Süleyman Demirel Üniversitesi
İktisadi ve İdari Bilimler
Fakültesi Dergisi
Y.2011, C.16, S.2, s.263-279.

Suleyman Demirel University
The Journal of Faculty of Economics
and Administrative Sciences
Y.2011, Vol.16, No.2, pp.263-279.

REEL DÜNYADA SANAL AÇMAZ: SİBER ALANDA ULUSLARARASI İLİŞKİLER

UNREAL STALEMATE IN THE REAL WORLD: INTERNATIONAL RELATIONS IN CYBER SPACE

Yrd.Doç.Dr.Muharrem GÜRKAYNAK[*]
Adem Ali İREN[**]

ÖZET

Teknoloji kullanımı yaygınlaştıkça teknolojinin önemli faydalarıyla beraber çok önemli zararları da toplumsal yaşamı ve uluslararası ilişkileri etkilemektedir. Gerçek dünyanın varlığına ek olarak yaygın elektronik alt yapı kullanımıyla meydan gelen siber dünya; hem fiziki dünyada olan somut olaylardan etkilenmekte hem de siber alanda düzenlenen saldırılar yüzünden gerçek dünyayı etkilemektedir. Günümüzde tehdit asimetrik ve çok boyutlu bir hal almış, tek boyutlu ve devletten devlete olma özelliğini kaybetmiştir.

Çalışmada; kullanımı yaygınlaşan ve etkisi gittikçe artan internet ve siber alanın uluslararası barış ve güvenliğe yönelik risk ve tehditlerine dikkat çekmek amaçlanmaktadır. Çünkü siber alandaki faaliyetlerin kolay ve arkada iz bırakmadan yapılabilir oluşu terör örgütlerinin yanı sıra devletlerin de ilgisini çekmektedir. Günümüzde kimi ülkeler siber saldırı ve siber savaşı önemli stratejik savunma ve rakibe zarar verme yöntemi olarak görmektedirler. Önümüzdeki dönemde bazı savaşlar her ne kadar siber alanda yapılacak olsa da etkileri reel dünyada da hissedilecektir.

ABSTRACT

As use of technology becomes widespread, besides technology's important benefits, its important harms affect the social life and international relations. In addition to real world, cyber world, which comes up by use of common electronic substructure, both is affected by concrete events happening in physical world and affect the real world because of the attacks happening in cyber space. In our day, this threat has become asymmetrical and multidimensional, and has lost its property of being one dimensional and becoming one state to another state.

This study aims to attract attention to the risks and threats of internet and cyber space, whose usage is becoming spread and effect is

[*] Süleyman Demirel Üniversitesi İİBF Uluslararası İlişkiler Bölümü Öğretim Üyesi ve Epoka Üniversitesi/Arnavutluk İİBF Siyaset Bilimi ve Uluslararası İlişkiler Bölümü Misafir Öğretim Üyesi, muharremgurkaynak@sdu.edu.tr, mgurkaynak@epoka.edu.al

[**] Süleyman Demirel Üniversitesi Sosyal Bilimler Enstitüsü Uluslararası İlişkiler ABD Yüksek Lisans Öğrencisi, ademali@windowslive.com

progressively increasing, directed at international peace and security. Because, the fact those activities in cyber space can be done easily and without a trace, take attention of states besides terrorist organizations. Nowadays, some states regard cyber attack and cyber warfare as an important way of strategic defense and destructing the rival. In upcoming period, even if some wars are made in cyber space, their effects will be also felt in real world.

Siber Alan, Siber Terör, Siber Savaş, Siber Saldırı
Cyber Space, Cyber Terror, Cyber Warfare, Cyber Attacks

GİRİŞ

Teknoloji toplumsal hayatın ayrılmaz bir parçasını oluşturmaktadır. Günümüzde bilgisayarların yaygınlaşması ve bilişim (bilgi-iletişim) teknolojilerinin gelişmesi insanları birçok bakımdan bu teknolojiye bağımlı hale getirmiştir. Bilgisayar, internet, cep telefonu, uydu gibi bilişim ürünleri günlük hayatın vazgeçilmezleri arasındadır.

Bilişim teknolojilerinde yaşanan gelişmeler bireyler kadar uluslararası toplumun da ilgisini çekmekte ve bu toplumu da etkilemektedir. Özellikle bilgisayarlar kullanılarak oluşturulan araçlar ve yöntemler, gerçek dünyanın yanında bir de "siber alan" meydana getirmiş ve bu alan bireylerin ve toplumların günlük yaşamlarında çok önemli faydalar ve kolaylıklar sağlamaya başlamıştır. Ancak kötü niyetli ve bilinçsiz kullanımdan dolayı bazı dezavantajları da beraberinde bulundurmaktadır. Örneğin, terörün geleneksel yöntemlerin ötesinde siber alanda da boy göstermesi, dünyayı siber terör tehdidiyle karşı karşıya bırakmaktadır. Artık teröristler geleneksel yöntemlerinin ötesinde, yeni siber saldırı yöntemlerini de kullanmaya başlamışlardır.

Bilgisayar ve internet teknolojilerinde yaşanan hızlı gelişme, yönetimlerin sanal dünyayı izlemelerini zorlaştırmakta ve çoğu zaman da onları yetersiz ve çaresiz bırakmaktadır. Bu nedenle yönetimler kolaycılığa kaçarak, sanal dünyadaki kötü niyetli uygulamalarla mücadelede genellikle geleneksel yöntemleri, yani yasaklama ve erişimi engellemeyi tercih etmektedirler. Ancak özellikle terör grupları tarafından bilgisayarların bir saldırı aracı olarak kullanılmaya başlanmasıyla beraber, NATO ve AB gibi uluslararası örgütlerin yanında, ABD, Çin ve Rusya gibi ülkeler de muhtemel bir siber saldırıya karşı nasıl korunabileceklerini araştırmaktadırlar. Ayrıca görevi olası siber saldırılara hızla cevap vermek ve düşman kuvvetlerinin haberleşme ve koordinasyonunu sağlayacak bilgi teknolojilerini saf dışı bırakmak olan "siber kuvvetler" de bulundurmaya başlamışlardır (Billo ve Chang, 2004:2).

Siber alandaki faaliyetlerin kolay ve arkada iz bırakmadan yapılabilir oluşu terör örgütlerinin yanı sıra devletlerin de ilgisini çekmeye başlamıştır. Hatta kimi ülkeler siber saldırı ve siber savaşı önemli stratejik savunma ve rakibe zarar verme yöntemi olarak görmektedirler. Bu nedenle

önümüzdeki dönemde bazı savaşlar ve mücadeleler siber alana taşınacak olsa da muhtemel etkileri reel dünyada da hissedilecektir.

Reel dünyayı ve bu dünyadaki ilişkileri inceleyen klasik Uluslararası İlişkiler çalışmalarında, siber alan ve bu alandaki uluslararası ilişkiler genellikle ihmal edilmektedir. Bu nedenle çalışmamız temel olarak bu konuya dikkat çekmeyi amaçlamaktadır. Zira siber alanda yaşanan gelişmeler yeni güvenlik risklerini beraberinde getirmekte, yeni aktörlerin devreye girmesine neden olmakta ve böylece uluslararası ilişkilere farklı bir boyut kazandırmaktadır.

Çalışmamızda siber alan, siber terörizm ve siber savaş ile ilgili kavramsal bilgiler verildikten sonra, siber alandaki saldırı ve mücadelenin enstrümanlarını oluşturan siber silahlar açıklanmakta ve bu silahların kullanıldığı örnekler verilerek, konunun Uluslararası İlişkiler çalışmalarının ihmal edemeyeceği boyutta ve ciddiyette olduğu değerlendirilmektedir.

