Güvenlik Bilimleri Dergisi, Kasım 2017, 6 (2), 81-108

ULUSLARARASI SİSTEM VE GÜVENLİK AÇISINDAN DEĞİŞEN SAVAŞ KURGUSU; SİBER SAVAŞ ÖRNEĞİ

Vahit GÜNTAY*

ÖZ

Devletler temel olarak çatışma halinde hareket etmektedir ve bu eğilim sistemsel olarak farklı araçlara ihtiyaç duymaktadır. Bu araçların çeşitlenmesi aslında gelişen dünyanın bir sonucudur. Altyapı olarak da kendisini bu araçlara bağımlı kılan devletler yeni savaş konseptleri oluşturmaktadır. Genellikle savaş-saldırı-çatışma gibi yaklaşımlarla ifade edilen bu eğilimler siber ortamda da yerini almıştır. Siber savaş kavramının tartışmalı niteliği kendi özelinde devam ettirilse de uluslararası politika dâhilindeki varlığı artık dikkat çekici boyutlara ulaşmıştır. Çalışma dâhilinde siber savaş örneği siber terörizm, siber politikalar, siber caydırıcılık gibi unsurlarla temellendirilerek uluslararası ilişkilerdeki konumu açısından değerlendirilmiştir.

Anahtar Kelimeler: *Uluslararası İlişkiler, Güvenlik, Uluslararası Güvenlik, Siber Güvenlik, Siber Savaş*

CHANGING WAR CONCEPT IN TERMS OF INTERNATIONAL SYSTEM AND SECURITY; CYBER WAR SAMPLE

Abstract

States basically act with conflict and this tendency needs some different tools in systematic. Diversification of these tools is the result of changing world. The states that also defend on these tools create new war concepts. These tendencies which are generally expressed with the approaches like war-attack-conflict, have also been used in cyber area. Although the controversial feauture of the cyber war concept continves in itself, its presence within international politics has now reached remarkable dimensions. In this study cyber war sample has grounded with cyber terrorism, cyber politics, cyber deterrence and evaluated with its position in international relations.

Keywords: *International Relations, Security, International Security, Cyber Security, Cyber War*

* Yrd. Doç. Dr., Karadeniz Teknik Üniversitesi İktisadi ve İdari Bilimler Fakültesi Uluslararası İlişkiler Bölümü, Trabzon, vahitguntay@gmail.com

Makale Geliş Tarihi: 10.07.2017 Makale Kabul Tarihi: 09.11.2017

GİRİŞ

Siber güvenlik perspektifi ve alana ilişkin çalışmalar uluslararası ilişkiler temelinde yeni bir boyutu ortaya çıkarmıştır. Teorik bir zemine de oturtulmaya çalışılan siber güvenlik ve devletlerin bu yöndeki algıları politik alanda geliştirilmeye oldukça müsait gözükmektedir. Sunulan veriler de bu durumun devletlere ilişkin yönünü gözler önüne sermiştir. Siber güvenlik çalışmalarının uluslararası güvenlik perspektifine kattıkları yanında, uygulama alanına ilişkin yaptığı katkı önemli gözükmektedir. Uluslararası ilişkiler ve güvenlik ile ilgili temel yaklaşımlarda Soğuk Savaş'ın bitimiyle birlikte büyük güçlerin çatışma alanlarının azalacağı gibi bir tutumun siber alanın ele alındığı bütünlük içerisinde anlamsız olduğu ortaya konulmuştur.

Uluslararası ilişkilerin sadece çatışmacı bir ortamda ilerlemediği günümüzde, siber alanda yaşanan atılım küresel güçlerin dikte ettiği bir üretim ve tüketim algısını beraberinde getirmiştir. Bu algı aktörler düzeyindeki karmaşık ilişkiyi uluslararası ilişkiler boyutuna, siber güvenlik düzeyine çatışmacı boyutta taşımıştır. Bireysel ve toplumsal beklentiler, dalgalanmalar siber güvenlik alanında strateji düzeyindeki belirleyici niteliğini uluslararası politika çalışmalarına da yansıtmıştır.

Siber güvenlik temelindeki gelişmelerle birlikte askerî teknolojilerin belirli noktalara taşındığı kara, hava, deniz unsurlarında ve nükleer mücadelede kendini hissettiren siber alandaki çıkar birliktelikleri hedef unsurlara karşı özgüveni artırmaktadır. Siber alanın güç mücadelesinde ülkelerin savunma sistemlerine saldıracak ve etki edecek daha gelişmiş yöntemler üzerindeki tartışmaları sürmektedir. Bu yaklaşımlar dâhilinde klasik olarak güç algısı yerine farklı araçlarla gücün kapsamını artırma, yeni teorik bir yaklaşımın çıkış noktası olarak dikkate değerdir.

Siber güvenlik ve kendi özüne ilişkin çalışmaların varlık boyutu sadece uluslararası politika temelinde değerlendirilmemelidir. Akademik ve profesyonel düzlemde farklı alanlarda oluşmaya başlayan baskınlık bir güç mücadelesine dönüşmüştür. Teknik alandaki gelişim ve baş döndürücü hız devletleri karşı karşıya getirmekte ve ciddi bir veri trafiği oluşmaktadır. İnterdisipliner bir yön gösteren bu çeşitlilik, siber suç olgusunu beraberinde getirerek uluslararası hukuk boyutunda da bir farkındalığı oluşturmuştur.

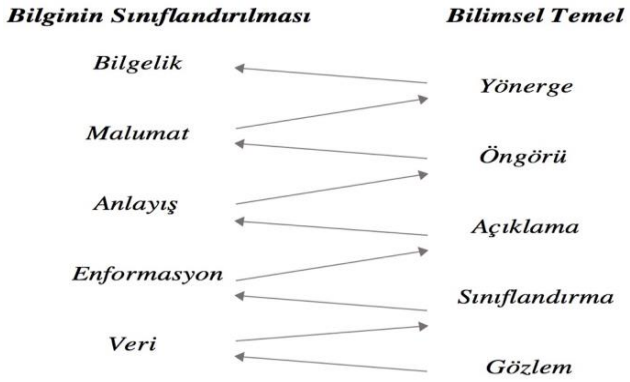
Siber savaş ortamındaki etkileşim, ekonomik açıdan yük getirmeyen zararlı yazılımların ortaya çıkışını ve nitelikli personelin tedariki hususundaki süreci hızlandırmıştır. Uluslararası güvenlik adına siber tehditler, güvenlikleştirme modeli açısından iç politikanın etkilenmesinde kendisine yer edinmeye başlamıştır. İç politikanın etkilenmesi ve ulusal çıkarın farklılaştırdığı tehdit algısı ile birlikte siber caydırıcılık açısından dış politikada çıktılar üretilmeye başlanmıştır. Siber uzayın uluslararası

güvenlik açısından tartışılması ve beraberindeki etkileşim devletlerin dış politikada ve iç politikada sahip olduğu çıktılara dair nedensel bir düzlem sağlamıştır. Siber alanın uluslararası ilişkiler açısından bir savaş alanı olup olmadığına dair eleştiriler olsa da dijital ortamdaki kaynakların sonlandırılması imkânsıza dönüştüğü için yersiz kalmaktadır. Bu kapsamın devamlılığı açısından çalışma dâhilinde değişen güvenlik kurgusu bağlamında siber savaş örneği incelenmiştir.

1. SİBER GÜVENLİK-SİBER POLİTİKALAR

Siber güvenlik ve bu alana ilişkin çalışmaların temeli, alan çalışmaları açısından herhangi bir başlığın tekelinde değildir. Dünya siyasetinin geleceği açısından çalışmalara konu olan siber güvenlik kavramı, *siber politikalar* kavramı ile ayrıştırılarak uluslararası ilişkiler açısından son yıllarda teorik olarak tartışılmaya başlanmıştır.

Teorik tartışmalar açısından Hayes ve Alberts (1995), Şekil 1'de ortaya koydukları enformasyon ve bilim tipolojisinde, enformasyon kaynaklarıyla ilişkilendirilen temellendirmelerde sürecin ilk çıkış noktasını izlenecek yönergelere bağlarken, gözlem temelinde bu basamağı sonlandırmıştır. Siber güvenlik temelindeki bilgi çeşitliliğinde bilimsel olarak bir güvenlik anlayışı ortaya çıkacaksa politik düzlemde bu ilişkinin sınıflandırılmış olması gerekmektedir. Bu tipolojide, bilginin sınıflandırılmasındaki basamaklar ve bilimsel temel, siber güvenlik anlayışının politik düzleme dönüşünde temel alınabilir.



Şekil-1: Enformasyon ve Bilimin Tipolojisi (Hayes ve Alberts,1995: 31)

Belli başlı tipolojiler arasında kamu ve özel sektörü ilgilendiren alana ilişkin temel parametreler sunan siber politikalar, uluslararası ilişkiler temelinde kimi zaman dünyayı salt saldırı-savunma ikileminde görmekte; kimi zaman teknik durumları kavramada başarısız olan bir tablo karşımıza çıkarmaktadır (Stone, 2012: 102). Siber güvenliğe ilişkin sosyal bilimler ve

uluslararası ilişkiler temelindeki çalışmaları doğru anlama adına *sibernetik, siber toplum, siber terörizm, siber tehdit, siber caydırıcılık, siber savaş, siber istihbarat* gibi kavramların doğru anlaşılması gerekmektedir.

