., "Researchers Connect Flame to US-Israel Stuxnet Attack", 06 Kasım 2012, erişilme tarihi 12 Temmuz 2013, <http://www.wired.com/threatlevel/2012/06/flame-tied-to-stuxnet/>

[5] Zetter, K., "Report: US and Israel Behind Flame Espionage Tool", 06 Aralık 2012, erişilme tarihi 12 Temmuz 2013, <http://www.wired.com/threatlevel/2012/06/us-and-israel-behind-flame/>

[6] Gostev, Alexander., "Kaspersky Security Bulletin 2012: Cyber Weapons" 18 Aralık 2012, erişilme tarihi 12 Temmuz 2013, <http://www.securelist.com/en/analysis/204792257/Kaspersky_Security_Bulletin_2012_Cyber_Weapons/>

[7] Chiesa, Raoul. "About Information Warfare: new rules for a new world", Ocak 2011, erişilme tarihi 10 Temmuz 2013, <http://www.chmag.in/article/jan2011/about-information-warfare-new-rules-new-world/>

[8] Şentürk, H., Çil, C. Z., Sağıroğlu, Ş., "Siber Güvenlik Makro Analiz Modeli Önerisi ve Türkiye'nin Analizi", 5'inci Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansı, 15-17 Mayıs 2012, Ankara, Turkey.

[9] Lewis, James A., "Conflict and Negotiation in Cyberspace : A Report of the Public Policy Program", Center for Strategic and International Studies (CSIS), Şubat 2013, <http://csis.org/files/publication/130208_Lewis_ConflictCyberspace_Web.pdf/>

[10] Avrupa Siber Suç Sözleşmesi, <http://conventions.coe.int/Treaty/en/Summaries/Html/185.htm/>

[11] APEC Cyber Security Strategy, Syf.2, <http://unpan1.un.org/intradoc/groups/public/documents/APCITY/UNPAN012298.pdf/>

[12] Birleşmiş Milletler Sözleşmesi Madde 51.

[13] Wallace, David., Reeves, R.Shane, "The Law of Armed Conlict's Wicked Problem: Levée en Masse in Cyber Warfare", International Law Studies, US Naval War College, Vol. 89, 2013

[14] Lewis, James A., "Thresholds for Cyberwarfare", IEE Security & Privacy, Eylül 2011, <http://csis.org/files/publication/101001_ieee_insert.pdf/>

[15] Koh, Harold Hongju, USCYBERCOM Inter-Agency Legal Conference, Ft. Meade, MD, 18 Eylül 2012, <http://www.state.gov/s/l/releases/remarks/197924.htm/>

[16] Tallinn Manual on the International Law Applicable to Cyber Warfare) , Cambridge University Press, ISBN 978-1-107-02443-4, 2013

[17] Aslan, M.Yasin, "Savaş Hukukunun Temel Prensipleri", TBB Dergisi, Sayı 79, 2008

[18] Schmitt, Michael N., "International Law in Cyberspace: The Koh Speech and Tallinn Manual Juxtaposed," 54Harvard International Law Journal. Online13 (2012), <http://www.harvardilj.org/2012/12/online-articles-online_54_schmitt/>

[19] Greenberg,L., Goodman, S., Hoo,K., "Information Warfare and International Law", National Defence University Press, 1998

[20] Schjolberg, Stein., "Peace and Justice in Cyberspace : Potential new international legal mechanisms against global cyberattacks and other global cybercrime", Norveç, 2012,

[21] Owens, William A., Dam, Kenneth W. and Lin, Herbert S., "Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabıılities", The National Academies Press, Washington, D.C., 2009

[22] Malawer, Stuart, "Cyberwarfare: Law & Policy Proposals for U.S. & Global Governance", (November 18, 2010). Virginia Lawyer, Vol. 58, p. 28, February 2010; GMU School of Public Policy Research Paper No. 2009-11. Available at SSRN: http://ssrn.com/abstract=1437002

[23] Gündoğan, Mete, Prof.Dr., "Siber Silah Endüstrisi ve Türkiye", Siber Güvenlik Konferansı, 22 Aralık 2011, Ankara.