1. SİBER ALAN

Uluslararası alanda kabul edilmiş bir tanımı olmamasına rağmen, siber alanı tanımlama çabaları mevcuttur. Bilişim teknolojisinde lider konumdaki ABD'nin Savunma Bakanlığı'nca yayınlanan terimler sözlüğünde siber alan; "işlemci ve kontrolörlerin bulunduğu internet, telekomünikasyon ağları ve bilgisayar sistemlerini de içine alan, birbirine bağlı bilgi teknolojileri altyapılarının olduğu küresel bir alan" olarak tanımlanmaktadır (United States of America Department of Defence, 2010:93). Yani bu alan aslında fiziki ve somut bir alan değildir. Kısaca stenografik[1] yazım şekliyle gösterilen siber alan; birlikte işleyerek bilgi akışı sağlayan bilgisayar ağları ve telekomünikasyon sistemlerinin bulunduğu w*orld wide web* (www.) olarak tanımlanabilir (Wingfield, 2000:17). Başka bir tanım ise Amerikan Kongre Araştırma Merkezi tarafından yapılmıştır. Buna göre siber alan; "insanların bilgisayarlar ve telekomünikasyon sistemleri aracılığıyla herhangi bir coğrafi sınırlamaya maruz kalmadan tamamen birbirine bağlı olma durumudur" (Hildreth, 2001:1).

Siber alanda gerçekleştirilen saldırıların geleneksel saldırılardan önemli farklılıkları bulunmaktadır. Her şeyden önce siber saldırılar ışık hızı gibi yüksek bir hızda gerçekleştirilebilme olanağına sahiptir. Bununla birlikte modern toplumlardaki altyapının yüksek teknolojiye ihtiyaç duyması nedeniyle, sanal dünya üzerinden gerçekleştirilen saldırıların etkileri konvansiyonel silahlar kadar büyük olabilmektedir. Ayrıca siber saldırıların maliyeti geleneksel saldırılarla mukayese edilemeyecek kadar düşüktür ve siber saldırının hedefinde yer alan objenin kasten mi yoksa kazayla mı saldırıya maruz kaldığının anlaşılması kolay değildir (Todd, 2009:68-69).

[1] Söylenen sözleri söylendiği kadar çabuk yazmaya elverişli, kısa ve yalın işaretlerden oluşan yazı yöntemi. Örn: www. (World Wide Web) http://www.tdksozluk.com/index.php?qu=stenografi&ne=a&Submit=Ara 15.05. 2011

Ayrıca uluslararası sistemdeki aktörlerin üzerinde uzlaştıkları bir siber alan tanımının yapılamamış olması, siber alan üzerinden yapılan saldırılarda uluslararası hukukun nasıl uygulanacağı konusunu da bir sorunsal olarak ortaya çıkarmaktadır. Çünkü siber alanın genel bir tanımının yapılamaması ülkelerin sahip oldukları siber alanların sınırlarının belirgin olmamasına da neden olmaktadır. Örneğin bir terörist örgütün herhangi bir ülkenin siber alanı üzerinden adres alarak, hedeflediği başka bir ülkeye zarar vermesi durumunda, saldırının hedefinde olan ülke ile saldırının düzenlendiği siber alana sahip ülke arasında sorunlar yaşanabilmektedir. Ayrıca siber saldırının devlet eliyle mi yoksa terörist gruplarca mı gerçekleştirildiğinin tespitinin net bir biçimde yapılamaması, saldırının düzenlendiği siber alana sahip ülke üzerinde de bir şüphe oluşmasına neden olmaktadır. 2008 yılında Rusya ile Gürcistan arasında yaşanan savaşta Rusya'ya ait siber alandan Gürcistan'a yapılan siber saldırı bu duruma örnek gösterilebilir. Rusya Gürcistan'a yönelik siber saldırılarda herhangi bir katkısı olmadığını iddia etse de (Markoff, 2008), bu saldırıların Rusya'nın bilgisi dahilinde devlet destekli olarak mı yoksa bu ülkede bulunan terör örgütleri tarafından mı gerçekleştirildiği kesinlik kazanamamıştır (Swaine, 2008; Ashmore, 2009:11).

2. SİBER TERÖRİZM

Siber terörizm, siber alanın terörist faaliyetler için kullanılması sonucu ortaya çıkmıştır. Bununla birlikte siber terörizmin de uluslararası alanda genel kabul gören bir tanımı yoktur. Zira terörizmin bile henüz tüm dünyada kabul görmüş ve zamana göre değişmeyen bir tanımının yapılamadığı bir ortamda, siber terörizmin herkes tarafından kabul edilmiş bir tanımının olmayışı gayet normaldir!

Bununla birlikte siber terör, bilgisayar ağlarını kullanarak kritik öneme sahip ulusal altyapılara (enerji, ulaşım ve devlet işlemleri) zarar vermeyi ya da tamamen kullanılamaz hale getirmeyi amaçlayan saldırılar biçiminde kendini göstermektedir (Weimann, 2005:130). Siyasal bir amaç uğruna insanlara zarar vermek veya acı çektirmek için devlet tarafından iyi korunan alanlardaki (telekomünikasyon, ulusal güvenlik ağları vs) bilgileri elde etmek, değiştirmek veya terörist amaçlar için kullanmak siber terörün önemli hedefleri arasında yer almaktadır. Saldırganın siber terör enstrümanlarını kullanarak saldırıyı gerçekleştirmesine yol açan nedenler ve saldırıyı düzenleyenin bilinçli olarak bilgi teknolojilerini kullanması ve böylece zarara yol açması onu geleneksel terörden farklı kılan özellikler olarak ortaya çıkmaktadır (Krasavin, 2004).

Siber terörü "bilgisayarlar aracılığıyla halkta yeterince paniğe yol açacak ve önemli zarar verebilecek faaliyetler" olarak da tanımlayanlar bulunmaktadır (Denning, 2001). Örneğin uçakların kullandığı sistemlere yapılan saldırılar sonrasında rotada sapmaya yol açarak, uçakların düşmesine neden olmak veya elektrik santrallerinin devreleriyle oynayarak uzun süreli elektrik kesintilerine neden olmak gibi eylemleri kapsayabilmektedir. Ya da,

acil servis ve polis imdat gibi hizmetlerin kullandığı çağrı merkezlerini tüm yurtta kullanılamaz hale getirerek halk arasında paniğe yol açmak, bankaların çok güvenli olarak bilinen sistemlerine girerek müşterilerin kimlik bilgilerini ve paralarını çalmak, siber terörün yol açtığı başka zararlardır. Özellikle bankalara yapılan siber saldırılar bankaların güvenliğini sorgulanabilir hale getirirken saldırıya uğrayan siteleri de büyük ekonomik zararlara uğratmaktadırlar.

Siber terör faaliyetleri başlı başına bir saldırı olarak meydana gelebileceği gibi genelde siyasi tansiyonun yükseldiği veya taraflar arasında silahlı çatışmalar yaşandığı sırada da meydana gelebilmektedir.

Siber terör saldırıları son dönemde artış göstermektedir. Siber terörün yükselişe geçmesinin önemli nedeni olarak, insanların ve hayati öneme sahip altyapı hizmetlerinin bilgisayar ağlarına gittikçe bağımlı hale gelmesi sonrasında yeni hassas noktaların ve dev elektronik zafiyet alanlarının oluşması gösterilmektedir (Lewis, 2002:1).