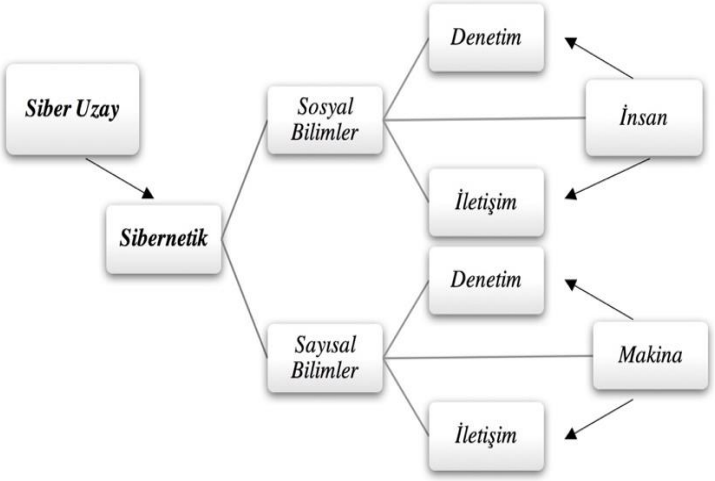
2. SİBERNETİK KAVRAMININ GÜVENLİĞE GİRİŞİ

Sibernetik canlı ve cansız tüm karmaşık sistemlerin denetlenmesi ve yönetilmesini inceler. Sibernetik, düzenli sistemlerin, bu sistemlerin yapılarının, limitlerinin ve sistemin imkânlarının araştırılmasına ilişkin disiplinlerarası bir yaklaşım içermektedir. Konu aldığı sistemler mekanik, fiziksel, biyolojik, düşüncel ve sosyal bilimlerin birçok farklı alanına ilişkin olabilmektedir. Sibernetiğin etkilediği ya da sibernetikten etkilenen çalışma alanları arasında oyun teorisi, sistem teorisi, algısal kontrol teorisi, sosyoloji, psikoloji, felsefe ve mimarlık yer almaktadır. Modern sibernetiğin kurucuları arasında gösterilen Amerikalı matematikçi ve felsefeci Norbert Wiener sibernetiği insan ve hayvanlarda kontrol ve iletişimi konu alan çalışma alanı olarak tanımlamıştır (Wiener, 1948: 54).

Sibernetiğin kavramsal olarak güvenliğe girişi teknolojik gelişim ve bunun doğurduğu etkileşim ile ortaya çıkmıştır. Tüm canlılar arasındaki bilişsel etkileşim teknolojik gelişmeler ile birlikte ekonomik ve fiziksel sonuçlar doğurmaya başlamıştır. Özellikle bilgi güvenliği ve korunmasına ilişkin siber araçlar ile birlikte uluslararası ilişkiler temelinde bireyler ve devletler de nasibini almıştır.

Devletleri ilgilendiren boyutuyla *siber uzay (cyberspace)* terimi ilk kez Amerikalı bilim-kurgu yazarı William Gibson tarafından kullanılmıştır. Terim, 1982 yılında basılan *Burning Chrome* adlı hikâye kitabında geçmiştir. *Siber uzay* ise sibernetik dediğimiz kavramın verisel olarak etkileşimde bulunduğu alana ilişkin bir terimdir ve uluslararası güvenlik açısından yeni bir savaş ortamını doğurmuştur. Siber uzay, içerisinde bilginin çevrimiçi olarak saklandığı, paylaşıldığı ve iletildiği, bilgisayar ağlarının ve arkalarındaki kullanıcıların yer aldığı karmaşık bir ortamdır. Siber uzayın en başta bir bilgi ortamı olduğunun anlaşılması önemli bir husustur. Bu durum aynı zamanda siber uzayın fiziki bir yer olmadığının anlaşılması ile ilişkili bir durumdur (Singer ve Friedman, 2015: 29). Siber ortam denildiğinde genellikle *sanal âlem* ve sanal âlemden kastedilen *internet ortamı* ilk olarak akla gelmektedir. Siber ortam internet ortamını da kapsayan bir üst kavramdır. İnternete bağlanamayan fakat sadece bir ekran vasıtasıyla içindeki sayısal değerlere ulaştığımız elektronik cihazdaki veriler siber ortamdadır. Siber ortam kapsamına bilgisayarla ulaşılan *sayısal ortam, internet ortamı, sanal gerçeklik ortamı* ve elektronik teçhizat ile ulaşılabilen *imgesel ortamlar* (rüya gibi) girmektedir. Dikkat edilmesi gereken husus etki doğurabildiği alanla ilgilidir ve burada fiziksel çevre devreye girmektedir.

Şekil 2'de sibernetik kavramının alana ilişkin kapsayıcılığı ile ilgili kurulum, sosyal bilimler ve sayısal bilimler dağılımıyla ortaya konulmaya çalışılmıştır. Özellikle siber uzay açısından kapsayıcılık insan ve makine özelinde bilimsel bir nitelik olarak çeşitlenmektedir ve sibernetiğin çıkış noktasını oluşturmaktadır. Her ne kadar sosyal bilimler içerisindeki çalışmalar son yıllara özgü gibi görünse de siber güvenliğe ilişkin felsefi ve sosyolojik yaklaşımlar belli bir birikime de sahiptir. Siber güvenlik ve alana ilişkin yapılan çalışmaların sosyal bilimlerde adaptasyonunu kolaylaştıran bu unsur olmuştur. Hatta günümüzde politik çıktılarla tartışılması bu uzantının devamı niteliğindedir. Farklı toplumlar birçok alanda olduğu gibi, sibernetik alanında da kendi yetiştirdikleri bilim adamlarıyla övünmektedirler.



Şekil-2. Sibernetiğin, Siber Uzay İçerisinde Bilimsel Olarak Kurulumu (Vinnakota, 2013: 109)

Siber uzayın uluslararası güvenlik açısından tartışılması, devletlerin dış politikada ve iç politikada sahip olduğu çıktılara ilişkin nedensel bir düzlem oluşturmasıdır. Güvenlik yaygın olarak anlaşıldığı gibi sadece tehlikeden uzak olmak değil, aynı zamanda bir düşmanın olmasıyla da ilgilidir ve siber uzay açısından taraflar farklı araçlarla bu mücadelenin içindedir. Siber uzayın uluslararası ilişkiler açısından bir savaş alanı olup olmadığına dair en büyük eleştiri, teknik anlamda dijital ortamdaki tüm araçların fişinin çekilmesi durumunda son bulacağıdır ve göreceli olduğudur.

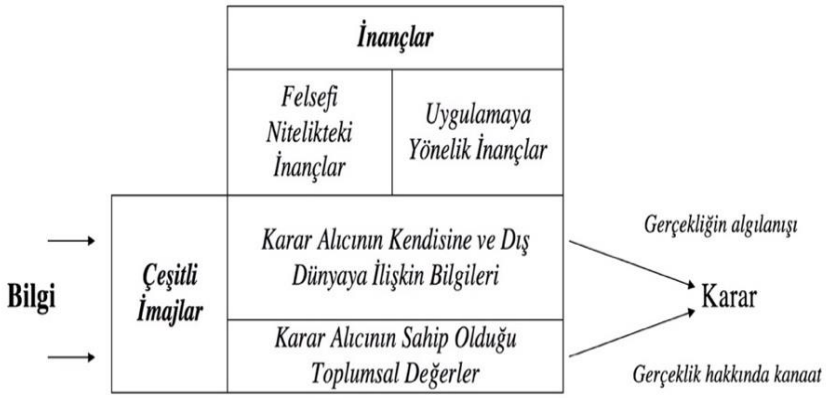
3. SİBERNETİK TOPLUM VE KARAR ALICILAR

Canlı ve cansız varlıkların denetimine ilişkin kullandığımız sibernetik kavramı toplumun nitelendirilmesinde ve kavramın siyasileşmesinde öze ilişkin bazı unsurlar barındırmaktadır. Özellikle bilgi teknolojilerinin günlük hayatın bir parçası haline gelmesi ve insanların haberleşme şekillerini değiştirmesi, sadece sosyalleşme adına bir çerçeve oluşturmamış; bunun yanında bilgi, tavsiye ve karar verme sürecinde iş birliği yapabilir hale gelmiştir (Bayraktar, 2015: 139). Günümüzde *Bilgi Teknolojisi* terimi, bilgisayar ve teknolojinin çeşitli yönlerini içine alacak şekilde genişlemiş ve bilinir hale gelmiştir. Bilgi teknolojileri alanında çalışanlar, uygulama yüklenmesinden karmaşık bilgisayar ağlarının ve veri tabanlarının tasarımına varan çeşitli görevleri yerine getirirler. Bu görevlerden bazıları veri yönetimi, ağ bağlantıları, bilgisayar donanımı, veri tabanı-yazılım tasarımı ve sistem yönetimini içerir.

Bilişim teknolojilerindeki gelişme toplum ile karar alıcılar arasında iki yönlü bir iletişim kanalı da oluşturmuştur. Bu iletişim kanallarından ilki bireylerin karar alıcılara etki edebilmesi ile igilidir ve başlı başına medyadaki gelişmelerle birlikte ayrı bir çalışma konusudur. Sibernetik toplum ve karar alıcılar arasındaki yönetim biçimi de bu geniş çalışma içinde otokontrol, bilgi aktarımı, bilişsellik gibi unsurlarla interdisipliner bir yön göstermektedir. Sibernetik konusunda çeşitli üniversite ve tıp fakültelerinde çalışmalar yapılmaktadır. Bu çalışmalarla birlikte sibernetik bilim çevrelerinin olduğu kadar halkın da ilgilendiği bir bilim dalı haline gelmiştir. Örneğin günümüzde bilgisayar işlemleriyle beynin çalışması arasındaki ilgi birçok kesimin yakından bilgi sahibi olduğu bir konu haline gelmiştir. Bu konudaki gelişim tahmin edilemeyecek bir boyuta ulaşmıştır ve devletler yönünde artık bir yarış haline gelmiştir.

Bilgi teknolojileri, özellikle karar alıcılar açısından toplumsal tepkinin ölçülmesi ve takip edilmesi adına önemli bir araç haline gelmiştir. Diğer yönü ise politika oluşturmaya ilişkindir. Devletler bu kapsam dâhilinde kendi içerisinde uzman ekipler oluşturarak karar alıcılar açısından takip edilen bir alanı ortaya çıkarmıştır. Bu alan içerisine askerî unsurların da dâhil olması, organizasyonel bir gerekliliği gündeme getirmiştir. Siber uzayda stratejistler ve karar alıcıların caydırıcı olma adına taktiksel unsurlar geliştirmesi, toplumsal değişimi de sağlamıştır. Fakat karar alıcılar ve toplumsal özellikler açısından bu alanda gelişmiş veya gelişme arzusu içinde olan devletler arasındaki fark daha açık bir şekilde ortaya çıkmıştır (Stevens, 2012: 149).