[24] Friedman, Rebecca., "Cyber Attacks Update", 26 Ocak 2012, erişilme tarihi 11 Temmuz 2013, <http://blog.thomsonreuters.com/index.php/tag/cyber-attacks/%EF%BB%BF/>

[25] US National Defense Authorization Act 2012, erişilme tarihi 14 Temmuz 2013, <http://www.gpo.gov/fdsys/pkg/BILLS-112hr1540enr/pdf/BILLS-112hr1540enr.pdf/>

[26] US National Defense Authorization Act 2013, syf. 257, erişilme tarihi 14 Temmuz 2013, <http://www.gpo.gov/fdsys/pkg/BILLS-112hr4310enr/pdf/BILLS-112hr4310enr.pdf/>

[27] US White House "National Security Strategy", May 2010, syf 27, erişilme tarihi 14 Temmuz 2013, <http://www.whitehouse.gov/sites/default/files/rss_viewer/national_security_strategy.pdf/>

[28] US White House "International Strategy for Cyber Space", May 2011, syf 10, erişilme tarihi 14 Temmuz 2013, <http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf/>

[29] US Department of Defense, "Strategy for Operating in Cyber Space", July 2011, syf. 5, erişilme tarihi 14 Temmuz 2013, <http://www.defense.gov/news/d20110714cyber.pdf/>

[30] US White House, "The Comprehensive National Cybersecurity Initiative", <http://www.whitehouse.gov/cybersecurity/comprehensive-national-cybersecurity-initiative/>

[31] Fransa Basın Ajansı, "NSA director: U.S. needs offensive weapons in cyberwar", 04 Ekim 2012, erişilme tarihi 02 Temmuz 2013, <http://www.rawstory.com/rs/2012/10/04/nsa-director-u-s-needs-offensive-weapons-in-cyberwar/>

[32] Glaser, J., "Pentagon Lays Out 'Offensive Cyber' Attack Policy", 15 Kasım 2011, erişilme tarihi 02 Temmuz 2013, <http://news.antiwar.com/2011/11/15/pentagon-lays-out-offensive-cyber-attack-policy/>

[33] Hoover, Nicholas J., "DARPA Boosts Cybersecurity Research Spending 50%", Information Week, 07 Kasım 2011

[34] Gjelten,T., "First Strike: US Cyber Warriors Seize the Offensive", World Affairs Dergisi, Ocak/Şubat sayısı, erişilme tarihi 04 Temmuz 2013, <http://www.worldaffairsjournal.org/article/first-strike-us-cyber-warriors-seize-offensive/>

[35] FryerBiggs, Z., "Cyber's Next Chapter: Penetrating Sealed Networks", 16 Aralık 2012, erişilme tarihi 03 Temmuz 2013, <http://www.defensenews.com/article/20121216/DEFREG02/312160

002/Cyber-8217-s-Next-Chapter-Penetrating-Sealed-Networks?odyssey=tab%7Ctopnews%7Ctext%7CFRONTPAGE/>
[36] Gorman, Barnes., Barnes, J. "Cyber Combat :Act of War", 30 Mayıs 2011, erişilme tarihi 06 Temmuz 2013, <http://online.wsj.com/article/SB10001424052702304563104576355623135782718.html#ixzz1NwkCMvXU/>
[37] Corrin, A., "Defense Bill Emphasize Cyber Operations", 03 Ocak 2013, erişilme tarihi 06 Temmuz 2013, <http://fcw.com/articles/2013/01/03/ndaa-provisions.aspx/>
[38] Türköz, Tahsin, "Ulusal Siber Güvenlik Stratejisi ve Yürütülen Çalışmalar, Siber Güvenlik Konferansı, İstanbul, 17 Mayıs 2013.
[39] Vidinli, İ.B., "Ulusal Siber Güvenlik Çalışmaları ve USOM", Siber Güvenlik Konferansı, İstanbul, 17 Mayıs 2013.
[40] Resmi Gazete, 20 Ekim 2012, <http://www.resmigazete.gov.tr/eskiler/2012/10/20121020-18.htm/>
[41] Resmi Gazete, 20 Haziran 2013, <http://www.resmigazete.gov.tr/eskiler/2013/06/20130620-1-1.pdf/>
[42] SSM Web Sitesi, erişilme tarihi 06 Ocak 2013, <http://www.ssm.gov.tr/anasayfa/hizli/duyurular/etkinlikler/torenler/Sayfalar/20122507ButSbrGuvSist.aspx/>
[43] Sarıdoğan,Neşe.,Star Gazetesi, 21 Aralık 2012, erişilme tarihi 10 Temmuz 2013, <http://haber.stargazete.com/politika/meclisten-siber-komutanlik-onerisi-geldi/haber-713682/>
[44] TÜBİTAK Web Sitesi, "2.Ulusal Siber Güvenlik Tatbikatı Başarıyla Tamamlandı", erişilme tarihi 14 Temmuz 2013, <http://www.tk.gov.tr/sayfa.php?ID=153/>