Siber saldırı yöntemlerinin terörist gruplarca kullanılmasının birçok nedeni bulunmaktadır: Siber saldırı yöntemleri fiziki tahribata dayanan geleneksel saldırı metotlarından daha ucuza mal edilebilmektedir. Sıradan bir bilgisayar yardımıyla bilgisayar ağlarına önemli zararlar verilebilmektedir. Bugüne kadar gerçekleştirilmiş siber saldırıların gösterdiği üzere, basit bir virüs saldırısının bile verebileceği ekonomik zarar milyar dolarları bulabilmektedir (Lacho ve Richardson, 2007:101). Siber alanda saldırıyı düzenleyen kişilerin izlerini takip etmek oldukça güç olduğu için siber saldırı yöntemi terör grupları tarafından benimsenmektedir. Bu sayede daha hızlı ve kolay bir şekilde saklanma imkanı bulmaktadırlar. Siber saldırı yöntemi gerçek dünyada meydana gelen saldırı yöntemlerine göre daha anonim bir kimliğe sahip olduğu için saldırı düzenlemek niyetinde olan gruplar herhangi bir gümrük noktası veya havaalanı kontrolünden geçmeden siber alan üzerinden hedef ülkeye ulaşabilmektedir. Diğer önemli bir unsur ise, siber saldırı düzenlenebilecek çok sayıda hedef olmasıdır. Çeşitli kamu kuruluşlarının ya da özel şirketlerin internet siteleri hedef olabileceği gibi ülke çapında polis ve sağlık sektörü tarafından kullanılan çağrı merkezleri de devre dışı bırakılabilmektedir. Bu kadar çok çeşitlilik arasında siber terör grupları saldırı düzenleyebilecekleri bir zayıf halka bulmakta zorlanmamaktadırlar. Ayrıca siber saldırılar fiziki eğitim ya da psikolojik motivasyon gerektiren ve ölüm riski bulunan konvansiyonel saldırılardan oldukça farklıdır. Bu şekilde uzaktan, kimliklerini ve bulundukları yerleri gizleyerek saldırı düzenleme imkanı bulan siber suç grupları bu tür saldırıları düzenleyebilecek adamları kiralama ya da yetiştirme konusunda sıkıntı çekmemektedirler. Son olarak ise siber terör fiziki terörün etkilediği insandan daha büyük bir kitleyi etkileyebilme gücüne sahiptir. Tüm bu nedenler siber saldırıların terör örgütlerince kullanılmalarını sağlamakta ve onlara hem reel dünyada hem de sanal dünyada gerçekleştirecekleri eylemlerde kolaylıklar sunmaktadır.

3. SİBER SAVAŞ

Siber alan, siber terörizm gibi kavramların uluslararası sistemde kabul görmüş tanımları olmadığı gibi siber savaşın da herkesçe benimsenen bir tanımı yoktur. Bununla birlikte siber savaş için de bazı tanımlar yapılmıştır. ABD Savunma Bakanlığı siber operasyonları, "saldırıyı düzenleyenlerin temel amaçlarına ulaşmak için sahip oldukları siber kapasitenin siber alanda kullanılması" olarak tanımlamıştır (United States of America Department of Defence, 2010:93). Siber savaş, "bilgi teknolojilerini korumak için siber alanda savunma yapmak veya saldırmak ya da rakip saldırıları engellemek için yapılan faaliyetlerin tümü" olarak da görülebilir. (Hildreth, 2001:1)

Günümüzde ülkeler konvansiyonel savaş stratejilerinin yanı sıra siber savaşa karşı da hazırlık yapmaktadırlar. Çünkü gelişmiş ülkelerin ulusal savunma sistemleri ileri düzeydeki bilgi teknolojileriyle korunmaktadır. Bu da gelişmiş ülkeleri olası bir savaşta siber saldırı tehdidi altında bırakmaktadır. Ulusal savunma ve bilgi depolama gibi alanlarda teknolojiden üst düzeyde yararlanmanın getirdiği kolaylıkların yanında, savunma sistemlerinin güvenliği açısından önemli hassasiyetler de bulunmaktadır. Teknolojiyi verimli kullanarak rakiplerine üstünlük sağlayan gelişmiş ülkeler, terör grupları tarafından hedef alınıp haberleşme, savunma veya temel alt yapı hizmetleri gibi alanlarda zarara uğratılabilmektedir. Trafik ışıklarının ya da metro hatlarının sinyalizasyon sistemlerini devre dışı bırakabilecek kadar siber kapasite kullanımına sahip gruplar tarafından düzenlenebilecek siber saldırılar, teknolojik gelişmişlik düzeyi yüksek olan ülkelerin de kendi güvenliklerinin ve düzenin tesisi konusunda zafiyet yaşamasına neden olabilmektedir.

Siber savaş ile siber terörü birbirinden ayırmak çok kolay değildir. Siber savaşı siber terör faaliyetlerinden ayıran farklılık, ülkeler arasında ortaya çıkan fiziki savaş haline eşlik etmeleri veya fiziki savaş olmasa bile iki rakip tarafın siber alanda birbirlerine saldırmalarıdır.

Çin, Rusya ve Kuzey Kore gibi ülkeler siber savunma alanına önemli yatırımlar yapan ülkelerin başında gelmektedirler. Çin şu anda önemli siber saldırı kapasitesine ve gelişmiş istihbarat alt yapısına sahip bir devlet olarak 2050 yılına kadar elektronik egemenliği hedefleyen ve düşman kuvvetlerinin altyapılarını etkisiz hale getirebilmeyi de içeren bir "siber doktrin" benimsemiştir (United States-China Economic and Security Review Commission, 2008). Çin'deki Halk Özgürlük Ordusu (*People's Liberation Army*) siber savaşın kara, deniz ve hava savaşıyla aynı öneme sahip olduğu ve bunun için de kendi ordusunun bulunması gerektiğini bildirmiştir. (Alexander, 2007:59) Çin rakiplerine karşı siber saldırı kapasitesini artırarak sadece fizik dünyada yapılan savaşların üstünlük için yeterli olmadığını kabul etmiştir. Özellikle ABD ve Rusya gibi güçlü rakipleriyle siber alanda başa çıkabilmek için önemli çalışmalar yapmaktadır. Güçlü virüsler ve kötü amaçlı yazılımlar (*malware*) düzenleyerek düşmanlarının elektronik alt yapılarının çökertmeyi amaçlamaktadır (Coleman, 2008; Schaap, 2009: 132).