Toplumsal alanda siber güvenliğe ilişkin karar alınmasında vurguladığımız bilgi teknolojilerinin kullanılış amacı ve ortaya çıkış noktası ile karar alıcıların sahip olduğu arka plan belirleyici olmaktadır. Oluşturulan uzman ekipler bu vizyon dâhilinde ortaya çıkmaktadır. Şekil 3'te karar alma sürecinde inancın felsefi boyutunda ve uygulama niteliğinde çeşitli imajlarla bilginin karar alma çıktısına dönüşümü gösterilmektedir. Sibernetik toplum adına bilginin, bilgi teknolojileri ile daha kapsamlı hale gelmesi ve karar alıcının siber güvenlik alanına verdiği öncelik stratejik açıdan bir kazanç oluşturacaksa benzer bir süreçle ele alınmalıdır. Bu noktada karar alıcının kendisine ve dış dünyaya ilişkin bilgileri ile sahip olduğu toplumsal değerler bu döngüde belirleyici olacaktır.



Şekil-3. İnanç Sistemi, İmaj ve Karar Alma Süreci (Sönmezoğlu, 2014: 322)

Bu alan içerisindeki toplumsal dalgalanmalar, günümüzde çağdaş toplumun biçimlendirilmesinde önemli bir yere sahip olmuştur ve teknolojinin yarattığı olanaklar sayesinde birbirine elektronik olarak bağlanmış bilgisayar kullanıcılarının her biri özel birer aktör haline gelmiştir. Karar alıcıların bu konudaki çelişkisi iç ve dış politikaya ilişkin alanda şeffaflık ile politika üretmeye ilişkin olmuştur (Çakmak ve Altunok, 2009: 27).

Politika üretiminde karar alıcıların siber güvenliğe ilişkin gizlilik esasları bu alandaki belirleyici unsur haline gelerek toplumsal bir gelecek kurgusunun temelini oluşturmaktadır. Teknolojik anlamda günümüzün gelişmiş ülkelerinde dış politika kararlarının geniş ve karmaşık bir düzende ortaya çıkışı, kişilerin psikolojik çevrelerinin oluşumunda sibernetik toplum açısından ciddi farklılıklar oluşturmaktadır.

4. SİBER TERÖRİZM VE SİBER TEHDİT ALGISI

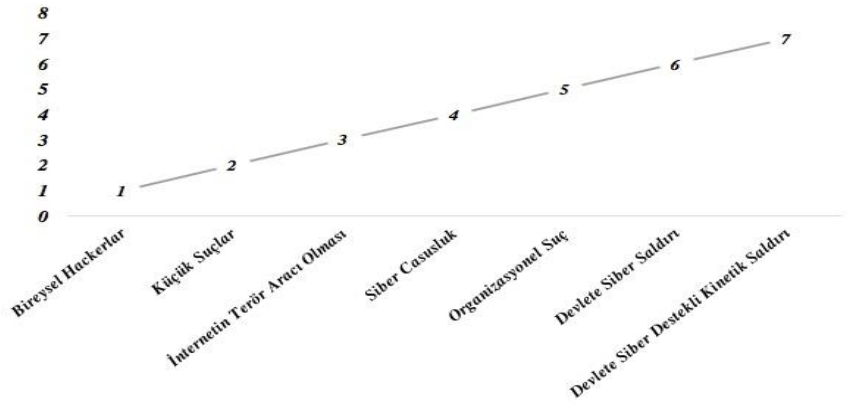
Savaş ve diplomasi yoluyla elde edilemeyenin sonuçlarına yaklaşmak amacıyla, korkutmak ve itaat ettirmek için bir teoriye, felsefeye ve ideolojiye dayandırılarak siyasi maksatlarla, iradi olarak şiddetin sistemli bir şekilde kullanılmasına "*terörizm"* denmektedir (Caşın, 2008: 35). *Siber terörizm* kavramının ise uluslararası alanda gelişimine ilişkin tartışmalı bir durum söz konusudur. Terörizmin nitelikleri göz önüne alındığında siber faaliyetlerin bir terörizm olduğu ya da siber terörizm olarak ifade edilmesi hususu hâlen tartışma konusudur. Bunun temel sebebi küresel sorunların hızla arttığı düzeyle ilgilidir. Terörizm olgusu içerisinde tartışılabilecek bir hususun nasıl ve ne şekilde ifade edileceği tarihi bir süreçle açıklanması beklenilen bir husustur.

Siber terörizm, bilgisayar ağlarını bozmaya yönelik kasıtlı ve geniş kapsamlı eylemler dâhil olmak üzere, terör eylemlerinde internet tabanlı saldırıları ve internete bağlı kişisel bilgisayarların kullanımını kapsamaktadır. Dar anlamına bakıldığında insanların can ve mallarını tehdit eden saldırılar bu kapsama girerken, geniş anlamda can ve mal tehdidine ilave olarak sosyal, dinî, ideolojik, politik veya başka amaçlarla bilgisayar ağlarına yapılan saldırılar siber terörizm kapsamına girmektedir (Çifçi, 2013: 6). Tarihin stratejik olarak şekillenmesinde olayların sonuçlarına ilişkin yaklaşımda tehdit olgusunun algısı ve modern olarak tehdit, siber terörizmin kapsamını da şekillendirmektedir (Gray, 2007: 264). Bu açıdan bakıldığında siber terörizm adına bir birikimin olduğu da gözler önündedir. Teorik bir düzeyin dahi uluslararası ilişkiler açısından tartışılabileceği siber terörizm olgusu farklı disiplinlerden ve teknik hususlardan beslenmektedir.

Siber terörizmin beslendiği nokta ve harekât bulma süreci *siber tehditlerle* ilgilidir ve kaynaklandığı noktalar bu kavrama dâhildir. Siber tehditler internete bağlanmayı sağlayan ve çevrimiçi saldırılara maruz kalmayı olanaklı kılan araçların oluşturduğu unsurlardır. Siber tehdit yöntemleri ve ortaya çıkış süreci sanal ortamda gerçekleşince maddi ve manevi, fiziksel sonuçlar doğurmaktadır ve bu sonuçların geri dönüşü olmayabilir. Bu suçların etkileyici olmaları bireysel olmalarına, kurumsal bir etki oluşturmasına ya da devlet gibi uluslararası aktörlere etki edişine göre farklılaşmaktadır. Sorunun küresel anlamda tartışılması da bu noktada başlamaktadır. Devletler adına terörizmin takip edildiği boyut siber alana da taşmıştır ve bu durum ilgi uyandırmıştır.

Grafik 1'de görüldüğü üzere özellikle bireysel anlamda işlenen bilişim suçları ve bunların etki düzeyleri, istihbarat alanına ilişkin tehditsel unsurlar ve devlete yönelik siber saldırı ya da devlete siber destekli kinetik saldırılar aynı yoğunlukta değildir ve bir etki alanına sahiptir. Devletlerin müdahil

olduğu siber olaylar, çoğu zaman organizasyonel suçlardan daha etkili sonuçlar doğurabilmektedir. Bu noktada devletleri de ilgilendiren düzey çok yönlü bir ilişki ağına sahiptir. Bu konuda devletler siber tehditlerin derecelendirildiği düzey açısından önemli bir konuma sahiptir.



Grafik-1. Siber Tehditlerin Dereceleri (Bucci, 2009)

Siber tehditlerin uluslararasılaştığı boyutta felsefi ve ideolojik yaklaşım uluslararası güvenlik sorunlarıyla birlikte ele alınmaktadır. Bu noktada siber güvenliğe ilişkin veriler ve çalışmalar siber terörizmin gelişimine ilişkin kavramsal bir durumu ortaya çıkarmaktadır. Siber uzaya artan bağımlılık, terörizm boyutuyla farklı derecelendirmeler sunmaktadır (Choucri, 2012: 19). Siber tehditlerin ve terörizme ilişkin bu derecelendirme bir siber savaş olgusunu beraberinde getirmektedir. Savaşanlar açısından taraf ve ittifak düzeyinden bahsedilmesi gerekirken siber savaş olgusu açısından bu durum tartışmalı düzeydedir. Uluslararası ilişkilerin kuramsal düzeyi bu çerçeveyi açıklamada yetersiz kalmaktadır. Özellikle güç dağılımının savaşanlar açısından tespiti bu yetersizlik düzeyinde belirleyici bir öneme sahiptir.

Siber terörizmin hem uluslararası alanda verisel güvenliği tehdit eden düzeyi, hem de bireylerin sahip olduğu kapasite Tablo 1 üzerinde sınıflandırılmıştır. Siber terörizme ilişkin verilerin örgütsel kapasiteye sahip olması durumunda ve koordinasyonlu boyutunda daha stratejik ve karmaşık eylemler gerçekleştirilebilmektedir. Bu konuda hedeflenilen amaca yönelik strateji belirlenmesinde ciddi ve derin bir analize ihtiyaç duyulmaktadır. İleri düzey ve karmaşık koordinasyonlu siber terör düzeylerinde birden fazla hedef gösterilen ağlarda, tehdit derecelerinin artmasıyla yıkıcı ve fiziksel sonuçlar doğabilmektedir. Karmaşık-koordinasyonlu düzeylerde fayda olarak stratejik eylemler, potansiyel fayda olarak tanımlanmaktadır ve hedef analizi ayrıntılı bir şekilde yer almaktadır.

Tablo-1. Siber Terör Eylem Düzeyleri (Bayraktar, 2015: 80)

Siber Terör Düzeyleri	Hedef	Hedef Analizi	Örgütsel Kapasite	Etki Kontrolü	Potansiyel Fayda
Basit-Yapılandırılmamış	Tek Sistem ya da Ağ	Başlangıç Seviyesinde	Az Seviyede	Odaklı Değil	Propaganda
İleri Düzeyde-Yapılandırılmış	Birden Çok Sistem ya da Ağ	Orta Seviyede	Orta Seviyede	Odaklı	Taktiksel Eylemler
Karmaşık-Koordinasyonlu	Birden Çok Ağ	Detaylı	Çok İleri Düzeyde	Kontrol Edilebilir	Stratejik Eylemler

Düzey olarak sosyal, dinî, ideolojik ve politik amaçlarla siber tehdit oluşturan terörist ya da terörist grupların bilgi harekâtlarını kullanış mantığı ve çerçevesi değişmiştir. Özellikle *kritik altyapıların* hedef alınması uluslararası terörizm açısından siber terörizmin daha anlaşılabilir ve mücadele edilmesi gereken bir yönü olduğunu ispatlamıştır. 2011 sonrasında ABD'deki kritik altyapı bilgisayar ağlarının takibi ve izinsiz girişler %1700 artmıştır (Singer ve Friedman, 2015: 136). Kritik altyapı kavramı bu temelde özel bir öneme sahiptir. Bu altyapılardan işlenilen bilginin gizliliği, bütünlüğü veya erişilebilirliği bozulduğunda can kaybına, büyük ölçekli ekonomik zarara, ulusal güvenlik açıklarına veya kamu düzeninin bozulmasına varabilecek ciddi sıkıntılar doğabilmektedir. Kritik altyapılar devlet düzeninin ve toplumsal düzenin sağlıklı bir şekilde işlemesi için gerekli olan ve birbirleri arasında bağımlılıkları olan fiziksel ve sayısal sistemlerdir. Enerji üretim ve dağıtım sistemleri, telekomünikasyon altyapısı, finansal servisler, su ve kanalizasyon sistemleri, güvenlik servisleri, sağlık servisleri ve ulaştırma servisleri en başta gelen kritik altyapılar olarak sıralanabilir.

Kritik altyapı gibi unsurlara saldırılar özellikle siber terörün klasik terör mantığı ve anlayışıyla ayrıştığı ve benzeştiği noktaları gruplandırma olanağını bizlere sunmuştur. Tablo 2'de görüldüğü üzere, klasik terör ve siber terör arasındaki farklara ilişkin kullanılan araçların ve etki alanının baskın şekilde farklılaştığını görmekteyiz. Donanımsal ve yazılımsal anlamdaki silahların artık fiziksel sonuçlar doğurduğu, kullanılan araçların çıktısı açısından benzerlik göstermektedir. Siber terörün yaşamsal risk olmadan neticeye götürmesi ve sonuç verdirmesi bu alandaki terörist aktivitenin çok büyük derecelerde artmasını sağlamıştır. Denetim açısından ciddi bir avantaja sahip olan siber terör özellikle karar alıcılar açısından tercih edilir bir noktada yasadışı gruplarla iş birliğini de kolaylaştırmıştır.

Tablo-2. Klasik Terör ile Siber Terör Arasındaki Farklar (Bayraktar, 2015: 77)

	Klasik Terör	Siber Terör
Kullanılan Araç	Silah, bomba gibi araçlar	Çipler, bilgisayarlar veya bilgi sistemlerinde kullanılan diğer donanımlar, yazılımlar
Amaç	Siyasi rejime ve topluma mesaj vermek için terörizm bir amaç	Yaplan eylemler ile topluma veya devlete zarar verme, siyasi ve sosyal olarak etkilemek için terörizm bir amaç
Etki Alanı	Saldırının yapıldığı bölge ya da alan ile sınırlı	Ulusal veya uluslararası boyutlarda etkili
Karşılaşılan Risk	Eylemi gerçekleştiren kişi ya da grup yaşamsal risk altında	Herhangi yaşamsal riski olmadan etkili saldırı
Denetim	Terörü kontrol altında tutma, izlemek ve yok etmek kısmi anlamda mümkün	Siber teröristleri tespit etmek veya yok etmek imkansız
Uygulanacak Ceza	Suçun niteliğine göre uygulanacak ceza belli	Suçun niteliğine göre uygulanacak ceza belli

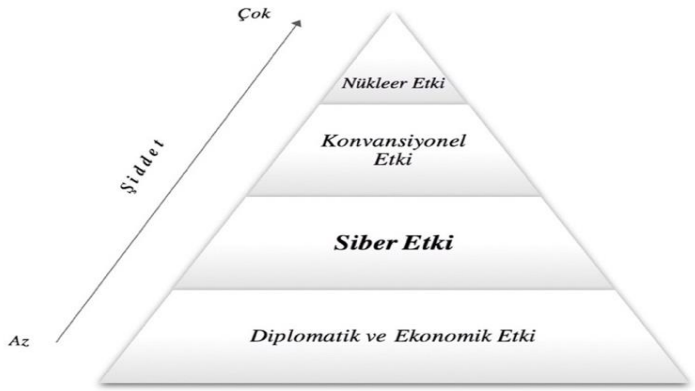
5. SİBER CAYDIRICILIK

Caydırıcılık bir devlet veya topluluğun, başka bir devlet veya topluluğun aleyhine olabilecek hareketlerden sakınması için gerekli tedbirleri alması olarak tanımlanmaktadır. Caydırıcılık bir bakıma, anlaşmazlığın tırmanarak askerî kuvvet kullanımını gerektirmesine engel olmaktadır. Uluslararası güvenlik literatüründe caydırıcılığın *esirgeme (deterrence by denial)* ve *missileme (deterrence by retaliation)* olmak üzere iki yönü bulunmaktadır (İduğ ve diğerleri, 2013: 287).

Caydırıcılık dediğimiz kavram stratejik olarak farklı tarzlarda incelenmektedir. Bazıları tekil (tek defalık), bazıları tekrarlı, bazıları simetrik (karşılıklı), bazıları ise asimetrik (tek taraflı) olabilir. *Siber caydırıcılık* kavramı üzerinden birçok çalışmaya dair tespitler, caydırıcılık kavramının Soğuk Savaş teorileriyle kıyaslanması üzerinden ele alınmaktadır ve tartışılmaktadır (Lupovici, 2011: 51). Bunun en önemli sebebi caydırıcılığa ilişkin uluslararası ilişkiler perspektifinde daha önce bahsettiğimiz iki yönlülüğe dair, savunmayla ilgili kargaşa ve yanlış anlaşılmanın mevcut oluşudur. Siber saldırıların bir yönü vardır fakat savunması zordur ve tespitine ilişkin kesin veriler kimi zaman olmayabilmektedir.

Libicki (2009) verisel gelişmelere bağlı olarak siber etkiyi ve oluşturduğu caydırıcılığın, diplomatik ve ekonomik yaptırımların önüne geçtiğini yapmış olduğu karşılaştırma ile göstermiştir. Şekil 4'te görüleceği üzere, hâlâ konvansiyonel ve nükleer etkinin sahip olduğu caydırıcılık temeli şiddet olarak daha üstlerde yer alsa da konvansiyonel ve nükleer

altyapıların siber altyapılara bağlandığı uluslararası sistemde bu şiddet sarmalı ve hiyerarşisi her an değişiklik gösterebilir ve hatta farklı örneklerde siber etki üst sıralara taşınabilir. Martin Libicki'ye göre siber caydırıcılık Soğuk Savaş dönemindeki nükleer caydırıcılık gibi işe yarayabilir. Fakat bunun imkânlı olması için devletlerin siber uzaya bağlılığı tam ve eksiksiz olmalıdır.



Şekil-4. Siber Caydırıcılığın Etkisel Olarak Karşılaştırılması (Libicki, 2009: 29)

Nükleer caydırıcılık, tekil ve simetrik bir özellik göstermektedir. Tekil olmasının sebebi etkilerinin korkutucu ve geri dönüşünün olmayışından kaynaklanmaktadır. Bu anlayış çerçevesinde kimse nükleer etkiyi kullanmaya cesaret edememektedir. Misilleme durumunda karşı tarafın saldırıya cevap vermesi ile her iki taraf için büyük yıkım olabilir. Siber caydırıcılıkta ise tekrarlılık söz konusudur. Uygulanan siber misilleme, muhtemelen saldıran devleti bertaraf etmez, hükümetin düşmesine neden olmaz veya saldıranın silah bırakmasını sağlamaz. Siber saldırılar emsaller arasında meydana geldiği için aynı zamanda simetrik bir özellik gösterir (Çifçi, 2013: 306). Uluslararası güvenlik açısından siber saldırıların savunulmasındaki belirsizlik ya da kimi zaman anlam kargaşası, klasik anlayış açısından caydırıcılığın farklı tarzlarda gerçekleşmesi ve hiyerarşisi açısından bir tespiti gerekli kılmaktadır (Hosein ve Eriksson, 2007: 162).

Siber caydırıcılığa yapılan en büyük eleştiri bir siber saldırının nereden gerçekleştiğini bulmanın güç oluşudur. Siber savunma kabiliyeti yüksek olduğu sürece siber saldırılar boş çaba olarak görülecek ve bu yola başvurulmayacaktır. Böylece siber savunma kendi başına bir caydırıcılık

sağlayacaktır. Stuxnet örneği göstermiştir ki, hedefte büyük tahribata yol açmayan siber saldırılar güvenlik açıklarının görülmesini sağlayarak bu açıklıkların giderilmesine olanak verecek ve bir sonraki benzer saldırıları boşa çıkarabilecektir (İduğ ve diğerleri, 2013: 288).

Libicki'nin modeliyle benzerlik gösteren tırmanma modelinde saldırıların niteliğine göre tırmanmanın en üstünde nükleer silahlar yer almaktadır. Bendiek ve Metzger (2015: 11) yapmış oldukları bu analizde, Şekil 5'te görüleceği üzere yüksek seviyeli siber saldırıların niteliksel olarak kinetik vuruşlardan daha etkin olduğunu vurgulamıştır ve özellikle son yıllardaki gelişmelere paralel olarak bu doğru bir tespittir. Kritik altyapılara ilişkin fiziksel saldırıların niteliği korkutucu boyutlarda etki yaratma kapasitesine sahiptir. Düşük seviyeli siber saldırılar bu kapsamda tırmanma modeli açısından politik ve ekonomik yaptırımlardan daha etkili sonuçlar doğurabilmektedir. İran'ın Natanz Nükleer Santrali'ni hedef alan Stuxnet örneğinde görüldüğü gibi siber dünyada başlatılan ancak fiziksel dünyada yıkıcı sonuçlar doğuran gelişmiş siber silahlar günümüzde yadsınamayacak bir gerçekliktir. Maryland Üniversitesi'nin oluşturduğu *Küresel Terörizm Veri Tabanı*'na (Global Terrorism Database) göre 1970'lerden 1990'lı yılların ortalarına kadar enerji üretim tesislerine, boru hatlarına ve sektör çalışanlarına yönelik yılda 100'den az saldırı kaydedilmişken, yalnızca 2013 yılında bu saldırıların sayısı 600'e yaklaşmıştır (Gücüyener, 2015).