Çin siber savaşa karşı aldığı bu önlemlerinde yalnız değildir. Diğer gelişmiş teknolojiye sahip ülkeler de kendi önlemlerini almaktadırlar. Örneğin, Rus ordusu bilgi teknolojilerinde uzmanlar ve akademisyenlerle birlikte çok dirençli virüsler ve yazılımlar geliştirmeye dayanan siber savaş doktrininden hareketle dikkat çekici siber saldırı silahları geliştirmiştir (Billo ve Chang, 2004:4). Rusya'nın da diğer ülkelerin sahip olduğu gibi ileri düzey siber saldırı silahları ve gelişmiş stratejileri bulunmaktadır. Rusya muhtemel bir saldırı veya savaşta karşı tarafın bilgi teknolojilerine dayanan altyapısını ortadan kaldırabilmenin yanında aynı zamanda finansal ve askeri sektörler ile sivil iletişim sistemlerini çalışamaz duruma sokabilecek önemli donanımlara da sahiptir. Kuzey Kore'nin teknolojisi de daha önce bahsedilen devletlerin sahip olduğu siber saldırı kapasitesinden aşağı değildir. Kuzey Kore ordusu da *Unit 121* adında siber savaşa odaklanan ve olası bir savaşa karşı kapasitesini geliştirmeye çalışan bir birim kurmuştur (Schaap, 2009:133). Siber savaşı ciddiye alan diğer bir devlet ise Hindistan'dır. Pakistan'la yaşanan Keşmir sorunu ve nükleer silah denemelerinde maruz kaldığı siber saldırılara önlem almak amacıyla sanal dünyada yaşanan rekabete kayıtsız kalamamıştır. Hindistan bugüne kadar önemli siber saldırılara uğradığı için, 1998 yılından itibaren siber savaşı da içine alan yeni güvenlik doktrini doğrultusunda hareket etmektedir. Ulusal Savunma Üniversitesi (*National Defense University*) ve Savunma İstihbarat Birimi'ne (*Defense Intelligence Agency*) sahip olan Hindistan, bu birime bağlı; siber savaş, psikolojik operasyon, elektro-manyetik ve dalga teknolojilerinde uzman alt birimler kurmuştur. İran ise siyasi ve ekonomik açıdan savunma sistemlerinin korunmasına yönelik teknolojik yatırımlara ağırlık vermektedir. İran'daki silahlı kuvvetler ve teknik üniversiteler bağımsız olarak siber alanda araştırma geliştirme çalışmaları yapabilecek ve bilgi teknolojileri alanında nitelikli eleman yetiştirebilecek merkezler oluşturmaya çalışmaktadır. Ayrıca, Tahran'daki yetkililer dışarıdan bilgi teknolojileri satın almakta, askeri alanda teknik yardım aramakta, Rusya ve Hindistan gibi ülkelerden de eğitim desteği almaktadırlar. Siber savaşın geleceğin en önemli üstünlük sağlama mücadelesi olacağını öngören ülkeler kendilerini bu alanda hazırlamaya çoktan başlamışlardır. Hem kendilerine yönelecek siber tehditlere anında karşı koyabilmek hem de karşılarındaki güçlerin teknik donanımlarını kullanılamaz hale getirebilmek için siber savaşa ciddi olarak hazırlanmaktadırlar (Billo ve Chang, 2004:3).

Siber alan, siber terörizm ve siber savaş kavramlarını kısaca açıkladıktan sonra bu kavramlara hayat veren araç ve yöntemlerden yani siber silahlardan bahsetmek anlamlı olmaktadır. Zira bu silahlarla birlikte yukarıda anlatılanlar daha iyi anlaşılacaktır.

4. SİBER SİLAHLAR

Siber alanda gerçekleşen saldırıların ve savaşların kendine özgü silahları bulunmaktadırlar. Bu silahlar doğrudan fiziki dünyayı hedef almasalar da sanal dünya ile eklemlenmiş günlük hayatımızda olumsuz sonuçlara yol açabilmektedirler. Örneğin ulusal haberleşme ağlarına zarar

verebilmekte veya elektrik santrallerini devre dışı bırakarak kullanılamaz hale getirebilmektedirler.

Siber silahları üç ana başlıkta toplamak mümkündür. Bu silahlar genel olarak sözdizimsel (*syntactic*), anlamsal (*semantic*) ve karışık (*mixed*) tipteki silahlar olarak adlandırılmaktadır (Brenner ve Goodman, 2002). Sözdizimsel silahlar DoS (*Denial of Service*) saldırılarını ve kötü niyetli yazılımları (*Malicious Code, Spyware, Trojan Horses* ve *Worms*) kullanarak bilgisayarların işletim sistemlerine zarar verirler. Anlamsal (*semantic*) siber silahlar ise bilgisayarda karşımıza çıkan bilgilerin doğruluğunu değiştirerek bilgisayar kullanıcılarına kendini fark ettirmeden yanlış bilgi edinmelerini sağlarlar. Karışık tipteki siber saldırı araçları ise hem sözdizimsel (*syntactic*) hem de anlamsal (*semantic*) silahların birlikte kullanılmasıyla oluşurlar ve sadece bilgisayarın işletim sistemlerine zarar vermekle kalmaz aynı zamanda bilgisayar kullanıcılarının elde ettiği bilgilerin doğruluğunu da değiştirirler. Bu bakımdan karışık tipteki siber silahlar daha profesyonel saldırı aracı olarak görülmektedir. Aşağıda siber savaş silahları ve bu saldırı araçlarının kullanıldığı bazı örnek olaylar ele alınmaktadır.

4.1. Hizmet Aksatma (DoS) ve Dağınık Hizmet Aksatma (DDoS) Saldırıları

DoS (*Denial of Service*) saldırılarındaki amaç kritik bilgileri çalmak, onları düzenlemek veya yok etmek değildir; DoS saldırıları herhangi bir ağın işleyişini bozmaya yönelik saldırılardır (Xiang vd., 2010:2). Böylelikle ağ kullanıcıları, bilgi akışını yavaşlatacak veya tamamıyla durduracak biçimdeki yenileme istekleri nedeniyle ağa ulaşamaz duruma gelebilmektedirler. Bu saldırılar herhangi bir internet sitesinden hizmet alan kullanıcıların o siteye erişimlerini engelleyerek hizmet akışının durmasını sağlamaktadır. Bu tarz saldırıların en önemli özelliği saldıran tarafa çok sınırlı imkanlarla bile saldırıyı düzenleyebilecek fırsatı vermesidir. Eski model bir bilgisayar ve sıradan bir modemle son teknolojiyi kullanan bir bilgisayar ağını çökertmek mümkün olmaktadır. Hem maliyeti düşük ve faili bulunamayan, hem de etkisi önemli olan DoS saldırıları siber savaşta kullanılan önemli silahlardandır.

DDoS (*Distributed Denial of Service*) saldırıları ise virüsler tarafından etki altına alınmış çok sayıda bilgisayar sistemlerinin veya ağlarının tek bir bilgisayara saldırmasıdır. Böylece binlerce bilgisayar aynı anda tek bir bilgisayara saldırarak onu etkisiz hale getirebilmektedir (Douligeris ve Mitrokotsa, 2003:643-644; Gupta vd., 2009:225). DDoS tarzdaki saldırılar DoS saldırılarına kıyasla durdurulması daha güç saldırılardır. Çünkü birçok farklı noktadan aynı anda saldırmaktadırlar.

Siber saldırılar tek başına ortaya çıkabileceği gibi taraflar arasında çıkan fiziki mücadelenin ardından da görülebilmektedir. Devletler veya o devletler içindeki çeşitli gruplar zaman zaman sorun yaşadıkları ülkelere karşı siber saldırı silahlarını kullanabilmektedirler.

Herhangi bir konuda sorun yaşayan taraflardan biri diğer tarafa maddi zararlar vermek ve ülke güvenliğini sağlayan yönetimlerin itibarını

sarsmak için de siber saldırı yöntemlerine başvurmaktadırlar. Örneğin, İsrail ve Filistin arasında yaşanan siyasi gerilimler gerçek ve siber dünyada birbirine paralel olarak gerçekleşen saldırılara sebep olmuştur. Filistin'de ikinci intifadanın Eylül 2000 tarihinde başlamasıyla birlikte "siber intifada" ya da "Inter-Fada" olarak adlandırılan siber savaş da başlamıştır. İsrail yönetimi, 6 Kasım 2000 tarihinde üç İsrail askerinin Hizbullah tarafından kaçırılmasını takiben, Hizbullah ve Hamas'ın internet sitelerine yoğun biçimde DDoS saldırıları düzenlemiştir. Bu saldırılara cevap olarak Filistin sempatizanı hackerlar da İsrail savunma güçlerinin, Dışişleri Bakanlığı'nın, Tel Aviv Borsası'nın ve Merkez Bankası'nın web sitelerinin çökmesine neden olmuşlardır. (Lev, 2000) Böylece iki taraf aralarındaki anlaşmazlığı ve savaşı siber alana da taşımışlardır (Whitaker, 2000).

Bu tarihlerdeki bir diğer örnek ise Çin ile ABD arasında yaşanan siber gerilimdir. 2001 yılının Nisan ayında bir Çin savaş uçağıyla ABD gözetleme uçağının çarpışması sonrasında bazı Çinli hacker grupları (*Honker Union of China* ve *Chinese Red Guest Network Security Technology Allience* gibi) ABD'ye karşı yoğun ve uzun süreli siber saldırılar düzenlemişlerdir. Çinli hacker grupları Beyaz Saray, Amerikan Enerji Bakanlığı ve Amerikan Hava Kuvvetleri'nin de içinde bulunduğu yaklaşık 1200 siteye DDoS saldırıları düzenlemişlerdir (Vatis, 2001:8). ABD'yi hedef alan siber saldırıların kaynağının belli olmasına rağmen, Çin hükümeti bu saldırılara karşı bir yaptırım uygulamamıştır. Bu saldırıların Çin hükümeti tarafından desteklendiği ya da en azından görmezden gelindiği açıktır.

Siber saldırıların daha güncel örnekleri ise 2007 yılında Estonya'ya düzenlenen yüksek yoğunluklu saldırılardır. Estonya'ya düzenlenen bu yoğun siber saldırıların başlangıç noktasını ülkede yaşayan Rus kökenli azınlıklarla Estonyalılar arasındaki sorun oluşturmuştur. Geçmişten gelen anlaşmazlığa 2007 yılının Nisan ayında ortaya çıkan sorunlar da eklenince ülke yoğun bir siber saldırı tehdidi altına girmiş, Estonya hükümetine ve ulusal medyaya ait sitelere yoğun DDoS saldırıları yapılmış ve bazı siteler de kullanılamaz hale getirilmiştir. (Davis, 2007) Estonya'yı hedef alan siber saldırılar internete dayalı bilgi teknolojilerinin ne derece hassas ve saldırılara açık olduğunu bir kez daha göstermiş bulunmaktadır.

Yakın dönemde yaşanan siber saldırı hedeflerinden bir başkası olan Gürcistan ise, 2008 yılında yaşanan Rusya-Gürcistan savaşıyla birlikte yoğun olarak siber saldırıyla karşı karşıya kalmıştır. 8 Ağustos 2008'de Rusya'nın Gürcistan'a saldırısını takiben Gürcistan hükümetine ait internet sitelerine DoS saldırıları düzenlenmiştir. Fiziki saldırıyla eş zamanlı düzenlenen siber saldırılar gerçek dünyada oluşan sorunların anında sanal dünyaya da yansıyabileceğini göstermiştir. Gürcistan ve Rusya arasındaki siber savaş kamuoyunu şekillendirmek amacı da taşımaktadır. Her iki tarafın destekçileri tarafından gerçekleştirilen DoS saldırılarına ek olarak sahte siteler hazırlanmış ve bu sitelerde iki grup da kendi doğrularını halka ulaştırmaya çalışarak propaganda yapmışlardır (Thomas, 2009:39). Bankacılık, medya ve hükümete ait sitelere bilgi akışının sağlanması durdurularak Gürcistan içinde ve uluslararası alanda haberlere ulaşım engellenmiştir. Bu saldırılara

Gürcistan tek başına karşı koymakta zorlanmış ve dışarıdan yardım almak durumunda kalmıştır. Gürcistan Dışişleri Bakanlığı sitesi ve Gürcistan'a günlük haber akışını sağlayan siteler *Google*'ın sağlamış olduğu *domain* alanı sayesinde korunmuştur. Başka bir yardım da yöneticisi Gürcü olan özel bir Amerikan internet servis sağlayıcısından gelmiş ve Gürcistan Devlet Başkanının resmi sitesinin yeniden kullanıma açılması sağlanmıştır (Ashmore, 2009:11).

Bir diğer siber saldırı Kırgızistan'da 2009 yılında meydana gelmiş ve ülkenin iki ana internet sağlayıcısı hedef alınarak, DoS saldırılarıyla web sitelerinin çökmesine, ülkedeki elektronik posta servisinin de kullanılamaz hale gelmesine neden olmuştur. Bu saldırıların Rusya kaynaklı olduğu tespit edilmiş (Rhoads, 2009), ancak saldırıların arkasında Rus hükümetinin olduğuna dair herhangi bir kanıt bulunamamıştır. [2]

Siber saldırılardan muzdarip olan devletlere Pentagondan yapılan açıklamaya göre son dönemde yaşamış olduğu siber ataklar nedeniyle ABD de katılmıştır. ABD Savunma Bakan Yardımcısı (*Deputy Secretary of Defense*) William J. Lynn siber tehlikenin farkında olduklarına vurgu yaparak "tek bir tuş darbesinin göz açıp kapayıncaya kadar önemli zararlara yol açabileceği"ni ifade etmiştir. 2011 yılı Mart ayında Ulusal Savunma Ağından tek bir seferde 24 bin belgenin çalındığını duyuran Bakan Yardımcısı Lynn "21. yüzyılda '*bit*' ve '*byte*'ların kurşun ve bombalar kadar tehlikeli olduğu"nun altını çizmiştir (Lynn, 2011). Siber saldırıların hedefinde olan ABD, kendisine yöneltilecek herhangi bir siber saldırıyı savaş sebebi sayacağını da ilan etmiştir. (Gorman ve Barnes, 2011)

4.2. Kötü Amaçlı Yazılımlar

Kötü amaçlı yazılımlar bilgisayarın işletim sistemini hedef alarak kullanılmaz hale getirebilen değişik türdeki yazılımlardır. Bu yazılımlar çeşitli amaçlara yönelik olarak da geliştirilebilmektedir.

4.2.1. IP Aldatmacası (*IP Spoofing*)

IP kandırmacası olarak kullanılan bu saldırı biçiminde saldırgan ve korsan yazılım çok bilinen güvenli bir sitenin IP adresini kullanarak kendi kimliğini gizlemeyi başarır. Gizlemiş olduğu kimlik sayesinde sisteme sızdığı tarayıcıdan (*browser*) veya bağlantı kurduğu ağdan bilgilere ulaşabilmektedir (Vatis, 2001). IP aldatmacası sayesinde sisteme sızan korsan URL (*Uniform Resource Locator* - Birörnek Kaynak Bulucu) adreslerinin bir sahtesini hazırlayabilmektedir. Böylece orijinal siteyle aradaki fark anlaşılamaz hale gelmekte ve bu farkı anlayamayan kişi ve kurumların önemli bilgilerine ulaşılabilme imkanı doğmaktadır.

[2] Rusya Bişkek'teki hava üssünün Amerikan kuvvetleri tarafından kullanımının durdurulmasını istiyordu; bu nedenle Kırgızistan'a yönelik baskı oluşturmuştu. Kırgızistan'daki siber saldırılar ise Rusya hükümetinin Kırgız hükümetine yaptığı baskıyla aynı döneme rastlamıştır. Bişkek'te bulunan hava üssü Afganistan'da Amerika tarafından yürütülen operasyonlar için stratejik öneme sahip kritik bir lojistik destek merkeziydi. Bu açıdan bakıldığında gerçek dünyada ortaya çıkan herhangi bir sorunun, siber dünyada yansımalarının görülebileceğine dair diğer önemli örnek gözler önüne serilmektedir (Rhoads, 2009).