Şekil-5: Tırmanma Modeli (Bendiek ve Metzger, 2015: 11)

Cyber War, The Next Threat to National Security and What to Do About It adlı kitabın da yazarı olan Clarke, *Siber Savaş* olarak adlandırdığı çekişme alanıyla ilgili ABD'de bağımsız bir merkezin yürütülmesinde önemli görevler almıştır. Richard Clark'ın özellikle caydırıcılık ve siber caydırıcılığın bütününe ilişkin yapmış olduğu tespitler kayda değerdir ve düzlem olarak siber uzaya ilişkin verdiği örnek ve anlatım şu şekildedir (Clarke ve Knake, 2011: 98):

> *"…Gerçek dünyada ABD neden olacağı karşı saldırının Amerikan ağları üzerindeki asimetrik etkisinden çekineceği için büyük ölçekli siber savaş başlatmayacaktır.*
> *…Ancak, 1960'lı yıllarda kitaplar yazmış olan Herman Kahn gibi stratejistlerin teorilerinin aksine, siber savaş caydırıcılığı çok daha değişik olasılıklar içermektedir. Nükleer silahlara ilişkin bütün ayrıntılar bilinmektedir. Siber silahların ise ne yapacağı şu ana kadar dünya devletleri tarafından gözlenmemiştir.*
> *…Nükleer savaşta iki tarafın da saldırı kabiliyetleri bilindiği için, ortada bir sır yoktu ve herhangi bir saldırı anında büyük bir olasılıkla dünyadaki tüm yaşamın yok olacağını herkes bilmekteydi. Siber savaşta ise, saldırının gücü bir sır olarak kalmaya devam ediyor. Etkin bir savunma kurma olasılığı var. Bu yüzden, hiçbir ulus bir kriz halinde caydırıcılıktan dolayı siber silah kullanmazlık etmeyecektir."*

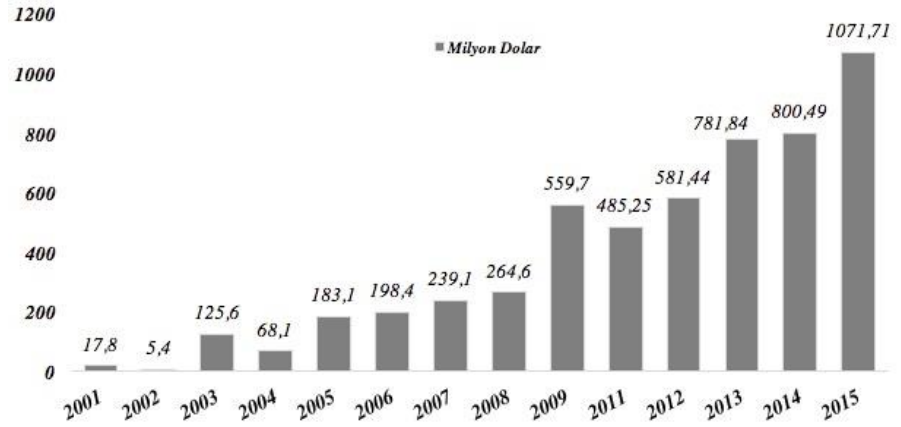
6. SİBER SAVAŞLAR GERÇEK Mİ?

Toplumlararası ilişkilerin doğası çatışmaya dayalıdır. Bu çatışma bazı dönemlerde açık bir hal alırken bazı dönemlerde kendisini gizlemiştir. Uluslararası ilişkiler çalışmaları adına kırılma noktası olan I. Dünya Savaşı'nın öncesinde ve 1815 Viyana Kongresi sonrasında Avrupalı güçler arasında hâkim olan hava artık Avrupa coğrafyasında bir savaş olmayacağı, ortaklıklara daha fazla vurgu yapılacağı yönündeydi (Toptaş, 2009: 15). Fakat 20. yüzyıl içerisindeki başdöndürücü gelişmeler tarihin gördüğü en büyük iki savaşı beraberinde getirmiştir.

Yaşanan iki savaş ve çıkarılabilecek derslerin aksine değişimin getirmiş olduğu imkânlar ve stratejiler askerî unsurların yıkıcı özelliklerini inanılmaz boyutlara taşımıştır. Bu durumu göze almak istemeyen aktörler birbirlerini caydırmada ve etkilemede farklı saldırı ve savaş tekniklerini geliştirmeye başlamıştır. *Siber savaş* olarak adlandırdığımız gücün göreceliği üzerine kurulu küresel mücadele ciddi bir karmaşıklığı beraberinde getirmiştir.

Karmaşıklığın özü sadece savaş alanına ilişkin verilerle evrimini devam ettirmemiştir. Siber savaşın maddi ve fiziksel olarak etkisi ciddi bir maliyeti beraberinde getirmiştir. Grafik 2'de IC3'e raporlanan maddi kayba ilişkin verilerde son 15 yılda yaşanan değişimin ciddi bir artış içinde olduğu

gözlenmektedir. Uluslararası sistemde toplam maliyetin uluslararası aktörler bazında ne kadar olduğuna dair kesin veriler olmasa da siber savaşın kapasitesi ve etkisine ilişkin değerler mücadelenin yönünü ortaya koymaktadır.



Grafik-2: 2001-2015 Yılları Arası Siber Saldırı ve Suçlardan Dolayı IC3'e Raporlanan Maddi Kaybın Değişimi (The Statistics Portal, 2016)

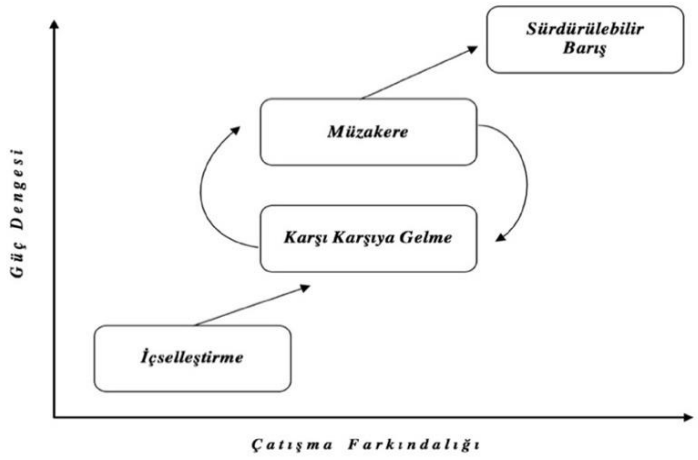
a) Asimetrik Savaş

Özellikle 11 Eylül sonrası dönemde kendisine yoğun biçimde referans verilmeye başlanan *asimetrik savaş* kavramı kimilerine göre yeni bir savaş mantığına karşılık gelmekte kimilerine ise yeni bir terör türünü çağrışım yapmaktadır. Asimetri farklı düşünerek, farklı örgütlenerek, farklı hareket yöntemleri seçerek mevcut dengeyi bozmaktır. Var olan dengenin bir dengesizlik üzerinde kurulduğu düşünülecek olursa yürütülen mücadele yöntemlerinin anlayışsal boyutu tartışma konusudur. Tarafların aynı kuvvet unsurlarını kullanmasıyla karşımıza çıkan simetrik savaşa karşın asimetrik savaşta düşmanın dengesini kaybettirme adına tarafların birinde olmayan farklı unsurlar karşımıza çıkabilir. Bu yönüyle asimetrik savaş benzeşmeyen güç unsurlarının, muharabe yöntemlerinin, vasıta ve silahlarının kullanıldığı savaştır (Varlık, 2013: 125). Asimetrik güç etkinliği teknolojik üstünlük, nitelik, sevk ve irade, komuta-kontrol, disiplin-moral ve motivasyon üstünlüğü gibi kuvvet çarpanı olabilecek herhangi başka bir unsurun devreye girmesiyle ortaya çıkmaktadır.

Farklı unsurların ortaya çıkışıyla asimetrik savaş adına rakip hedeflere yönelik zararın kapsamı daha da artmıştır. Düşmanın modern koşullar altında görünür niteliğinin kaybolması, saldırganlık güdüsünü ortadan kaldırmaktadır. Asimetrik unsurlarla savaşın devamlılığı *ölçülülük* düşüncesini de ortadan kaldırmaktadır ve savaşın ruhuna yeni bir boyut katmaktadır. Özellikle konvansiyonel silahların değişimi ile birlikte askeri kayıpların yanında, inanılmaz boyutlardaki sivil kayıpları savaşın olumsuz şekillerde ve asimetrik ölçülerle devam ettiğini ispatlamıştır (Aral, 2007: 60).

Savaşın evrimine ilişkin asimetrik savaş dâhilindeki değişimin 11 Eylül saldırıları ile uluslararası toplumun gündemine taşındığı kabul edilmektedir (Bendrath ve diğerleri, 2007: 71). Fakat Soğuk Savaş sonrası uluslararası güvenlik ortamında yaşanan değişimlerin bir sonucu olarak devlet ve devlet dışı aktörler tarafından uygulanabilecek bir savaş anlayışı olduğuna ilişkin yaklaşımlar da asimetrik savaş adına mevcuttur. Bu anlayışa siber saldırılar kapsamındaki taktiksel unsurları ve gelişmeleri de dâhil edebiliriz.

Şekil 6'da görüldüğü üzere, yapısal olarak ortaya koyulan asimetrik çatışma sürecinde güç ve çatışmaya ilişkin taraflar arasındaki müzakere kültürü barışın sağlanmasında önemli bir basamaktır. Güç dengesi ve çatışma farkındalığı ekseninde ele alınan asimetrik çatışmanın evreleri sürdürülebilir barış noktasında kesişim olarak en üst dereceyi oluşturmaktadır.