4.2.2. Kötü Amaçlı Yazılım (*Malicious Program*)

Kötü niyetli bu yazılımlar bilgisayarın normal fonksiyonlarını yerine getirmesine engel olabilirken, bilgisayarlarda siyah pencereler açarak saldırıyı düzenleyen tarafından uzaktan kontrol edilmesini de sağlayabilmektedirler. Sanal dünyada "*trojan*", "*worm*" ve "*virus*" olarak bilinen yazılımların tamamı kötü amaçlı yazılım (*malicious program*) örnekleridir. Bu tip saldırı araçları bazı dosyaları silebileceği gibi bazılarını da kullanılamaz hale getirebilmektedir. Virüsler kendilerini bir takım program veya dosyalara bağlı hale getirebilir ve bu şekilde bir bilgisayardan diğerine diskler ve ağlar arasında -kendilerini kopyalayarak- hızla yayılabilirler. Siber saldırıda kullanılan bu tür yazılımlar hedefteki bilgisayarı kötü yazılımları barındıracak şekilde yeniden programlayarak önemli bilgileri ele geçirebilecekleri gibi bu bilgileri yok da edebilmektedirler (Dashora, 2011:246).

Worm (solucan) olarak bilinen zararlı yazılımlar virüsler gibi bilgisayarlar arasında hızla yayılabilirler. Ancak wormlar yayılırken bilgisayar kullanıcılarının yardımına ihtiyaç duymamaktadırlar (Weaver vd., 2003:11). Wormların en büyük özelliği kendilerini sayısız kez kopyalayabilmeleridir. Bu da bir bilgisayardan yüz binlerce wormun başka bilgisayarlara gönderilmesine neden olmaktadır.

Trojanlar ise zararsız ve faydalı olarak bilinen programların içine gizlenmiş yazılımlardır. İçinde bulundukları programları kontrol edebildikleri gibi onlara zarar da verebilirler. Trojanlar bir işlevi yerine getirirken aynı zamanda başka bir işlevi de gerçekleştirebilmektedirler. Örneğin bazı trojanlar yerleştikleri bilgisayar içinde farklı özel kelimeleri arayabilirler ve o kelimelerin geçtiği dosyaları kopyalayıp başka bir bilgisayara otomatik olarak gönderebilirler (Olovsson, 1992).

Kötü amaçlı yazılım programlarının en gelişmiş versiyonunu oluşturan *Stuxnet* adındaki worm, 2010 yılında ortaya çıkmıştır. Stuxnet'in en belirgin özelliği kendisini otomatik olarak kopyalayabilmesidir. Böylece içine yerleştiği ağı kullanılamaz hale getirene kadar yayılabilen bir tür yazılım bombası işlevi görmektedir (Hearn vd., 2010:9). New York Times, BBC ve Guardian gibi gazeteler bu virüsün ABD veya İsrail tarafından geliştirilmiş olabileceğini öne sürmüşlerdir.[3] Bunu düşündürecek en önemli gelişme ise Stuxnet'in hasara yol açtığı *host* sitelerinin %60'a yakınının İran'da bulunuyor olmasıdır. Bir çok kişi bu virüsün özel eğitimli uzmanlar tarafından devlet destekli bir siber saldırı amacıyla geliştirildiğini düşünmektedir (The Chemical Engineer, 2010:10).

1999'da NATO müttefiklerinin Yugoslavya Cumhuriyetini bombalamaya başlamalarının ardından, Yugoslavya sempatizanı bazı gruplar NATO'nun alt yapısını hedef alan siber saldırılar düzenlemişlerdir. NATO'nun yaklaşık 100'e yakın internet hizmet sağlayıcılarının (*server*)

[3] Daha detaylı bilgi için bkz. http://www.bbc.co.uk/news/technology-11388018; http://www.guardian.co.uk/technology/2010/sep/24/stuxnet-worm-national-agency; http://www.nytimes.com/2010/09/30/world/middleeast/30worm.html?_r=3&hpw=&p

hedef alındığı siber saldırılarda DDoS saldırıları ve yukarıda anlatılan tipteki binlerce virüslü e-mail gönderim yöntemlerinin kullanıldığı tespit edilmiştir. NATO'nun iletişim ağına yapılan siber saldırıları Amerikan hükümetinin, askeri birimlerinin ve ticari şirketlerinin web sitelerine Yugoslavya destekçisi Sırplar, Ruslar ve Çinliler tarafından yapılan saldırılar eşlik etmiştir (Messmer, 1999).

Pakistan ve Hindistan arasında yaşanan Keşmir sorunu sadece gerçek dünyada yaşanmakla kalmamış Pakistan sempatizanı çeşitli hacker gruplarının Hindistan web sitelerine saldırmasıyla sanal dünyaya da taşınmıştır. Her iki taraftan da siber saldırı grupları kendi propagandalarını yaymak için siber taktikler geliştirmiş ve bunları hayata geçirmeye çalışmışlardır. Öncelikle Pakistan destekçisi siber saldırı grupları Keşmir sorununun küresel alanda bilinirliğini artırmak için Hindistan'ın önemli web sitelerine (Hindistan Parlamentosu web sitesi, TV ağı Zee, Asian Age gazetesinin web sitesi, Hindistan Bilim Enstitüsü ve Bhabha Atom Araştırma Merkezi) saldırmışlardır (Prasad, 2000). Hindistan'a internet üzerinden düzenlenen saldırılar Keşmir sorununun yeniden alevlenmesiyle 1999–2001 arasında 5 kattan daha fazla artmıştır. (Vatis, 2001:5)

Doğrudan bir devleti hedef almayan veya ciddi bir siyasi gerilime bağlı olarak meydana gelmeyen siber saldırılar da görülebilmektedir. 2009 yılının sonlarına doğru *Google*'a yapılan saldırılar örnek olarak verilebilir. *Google* tarafından 2010 yılının hemen başında yapılan bir duyuruya göre kaynağı Çin olan siber saldırılar, *Google* şirketinin altyapısına sızarak çeşitli bilgileri çalmayı başarmış, buna ek olarak bazı insan hakları savunucularının *g-mail* hesaplarına ve 33 farklı şirketin ağına girebilmiştir (Thomas, 2010:101).

4.2.3. Yazılım Bombası (*Logic Bomb*)

Kötü niyetli yazılımların önemli bir örneği olan yazılım bombaları önceden belirlenmiş bazı olayların gerçekleşmesi şartıyla bazı uygulamaların kendiliğinden devreye sokulmasını sağlamaktadır (Olovsson, 1992:9). Örnek olarak, eğer korsan bir yazılım bilgisayardan bilgi çalmaya çalışırsa yazılım bombası otomatik olarak tüm bilgileri silebilir, karşı saldırıya geçebilir, bilgisayarı tamamen kapatarak erişimi engelleyebileceği gibi sayısız DoS saldırısı komutunu da saldırıyı düzenleyen bilgisayara karşı işleme koyabilir. Bu tip siber saldırı silahları hem mevcut bilgileri koruyarak dışarı sızmasını engellemeyi hedeflerken, hem de olası saldırılara otomatik cevap verebilmektedir. Kuzey Kore önemli siber saldırı silahlarını stratejik amaçlar için kullanmayı hedeflemiş ve 2007 yılında bilgisayar ağlarına zarar verebilecek hatta gizli bilgileri ele geçirebilecek önemli bir siber saldırı silahını denemiştir (Coleman, 2007).

4.2.4. Dijital Manipülasyon (*Digital Manipulation*)

Dijital manipülasyonlar herhangi bir imajı bilgisayar yardımıyla değiştirerek yeni anlam kazandırmayı hedeflemektedir. İstihbarat veya güvenlik birimlerinin kullandığı bu yöntem yanlış bilgilendirmeyi veya kandırmayı amaçlamaktadır. Bu sayede kamuoyu istenilen doğrultuda

yönlendirilebilmektedir. Örnek olarak, 2006 yılında İsrail ve Lübnan'daki Hizbullah örgütü arasında devam eden anlaşmazlıkta, Reuters ajansı yayınladığı fotoğraflarda dijital manipülasyona başvurduğunu kabul etmiştir (Lappin, 2006). Dijital manipülasyonun daha ileri versiyonu ise canlı yayınlanan videolarda kullanılabilmektedir. Ekranda akan video kareleri arasında saniyeden daha kısa süreli geçişlerde, bir nesne veya insan ekrandan çıkarılabileceği gibi ekranda olmayan nesne veya insan da ekrana eklenebilmektedir (Amato, 2000).

SONUÇ

Siber saldırıları engellemek için küresel anlamda işbirliğine ihtiyaç olduğu açıktır. Bugüne kadar sınırlı sayıda uluslararası antlaşmalar imzalanabilmiş ve birkaç kurum siber saldırıyla mücadele etmeyi amaçlamıştır. Avrupa ülkelerine düzenlenen siber saldırılar AB ve NATO gibi uluslararası örgütleri harekete geçirmiş ve siber tehdide karşı birlikte hareket etmenin gerekliliğini ortaya koymuştur. Avrupa Konseyi'nin 23 Kasım 2001 tarihinde siber suçla mücadele için düzenlediği zirve sonrasında kabul ettiği metin bu alandaki ilk uluslararası antlaşma niteliğini taşımaktadır (Council of Europe, 2001). Ana amacı ortak bir politika geliştirerek siber suçla mücadele etmek olan zirvede siber suçla mücadelede izlenecek yolun uluslararası işbirliği ve buna uyumlu yasalarla mümkün olabileceği vurgulanmıştır. 2004 yılında yürürlüğe giren antlaşmayı 22 Avrupa Konseyi üyesiyle birlikte ABD de imzalamıştır. Bilgisayar sistemlerine yasadışı erişim, sisteme ve içindeki bilgilere müdahale ve bilgisayarla ilgili diğer sahtecilik işlemleri de suç sayılarak bu durumun engellenmesi için her devletin sahip olduğu kanıtları karşılıklı işbirliği çerçevesinde paylaşması istenmiştir. (Ashmore, 2009:14).

Özellikle üyeleri arasında güvenlik ve işbirliğini teşvik eden AGİT siber saldırıya karşı önlemler alan diğer bir uluslararası örgüttür. Bu örgüt Estonya, Litvanya gibi Avrupa ülkelerine yapılan saldırılardan sonra siber terör konusunu daha dikkatle incelenmeye başlamıştır (Ashmore, 2009:15). Uluslararası sistemde bu ve benzeri güvenlik ve işbirliği arayışlarına rağmen siber teröre karşı etkili bir mücadele henüz sağlanamamıştır. Ayrıca ve daha da önemlisi küresel anlamda üzerinde uzlaşılan bir terör tanımlaması yapıldıktan sonra siber terörü de tanımlamak ve önümüzdeki dönemde bu tehdide karşı uluslararası aktörleri bir araya getirmek mümkün olabilecektir. Bu çok zor ve gerçekleşmesi imkânsıza yakın bir çabadır. Çünkü uluslararası sistemde Birleşmiş Milletler'e üye 193 devlet bulunmaktadır ve bu kadar devleti aynı tanım üzerinde uzlaştırmak bugüne kadar mümkün olmamıştır. Her devletin kendi terör tanımı vardır ve birinin terör dediğine diğeri özgürlük savaşı diyebilmektedir.

Üstün bir otoriteden ve dolayısıyla da etkin bir yaptırım gücünden mahrum olan uluslararası hukukta devletlerarası ilişkiler egemen eşitlik prensibi ile gerçekleşmektedir. Bu prensibe göre devletler, egemen oldukları sınırlar (*territoriality*) dahilinde yaptırım gücüne sahiptirler. Bu noktada akla

çok önemli bazı sorular gelmektedir. Örneğin devletlerin sahip oldukları bu yaptırım gücü, devletin kullandığı siber alanda da aynı şekilde olmalı mıdır? Ya da devletin hüküm sürdüğü toprak üzerindeki siber alandan sadece o devlet mi yararlanmaktadır? Siber alan fizik alan gibi üzerinde egemenlik kurulabilen bir alan mıdır? Kime ya da kimlere aittir? Bütün bu ve benzeri sorular devletin sahip olduğu coğrafyaya dayanan mülkiyet (*territoriality*) kavramını günümüzde gittikçe muğlak bir terim haline getirmektedir. Çünkü gelişen teknoloji sayesinde siber saldırılar, devletin hüküm sürdüğü coğrafyayı siber alan açısından tartışılır hale getirmiştir. Ayrıca gelişen teknoloji siber saldırı ve terörist eylemlerin aynı anda birbirinden farklı devletlerin egemen olduğu coğrafyalarda ortaya çıkmasına ve başka bir devlete zarar verebilmesine de olanak sağlamaktadır.

Böylelikle devletin egemen olduğu ülke ile o ülkeye ait siber alan gittikçe birbiriyle çelişen tutarsız yapılar olmaya başlamıştır. Ayrıca, siber güvenliği sağlayacak uluslararası işlemin maliyetinin devletler arasında nasıl paylaşılacağı da bir başka sorundur. Çünkü siber saldırılar genellikle bir devletten yürütülmediği için bu tip saldırı hazırlıklarının yürütüldüğü devletlerin siber alanlarının belirlenmesi ve faaliyetlerin önüne geçilmesi için gerekli olan insan, zaman ve ekonomik kaynağın nasıl sağlanacağı bir muammadır.

Öte yandan, devletlerin siber saldırı ve terör olaylarına bakış açıları farklı ve hatta bazen aynı devletin zaman içerisinde değişen tutarsız yaklaşımları olabilmektedir. Siber alanı daha az kullanan ve siber faaliyetleri düşük devletler, bu alanda daha aktif olan devletlere oranla siber saldırılara daha duyarsız kalabilmektedirler. Bazı devletler ise siber saldırıyı bir savaş yöntemi olarak kullanmaya meyilli olduğu için ve başka bir devletin siber güvenlik zafiyetinin kendi sorumluluklarında olmadığını düşündüklerinden küresel boyutta bir siber güvenlik oluşumuna sıcak bakmamaktadırlar. (Trachtman, 2006:279)

Henüz hangi eylemin saldırı, hangisinin saldırı tehdidi olduğu üzerinde dahi ittifak edememiş uluslararası toplumun; yakın gelecekte işinin daha da güçleşeceğini söylemek mümkündür. Zira artık uluslararası ilişkiler; reel dünya ile birlikte bir de siber alanda saldırı-siber saldırı kavramları gibi yeni kavramları tanımlamak ve üzerinde uzlaşarak uluslararası barış ve güvenliği şekillendirmek zorunluluğu ile karşı karşıyadır.

KAYNAKÇA

1. Alexander, K. B. (2007), "Warfighting in Cyberspace" *Joint Force Quarterly, National Defense University Press, 46* (3), s. 58-61.
2. Amato, Ivan (2000), "Lying with Pixels, Seeing is No Longer Believing", http://www.technologyreview.com/read_article.aspx?id =12115, 20.05.2011.
3. Ashmore, W. C. (2009), "Impact of Alleged Russian Cyber Attacks", *Baltic Security & Defence Review ,* 11, s. 4-40.