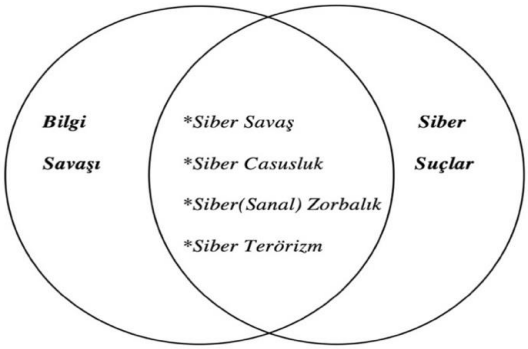
Şekil-6: Yapısal Olarak Asimetrik Çatışmanın Evreleri (Gallo ve Marzano, 2009)

Propaganda ve bilgi savaşına dayandırılan psikolojik harekâtlar da asimetrik savaş kavramı içerisinde siber güvenlik alanına dair bir parametre olarak ele alınabilir. Herhangi bir savaş alanına ihtiyaç duymadan gerçekleştirilebilen psikolojik harekâtların ihtiyaç duyduğu siber ortam harekât sürecini taraflara sunmaktadır. Kavramsal temeller ve asimetrik yaklaşımları değerlendiren bir taraf, güçlü rakibin bir yandan zayıf yönlerini alışılmadık taktiklerle saptarken diğer yandan kamuoyunda şok ve ani psikolojik etki yaratmayı ve bu güçlü tarafın kurumlarına duyulan güveni zayıflatmayı amaçlayabilir. Böylelikle rakibin toplumsal yapısında, özellikle ekonomisinde ve motivasyonunda negatif etki yaratarak toplumsal özgürlüklerin kısıtlanmasına bile neden olabilir.

b) Siber Savaş

Siber Savaş kavramını; "*ulusal bir hedefi gerçekleştirmek ya da süregelen bir savaşı desteklemek amacıyla, bir ülke tarafından veya inisiyatifinde, diğer bir ülkenin askeri ve sivil her türlü bilişim sistem ve altyapısının işlevselliğini engellemek, imha etmek ve kendi çıkarları doğrultusunda kullanmak için siber savaş yöntemlerinin kullanılması ve buna karşı koyacak tedbirler veya süreçler"* şeklinde tanımlamak mümkündür (Bayraktar, 2015: 48). Richard Clark'ın kavramsal olarak siber savaşa yüklediği anlam, *"Bir devletin, başka bir devletin bilgisayar sistemlerine veya ağlarına hasar vermek ya da kesinti yaratmak üzere gerçekleştirilen sızma faaliyetleridir."* şeklindedir ve kapsamı dar tutulmuştur. Bunun en önemli sebeplerinden birisi enformasyon sahibi olma veya çalınması şeklindeki yaklaşımın tanımsal olarak genişliğidir. Siber savaş bilgi teknolojilerine bağlı olarak ve siber suçlardaki farkındalığın artışıyla çıkarsal amaç içerisinde hareket eden aktörlerin ilgi alanına girmesiyle bugünkü küresel niteliğine ulaşmıştır.

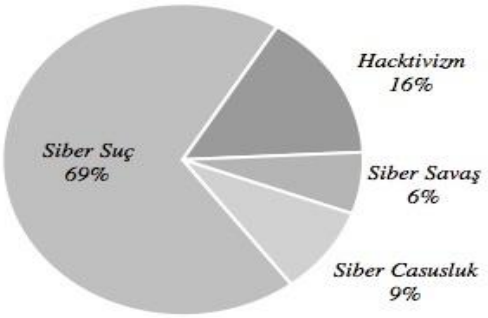
Şekil 7'deki kombinasyon dâhilinde bilgi savaşı ve siber suçlar *siber savaş*, *siber casusluk*, *siber zorbalık* ve *siber terörizm* gibi unsurları karşımıza çıkarmıştır. Bilgi savaşı ve siber suçlar uluslararası alana ilişkin sorunsal bütünlüğü artırırken diğer yandan teknolojik altyapının gelişmesinde/geliştirilmesinde dinamo görevi üstlenmektedir. Devletlerin savaş, casusluk, terörizm gibi unsurların karşılanmasına ilişkin algıları ar-ge faaliyetlerini siber alana kaydırmaktadır. Bu konuda devletlerin özel sektörle olan birlikteliği yapısal olarak çeşitli düzeylerde spekülasyonları da beraberinde getirmektedir.



Şekil-7: Geleneksel Bilgi Savaşı ve Siber Suç Kombinasyonu Olarak Siber Savaş (Merrick ve diğerleri, 2016: 5)

Yılmaz (2006: 615) bilgi savaşını; *"Karşı tarafa ait bilgi tabanlı işlemcileri, bilgi sistemlerini, bilgisayar tabanlı network sistemlerini etkileyecek bir hareket gerçekleştirmek ve kendi sistemlerini korumak."* şeklinde tanımlamıştır. Bilgi savaşı askerî bir boyutu olmasıyla beraber daha çok bilgi sistemlerini çökertmeye yönelik internet savaşlarını tanımlayan bir üst kavramdır. Bilgi savaşı ve siber suçlara yapılan atıfların yanında küresel olarak siber savaşın gelişimine ilişkin bazı yaklaşımlarda siber suçlar direkt olarak adres gösterilmektedir. Carr (2012: 5) *Inside Cyber Warfare* adlı çalışmasında sorunun askerî bir problem olduğunu ve derlediği diğer çalışmalara ilişkin, hukuksal bazı zorlayıcı unsurlarla siber savaşın bir kombinasyon içerisinde değerlendirilmesi gerektiğini vurgulamaktadır. Siber suçlar yazılımsal olarak bazı zararlı unsurların hareketliliği ile gelişmekte, siber savaş ise test edilebilen unsurlarla evrimini sürdürmektedir.

Her ne kadar siber savaşa dair gerçeklik ve gelişen olaylar daha önce vurgulanan tespitlere ilişkin süregelse de özellikle siber suçlara ilişkin ve iç hukuktan dolayı sonuç doğurabilecek gelişmeler siber savaş algısının önünde gözükmektedir (Rawnsley, 2008: 83). Grafik 3'te görüleceği üzere, siber savaşın sahip olduğu motivasyon düzeyi saldırıların kaynaklandırılış şekline göre oldukça düşük bir orana sahiptir. Siber savaşın motivasyon düzeyi düşük olmasına rağmen etki alanının belirginliği ve genişliği diğer unsurlara göre değişkenlik göstermektedir. Özellikle bireysel olarak çoğu zaman maddi kazançların sağlanması siber suçları oldukça öne taşımaktadır. *Hackmageddon; Information Security Timeline and Statistics*'ten alınan verilere göre aylık olarak dalgalanmalar belirgin şekilde, dört unsur dâhilinde değişmektedir. Haziran 2016 dönemine izlenen verilerde Mayıs 2016'ya göre siber suçlar %66.7'den az bir artışla, %69'a; hacktivizm %20'den düşerek %16 değerinde ifade edilmiştir.



Grafik-3: Saldırıların Motivasyonu (Passeri, 2016)

Siber savaş amaçlanılan unsur ve kapsamına göre stratejik ve operasyonel olmak üzere ikiye ayrılmaktadır. Stratejik siber savaşlar amaçlarına, olanaklarına, sınırlarına ve yürütülme şekline göre operasyonel siber savaşlardan daha geniş bir alanda kendini göstermektedir.

(1) Stratejik Siber Savaş

Libicki (2009: 117) stratejik siber savaşı bir devlet veya onun toplumuna karşı yürütülen fakat birincil amaç olarak devletin davranışını etkilemeyecek bir siber saldırı bütünü olarak tanımlamıştır. Saldıran birim devlet veya devlet dışı bir aktör olabilmektedir. Özellikle devlet dışı aktörler açısından saldırılan itibarıyla karşılık bulma ve tepki, daha güç ve karmaşık bir hal almaktadır. Devletler ise saldırılan ülke açısından diplomatik ve ekonomik birtakım yaptırımlarla karşılaşabilir.

Devletler stratejik siber savaşlarda provokasyon ve tırmandırma şekilleriyle farklı yollardan taktiksel unsurları benimseyebilir. Saldırılan aktör ise karşılıklı tırmandırma yoluyla çatışmanın boyutunu farklılaştırabilir. Bu durumda siber savaşın sınırlarının ne olduğu konusu gündeme gelmektedir. Her ne kadar nükleer tırmanmada pratik bir husus olan ikinci vuruş yeteneği tartışılsa da siber savaşlarda ikinci vuruş yeteneği olarak saldırı metotlarının ele alınması yakın gelecek için önemli bir husustur. Her iki taraf açısından yönetimsel olarak diplomatik tercihlerin mi kullanılacağı ya da kriz yönetimi kapsamında mı adımlar atılacağı farklı tercihler olarak masa üzerinde yer alacaktır.

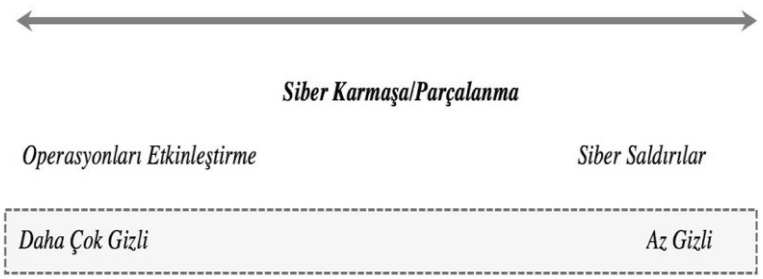
Rusya'nın 2007 Estonya ve 2015 yılı Ukrayna'ya karşı yürütmüş olduğu müdaheleler stratejik siber savaşa tipik örnekler olarak karşımıza çıkmaktadır. Stratejik siber savaşlar açısından devlet içi sistemin aksatılması ve toplumsal olarak psikolojik harekâta örnek oluşturabilecek bu türden olaylarda kısa dönem ve uzun dönemde devlet altyapılarında hasarların onarılması, nükleer ve konvansiyonel unsurların bıraktığı yıkıcı etkilere göre daha kolaydır.

(2) Operasyonel Siber Savaş

Libicki (2009: 139) operasyonel siber savaşı; *"Askerî hedeflere ve askerî bağlantılı sivil hedeflere savaş zamanı yürütülen siber saldırılar."* olarak tanımlamıştır. Profesyonel bir müdaheleyi içeren saldırılarda dikkatli ve eksiksiz bir şekilde, zamanında uygulanan güç unsurları olmalıdır.

Operasyonel siber savaş düzleminde eş zamanlı müdahale çeşitleri olduğu için operasyonların etkinleştirilme safhaları gizlilik bütünlüğü dâhilindedir. Şekil 8'deki siber çatışma spektrumunda görüldüğü üzere *siber saldırı* olarak ele aldığımız kavram, boyutsal ve niteliksel olarak daha düşük seviyeler taşıyabileceği için gizlilik konusunda çoğu zaman plan ve program içermeyebilir. Operasyonel siber savaşı da bu bu bağlamda adeta bir askerî çıkarma ya da bir gece yarısı askerî operasyonu gibi algılayabiliriz.