4. Billo, C., ve Chang, W. (2004). "Cyber Warfare Analysis of the Means and Motivations of Selected Nation States", Hanover: *Institute for Security Technology Studies at Dartmouth College,* Kasım 2004.

5. Brenner, S. W., ve Goodman, M. D. (2002), "In Defense of Cyberterrorism: An Argument for Anticipating Cyber-Attacks", *University of Illinois Journal of Law, Technology & Policy* .

6. Coleman; Kevin (2008), "China's Cyber Forces", http://defensetech.org /2008/05/08/chinas-cyber-forces/#more-2831, 15.05.2011.

7. Council of Europe. (2001), "Summary of the Convention on Cybercrime" http://conventions.coe.int/treaty/en/Summaries/Html/ 185.htm, 17.05.2011.

8. Dashora, K. (2011), "Cyber Crime in the Society: Problems and Preventions", *Journal of Alternative Perspectives in the Social Sciences , 3* (1), s. 240-259.

9. Davis, J. (2007), "Hackers Take Down the Most Wired Country in Europe" http://www.wired.com/politics/security/magazine/15-09/ff_ estonia?currentPage=all, 27.05.2011

10. Denning, D. (2001), "Is Cyber Terror Next?" http://essays.ssrc.org/ sept11/essays/denning.htm, 15.04.2011.

11. Douligeris, C., ve Mitrokotsa, A. (2003), "DDoS Attacks and Defense Mechanisms: Classification and State-of-the-Art", *Computer Networks, Department of Informatics University of Piraeus*, s. 643-666.

12. Gorman, S. ve Barnes Julian E. (2011), "Cyber Combat: Act of War", http://online.wsj.com/article/SB10001424052702304563104576355623135782718.html#articleTabs%3Darticle, 18.07.2011

13. Gupta, B. B., Joshi, R. C., ve Misra, M. (2009), "Defending against Distributed Denial of Service Attacks: Issues and Challenges", *Information Security Journal: A Global Perspective , 18* (5), s. 224-247.

14. Hearn, K., Williams, P., ve Mahncke, R. J. (2010), "International Relations and Cyber Attacks: Official and Unofficial Discourse", *Australian Information Warfare and Security Conference* Edith Cowan University, s. 7-11

15. Hildreth, S. A. (2001), "Cyberwarfare Congressional Research Service Report for Congress", *Congressional Research Service & The Library of Congress,* No: RL30375.

16. http://www.bbc.co.uk/news/technology-11388018, 05.08.2011

17. http://www.guardian.co.uk/technology/2010/sep/24/stuxnet-worm-national-agency, 05.08.2011

18. http://www.nytimes.com/2010/09/30/world/middleeast/30worm.html?_r =3&hpw=&p, 05.08.2011

19. http://www.tdksozluk.com/index.php?qu=stenografi&ne=a&Submit=Ara, 15.05. 2011

20. Krasavin, S. (2004), "What is Cyber-terrorism?" http://www.crime-research.org/library/Cyber-terrorism.htm, 04.05.2011

21. Lacho, I., ve Richardson, C. (2007), "Terrosit Use of the Internet The Real Story", *Joint Force Quarterly National Defense University, 45* (2), s. 100-103.

22. Lappin, Y. (2006), " Reuters Admits to More Image Manupulation", http://www.ynetnews.com/articles/0,7340,L-3287774,00.html, 13.05.2011.

23. Lev, Izhar (2000), " E-Intifada: Political Disputes Cast Shadows in Cyberspace", http://www.janes.com/security/international_security/news/jir/jir001103_1_n.shtml, 14.04.2011.

24. Lewis, J. A. (2002), "Assessing the Risks of Cybertwrrorism, Cyber War, and Other Cyber Threats", *Report Center for Strategic and Intemational Studies (CSIS)*, Washington DC.

25. Lynn, Wiiliam J. (2011), "Remarks on the Department of Defense Cyber Strategy", http://www.defense.gov/speeches/speech.aspx?speechid=1593, 18.07.2011.

26. Markoff, John (2008), " Before the Gunfire, Cyberattacks", http://www.nytimes.com/2008/08/13/technology/13cyber.html, 12.07.2011.

27. Messmer, E. (1999), "Serb Supporters Sock it to NATO and U.S. Computers", http://articles.cnn.com/1999-04-06/tech/9904_06_serbnato.idg_1_nato-personnel-nato-headquarters-nato-sources?_s = PM:TECH, 16.05.2011.

28. Olovsson, T. (1992), "A Structured Approach to Computer Security", *Department of Computer Engineering Chalmers University of Technology* S-412 96, Gothenburg, Sweden.

29. Prasad, R. V. (2000), "Hack the Hackers", http://www.hindustantimes.com/nonfram/191200/detOPI01.asp, 02.05.2011.

30. Rhoads, C. (2009), "Kyrgyzstan Knocked Offline", http://online.wsj.com/article/SB123310906904622741.html, 14.05.2011.

31. Schaap, M. A. (2009), "Cyber Warfare Operations: Development and Use under International Law", *Air Force Law Review , 64*, s. 121-173.

32. Swaine, Jon (2008), " Georgia: 'Russia Conducting Cyber War'", http://www.telegraph.co.uk/news/worldnews/europe/georgia/2539157/Georgia-Russia-conducting-cyber-war.html, 11.07.2011.

33. The Chemical Engineer (2010), "Stuxnet Targets Uranium Enrichment Plants" *The Chemical Engineer*, www.tcetoday.com 05.08.2011

34. Thomas, T. (2010), "Google Confronts China's "Three Warfares". *U.S. Army War College, 40* (2), s. 101-113.

35. Thomas, T. L. (2009), "The Bear Went Through the Mountain: Russia Appraises its Five-Day War in South Ossetia", *Journal of Slavic Military Studies*, 22(1) s. 31-67.

36. Todd, M. G. (2009), "Armed Attack In Cyberspace:Deterring Asymmetric Warfare With Anasymmetrıc Definition", *Air Force Law Review,* 64, s. 65-102.

37. Trachtman, J. (2006), "Global Cyberterrorism, Jurisdiction, And International Organization in The Law andEconomy of Cyber Security", Edt: M. Grady ve F. Parisi, The Law and Economics of Cybersecurity, Cambridge University Press, New York.

38. United States of America Department of Defence (2010), "Department of Defence Dictionary of Associated Terms", *Joint Chiefs of Staff*

39. United States-China Economic and Security Review Commission (2008), "China's Proliferation Practices, And The Development Of Its Cyber and space Warfare Capabilities" *United States-China Economic and Security Review Commission*, Washington.

40. Vatis, M. A. (2001), "Cyber Attacks During the War on Terrorism: A Predictive Analysis", *Institute for Security Technology Studies at Dartmouth College*, Hanover.

41. Weaver, N., Paxson, V., Staniford, S., ve Cunningham, R. (2003), "A Taxonomy of Computer Worms", *Proceedings of the 2003 ACM workshop on Rapid malcode* s. 11-18.

42. Weimann, G. (2005), "Cyberterrorism: The Sum of All Fears?", *Studies in Conflict & Terrorism, 28*, s. 129-149.

43. Whitaker, B. (2000), "War Games on the Net: But This Time It's For Real", http://www.guardian.co.uk/technology/2000/nov/30/ internetnews .onlinesupplement, 19.06.2011.

44. Wingfield, T. C. (2000), The Law Of Information Conflict: National Security Law In Cyberspace, Aeges Research Cooperation.

45. Xiang, Y., Zhou, W. ve Chowdhury, M. (2010), "A Survey of Active and Passive Defence Mechanisms against DDoS Attacks" *Deakin University, School of Information Technology , 51* (2), s. 1-42.