Siber çatışma spektrumu operasyonel boyut içindeki gizliliğin siber saldırıların yönüne göre daha fazla gizlilik içerdiğini bizlere sunmaktadır. Siber alanda çatışmanın yaşandığı boyut savaşın niteliğine göre değişkenlik göstermektedir. Askerî olarak konvansiyonel içerikli müdahalelerde benzer bir gizliliğin olduğu gözlerden kaçırılmamalıdır. Siber müdahaleler artık benzer bir organizasyonel altyapı gerektirmektedir.



Şekil-8: Siber Çatışma Spektrumu (Brown ve Tullow, 2012)

Operasyonel siber savaşlarda müstakil bir savaş kombinasyonu yoktur ve tekil bir amaç dâhilinde karakteristik özellikler mevcut değildir. Bir konvansiyonel savaşta, müdahale ya da askerî bir amaç güdülecekse fonksiyonel olarak siber unsurlarla destek gözetilmelidir. 2008 yılında Güney Osetya Savaşı esnasında Rusya'nın Gürcistan'a yürütttüğü eş zamanlı siber müdahaleler operasyonel siber savaşın tipik örnekleri arasındadır.

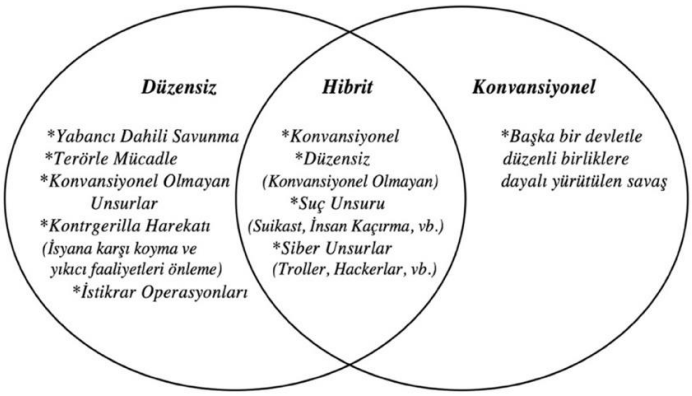
c) Hibrit Savaş

Elektronik savaşın tekniklerinden daha fazlasına ihtiyaç duyulan, geleneksel savaşla birlikte sürdürülen bileşke savaş tarzına *hibrit savaş* adı verilmektedir. Özellikle NATO, Soğuk Savaş sonrasındaki güvenlik ortamının belirsizliği nedeniyle ve örneklerden çıkarılan dersler ışığında geleneksel savaş imkânlarını bırakmadan yenilerine sahip olmayı düşünerek hibrit savaş yöntemini tercih etmiş ve bu konuda farklı raporlar ortaya koymuştur (Bıçakçı, 2012: 210). Çoğu uluslararası ilişkiler çalışmalarında hibrit savaş, operasyonel siber savaş yerine de kullanılmaktadır. Hibrit savaş, siber savaş başlığı altında incelediğimiz operasyonel siber savaşa göre daha özel durumları ve müdahale biçimine de işaret etmektedir.

Savaşın evrimi ve özellikle asimetrik olarak gelişen unsurlar farklı devletler ve NATO gibi örgütler bazında bu konunun tartışıldığı boyutu ortaya çıkarmıştır. Karma savaş olarak da vurgulanan terimsel ifadelerde, konvansiyonel kuvvet ve harekât yöntemleri ile *bilgi harekâtı, bilgi tabanlı (cyber) faaliyetler, gayrinizami harekât, kitle imha silahları* ve *suç örgütlerinin kullanımı* gibi geleneksel olmayan kuvvet ve yöntemlerin kullanıldığı bir muharebe stratejisi tanımlanmaktadır (Varlık, 2013: 125). Askerî yazında *karma savaş* terimi henüz yerleşmemiştir. Bunun yerine, İngilizcede karma ya da melez anlamına gelen *hybrid* sözcüğünün okunuşundan *hibrit savaş* terimi Türkçeye aktarılmıştır.

Hibrit savaş mantığına göre devletler kendilerini, kasıtlı bir tahrikten veya gerginliğin artmasından sonra bir siber savaş içinde bulabilmektedirler. Bir devlet, diğerine karşı kendini avantajlı duruma geçireceğine inandığı için siber saldırıda bulunabilir. Şekil 9'da düzensiz ve konvansiyonel unsurların bileşkesinde hibrit savaşın neleri kapsadığı sunulmuştur. Burada dikkat edilmesi gereken hibrit savaş içerisindeki unsurların gayrinizami nitelikler de taşıyabileceğidir. Suç unsuru oluşturabilecek ve siber unsurlarla birleştirilecek manevralarda amaç rakibi yıpratmaktır.

Hibrit savaş yaklaşımıyla yürütülen harekâtlarda rakibin tamamen devre dışı bırakılması pratikte imkânsız gözükmektedir. Bunun tek yolu rakibin tüm konvansiyonel unsurlarının siber ortama bağlı olması ve bir anda devre dışı bırakılabilme olasılığıdır. Hibrit savaşta asıl hedef bir bölgeyi ele geçirmek veya kontrol etmek değildir.



Şekil-9: Hibrit Savaşın Temel Unsurları (Briefing to the Subcommittee on Terrorism, Unconventional Threats and Capabilities, Committee on Armed Services, House of Representatives, 2010: 16)

Rakibi yıpratmaya yönelik ele aldığımız hibrit savaşta uzun süreli planlar yapılabilir ve zamana yayılabilir. Kısa sürede kesin sonuçlar beklemek hibrit savaşlar açısından gerçekçi durmamaktadır. Rusya'nın 2014 yılında Ukrayna'daki faaliyetleri yine Doğu Avrupa açısından Rusya'nın her fırsatta hibrit savaşı bir harekat biçimine dönüştürebileceği gerçeğini ortaya koymuştur. Karar alıcılar açısından yeni bir konseptin önlerinde olduğunu ortaya çıkaran benzer müdahaleler NATO gibi örgütlenmelerin de ajandalarında ilk sıralara yükselmiştir. Özellikle Rusya hibrit savaş uygulamalarıyla ile birlikte, Soğuk Savaş sonrasında son 15 yılda gücünden söz ettiremezken yeniden atağa geçmiştir. Rusya'nın özellikle Estonya ve Ukrayna gibi ülkelerde açığa çıkan saldırıları ve faaliyetleri bölge ülkelerini de tedirgin etmeye başlamıştır.

SONUÇ OLARAK;

Uluslararası ilişkiler boyutunda *siber politikalar* adı altında çalışma aritmetiği bulan siber güvenlik, siber saldırılar ile birlikte yeni bir çalışma alanını karşımıza çıkarmıştır. Ulus devletlerin veya bu düzeyde tartışma niteliği gösteren güncel çalışmalar da siber güvenlik konseptine ve özüne atıflarda bulunmaktadır. *Askerî işlerde ve gelişmelerde devrim* olarak adlandırılan bu durum elektronik, ileri teknolojik savaş unsurlarının ortaya çıkmasıyla çok boyutlu bir paradoks haline dönüşmüştür.

Siber savaş gibi bir olgunun askerî teknolojiler açısından önemli olduğu, konvansiyonel ve nükleer silahlar ile bunların caydırıcılığı gibi unsurlar bakımından ortak bir hiyerarşide yer alması ayrı bir öneme

sahiptir. Bu başlığın şekillenmesinde uluslararası ilişkiler temeli açısından kritik altyapıların, iletişim sistemlerinin ya da özelde hava savunma sistemleri gibi birçok unsurun tehlikede olması ve caydırıcı bir özellik kazanması siber güvenliği önemli bir analiz düzeyine taşımaktadır.

Siber savaş belli yönleri itibarıyla asimetrik çatışmalara benzetilmektedir ve bunu güçlendiren en önemli gösterge, zayıf durumda olanın da kimi manevralarla güçlü veya baskın olanı alt edebileceği ile ilgilidir. Uluslararası ilişkiler boyutundaki tartışma alanı ve konunun ele alındığı boyut bu yönde yoğunlaşmaktadır. Uluslararası aktörler adına makro savaş teorileri açısından kimi zaman tarafların ihtiyacı olan basit bir bilgisayar ve yazılım olabilmektedir. Bu derece basite indirgediğimiz bir durumla ilgili de doğal olarak ilk eleştiri siber savaşta kullanılan silahların, iyi birer silah olmadığı ile ilgili durumdur ve düşmana ciddi, yıkıcı zararlar vermediği için kışkırtma açısından bir riski içinde barındırabileceğidir.

Siber savaşların ve saldırı niteliklerinin nereden geldiği ile ilgili tespitler yapılabilmekte, sorumlular kimi zaman kolaylıkla ortaya çıkarılabilmekte ve bu durum uluslararası düzeydeki saldırgan yapıyı daha da körükleyebilmektedir. Bu ve benzeri türden siber güvenlik ile ilgili yaklaşımlarda, uluslararası politika açısından diplomasi masaları tesis edilebilir ve bunların uygulamadaki başarılarına göre çalışmalar oluşturulabilir. Bu çerçevede devlet merkezli olaya yaklaşılması ve siber güvenlik gibi alanın tek pencereden incelenmesi çoğu zaman teorik olarak beraberinde belirli sorunsalları getirse de çalışmanın temelinde bu sorunsalı kırma isteği yer almaktadır.

Bu boyutlar açısından ele alındığında, siber savaşın günümüzde çağdaş devletler açısından bir tehdit oluşturduğu, ciddi bir problem sahası ve tartışma alanı haline geldiği bir gerçektir. Eksik olan ise, uluslararası ilişkilere ilgi duyanlar açısından konunun hangi teorik yaklaşımlarla ele alınacağıdır. Görünen güçlerin, görünmeyen saldırısı haline gelen siber saldırılar, devletlerin ulusal güvenlikleri açısından ciddi bir risktir ve konunun analizi açısından önemli bir tartışma noktasını oluşturmuştur. Bu doğrultuda devletlerin siber alandaki tehditlerle mücadele edebilmek amacıyla siber savunma yöntemlerini geliştirdikleri, siber tehditlere karşı önleyici bir yaklaşımla siber taarruz tekniklerini araştırdıkları ve bu alanda politikalar geliştirdikleri bilinmektedir.

11 Eylül olaylarının yeni tehditleri beraberinde getirdiği yaklaşımda, hem siber güvenlik anlayışındaki hem de siber alandaki çeşitlilik benzer çalışmaların konseptini oluşturmuştur. Siber alandaki savunma ve saldırı

çeşitliliği güçlü ülkelerin her an tetikte olmaları gerektiğini göstermiştir. Birçok devlet için ise Soğuk Savaş'ın bitimi, güvenlik sorunları bağlamında çözümleri zor paradoksları oluşturmuştur. Siber kapasiteye dayandırılan unsurlar için ekonomik çıkar ve düşmanı zarara uğratma gibi arayışlar kendini hissettirmeye başlamıştır.

Siber güvenlik kavramının dâhil olduğu uluslararası güvenlik temelinde, nükleer caydırıcılığın hâlâ ulusal güvenlik konusunda en büyük tehlike olduğu ortadadır. Nükleer, kimyasal ve biyolojik kitle imha silahlarının yaygın olduğu sorunlarla birlikte, farklı sorunların devletleri meşgul ettiği süreçte güvenlik yaklaşımı ve yaklaşımın çeşitlendiği siber alandaki tehditsel durum her geçen gün artmakta ve bu durum politik girişimlerin rasyonelliğinin tartışılmasını gerekli kılmaktadır. Farklı alanlarda olduğu gibi devletler, güvenlik temelindeki tehlikeleri bertaraf etmek için rasyonel olduklarını zannettikleri birçok konuda çoğu zaman ittifak arayışlarına girmektedir. Tartışmaları da alevlendiren husus, uluslararası alanda ortak güvenlik oluşturulacaksa, bu anlayışın samimiyeti ve tarafsızlığı yönündeki atıflar olmaktadır. Ortak bir uluslararası aklın ortaya çıkamamasındaki temel nedenler zaten karmaşıkken siber güvenlik gibi bir konunun alana dâhil olması kartları çeşitlendirmiştir.

KAYNAKÇA

Aral, Berdal (2007), "Asimetrik Saldırı Savaşları, Siyaset ve Uluslararası Hukuk", **Uluslararası İlişkiler Dergisi**, 4(14), 39-83.

Arnold, Todd ve diğerleri (2013), "Professionalizing The Army's Cyber Army's Cyber Officer Force", **Army Cyber Center**, http://www.gregconti.com/publications/pro_ cyber.pdf (13.04.2016).

Barnum, Sean (2014), "Standardizing Cyber Threat Intelligence Information with The Structured Threat Information Expression", **STIX Whitepaper,** (1.1) http://stixproject.github.io/getting-started/whitepaper/ (12.04.2016).

Bayraktar, Gökhan (2015), **Siber Savaş ve Ulusal Güvenlik Stratejisi**, İstanbul: Yeniyüzyıl Yayınları.

Bendiek, Annegret ve Metzger, Tobias (2015), **Deterrence Theory in the Cyber Security, Working Paper RD EU/Europe**, Berlin: Research division/EU.

Bendrath, Ralf ve diğerleri (2007), "From 'Cyberterrorism' to 'Cyberwar', back and forth: How The United States Securitized Cyberspace", Johan Eriksson ve Giampiero Giacomello (Ed.), **International Relations and Security in The Digital Age**, 1. Baskı *içinde* (57-83), New York: Routledge Publishing.

Bıçakçı, Salih (2012), "Yeni Savaş ve Siber Güvenlik Arasında NATO'nun Yeniden Doğuşu", **Uluslararası İlişkiler Dergisi**, 9(34), 205-226.

Brown, Gary D., Tullow, Owen W. (2012), "On the Spectrum of Cyber Space Operations", **Small War Journals**, http://smallwarsjournal.com/jrnl/art/on-the-spectrum-of-cyberspace-operations (04.02.2016).

Bucci, Steven (2009), "The Confluence of Cyber Crime and Terrorism", **Lecture#1123 on National Security and Defence**, http://www.heritage.org/research/lecture/the-confluence-of-cyber-crime-and-terrorism (13.01.2016).

Burgess, Heidi ve Guy M. Burgess (1997), **Encyclopedia of Conflict Resolution**, California: ABC-CLIO, Santa Barbara, California.

Carr, Jeffrey (2012), **Inside Cyber Warfare**, 2nd Ed. Sebastopol: O'Reilly Publishing.

Caşın, Mesut Hakkı (2008), **Uluslararası Terörizm**, Ankara: Nobel Yayın Dağıtım.

Choucri, Nazli (2012), **Cyberpolitics in International Relations**, Cambridge: MIT Press.

Clarke, Richard A. ve Knake, Robert K. (2011), **Siber Savaş: Ulusal Güvenliğe Yönelik Yeni Tehdit**, (Çev. Murat Erduran), İstanbul: İKÜ Yayınevi.

Çakmak, Haydar ve Demir, Cenker Korhan (2009), "Siber Dünyadaki Tehdit ve Kavramlar", Haydar Çakmak ve Taner Altınok (Ed.), **Suç, Terör ve Savaş Üçgeninde Siber Dünya**, 1. Baskı *içinde* (23-55), Anakara: Barış Platin Kitabevi.

Çifçi, Hasan (2013), **Her Yönüyle Siber Savaş**, Ankara: TÜBİTAK Bilim Kitapları.

Gallo, Giorgio ve Marzano, Arturo (2009), "The Dynamics of Asymmetric Conflicts: The Israeli-Palestinian Case", **The Journal of Conflict Studies**, Volume 29.

Gray, Colin S. (2007), **War, Peace and International Relations: An Introduction to Strategic History**, New York: Routledge Publishing.

Gücüyener, Ayhan (2015), **Enerji Güvenliğinde Yeni Bir Arayış**, https://www.linkedin.com/pulse/enerji-güvenliğinde-yeni-bir-arayış-ayhan-gucuyener?forceNoSplash=true (15.06.2015).

Hayes, Richard E ve Alberts, David S. (1995), "Information Warfare and Deterrence: Appendix B. The Realm of Information Dominance: Beyond Information War", **Federation of American Scientists**, http://fas.org/irp/threat/cyber/docs/iwd/appb .html (08.01.2016).

Hosein, Ian ve Eriksson, Johan (2007), "International Policy Dynamics and The Regulation of Dataflows: Bypassing Domestic Restrictions", Johan Eriksson ve Giampiero Giacomello (Ed.), **International Relations and Security in The Digital Age**, 1. Baskı *içinde* (158-172), New York: Routledge Publishing.

İduğ Y. ve diğerleri (2013), "Siber Caydırıcılık ve Türkiye'nin İmkan ve Kabiliyeti", **6. Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansı Bildiriler Kitabı**, 1. Baskı *içinde* (287-290), Ankara: Bilgi Güvenliği Derneği.

Libicki, Martin C. (2007), **Conquest in Cyberspace: National Security and Information Warfare**, Cambridge: Cambridge University Press.

Libicki, Martin C. (2009), **Cyberdeterrence and Cyberwar**, Santa Monica: Rand Corporation.

Little, Richard (2007), **The Balance of Power in International Relations: Metaphors, Myths and Models**, Cambridge: Cambridge University Press.

Lupovici, Amir (2011), "Cyber Warfare and Deterrence: Trends and Challenges in Research", **Military and Strategic Affairs**, 3(3), 49-62.

Merrick, Kathryn ve diğerleri (2016), "A Survey of Game Theoretic Approaches to Modelling Decision-Making in Information Warfare Scenarios", **Future Internet**, 8 (3), 1-29.

Nye, Joseph S. (2010), **Cyber Power**, Cambridge: Harvard Kennedy School, Belfer Center for Science and International Affairs.

Passeri, Paolo (2016), "June 2016 Cyber Attacks Statistics", **Hackmageddon Information Security Timelines and Statistics**, http://www.hackmageddon.com/2016/07/25/16-30-june-2016-cyber-attacks-statistics/ (03.06.2016).

Rawnsley, Gary D. (2008), "The Laws of The Playground: Information Warfare and Propaganda Across The Taiwan Strait", Athina Karatzogianni (Ed.), **Cyber Conflict and Global Politics**, 1. Baskı *içinde* (79-94), London: Routledge Chapman Hall.

Singer, P.W. ve Friedman, Allan (2015), **Siber Güvenlik ve Siber Savaş**, (Çev. Ali Atav), Ankara: Buzdağı Yayınları.

Sönmezoğlu, Faruk (2014), **Uluslararası Politika ve Dış Poltika Analizi**, 6. Baskı, Der İstanbul: Der Yayınları.

Stevens, Tim (2012), "A Cyberwar of Ideas? Deterrence and Norms in Cyberspace", **Contemporary Security Policy**, 33(1), 148-170.

Stone, John (2012), "Cyber War will Take Place", **Journal of Strategic Studies**, 36(1), 101-108.

The Statistics Portal (2016a), "Amount of Monetary Damage Caused by Reported Cyber Crime to the IC3 from 2001 to 2015", http://www.statista.com/statistics/267132/total-damage-caused-by-by-cyber-crime-in-the-us/ (03.05.2016).

Toptaş, Ergüder (2009), **21. Yüzyılda Savaş**, Ankara: Kripto Yayınları.

United States Government Accountability Office (2010), **Briefing to the Subcommittee on Terrorism: Unconventional Threats and Capabilities**, Washington DC: Committee on Armed Services, House of Representatives.

Varlık, Ali Bilgin (2013), "Savaşı Tanımlamak, Terminolojik Bir Yaklaşım", **Avrasya Terim Dergisi**, 1(2), 114-129.

Vinnakota T. (2013), "Understanding of Cyberspace Using Cybernetics: An Imperative need for Cybersecurity of Enterprises", **IEEEXplore**, http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=6865791 (18.01.2016).

Viotti, Paul R. ve Kauppi, Mark V. (2014), **Uluslararası İlişkiler ve Dünya Siyaseti**, (Çev. Ayşe Özbay Erozan), Ankara: Nobel Yayıncılık.

Walt, Stephen M. (2003), "Güvenlik Çalışmalarının Rönesansı", **Avrasya Dosyası**, 9(2), 71-107.

Wiener, Norbert (1948), **Cybernetics, or Control and Communication in the Animal and the Machine**, Cambridge: MIT Press.

Yılmaz, Sait (2006), **21. Yüzyılda Güvenlik ve İstihbarat**, İstanbul: Alfa Yayınları.