International Journal of Academic Value Studies (Javstudies)

ISSN:2149-8598 | *Vol: 3, Issue: 9, pp. 24-34*
www.javstudies.com | *Javstudies@gmail.com*

Disciplines: Business Administration, Economy, Econometrics, Finance, Labour Economics, Political Science, Public Administration, International Relations

ABD-ÇİN REKABETİ BAĞLAMINDA SİBER SAVAŞ

Cyber Warfare In The Context Of Us-China Rivalry

Öğr.Gör. Altun ALTUN
Hakkari Üniversitesi, altunaltun6@hotmail.com

Altun, A., (2017), Abd-Çin Rekabeti Bağlamında Siber Savaş, International Journal of Akademik Value Studies, Vol: 3, Issue:9; pp:24-34 (ISSN:2149-8598)

ARTICLE INFO

Article History

Makale Geliş Tarihi
Article Arrival Date
25/01/2017
Makale Yayınlanma Tarihi
The Published Date
31/03/2017

Anahtar Kelimeler

Siber Saldırı, Bilgi Savaşları, ABD, Çin, Güç Mücadelesi, Savunma Stratejileri

Keywords

Cyber Warfare, Information Warfare,US, China, Power Struggle, Defense Strategies

JEL Kodları: K10, K24

ÖZ

Savaş belli amaçların elde edilmesi için düşman tarafların birbirleri üzerine güç ve şiddet kullanmalarıdır. Ülkelerin bilgi sistemlerine ve kritik altyapılarına yapılan planlı saldırılara ise "siber savaş" denilmektedir. Tarih boyunca bilimsel ve teknolojik gelişmeler savaşlarda kullanılmıştır. Küreselleşmeyle bilgi teknolojilerinin dünya çapında yayılması devletlerin, uluslararası arenadaki siyasi ve iktisadî mücadelelerinde savunma stratejilerini artık bu yeni savaş çeşidini dikkate alarak hazırlamalarına yol açmıştır. Savaşın beşinci boyutu olarak değerlendirilen bu yeni tür savaşta bilgisayarlar silahların yerini almıştır. Ülkeler bu yeni duruma hazır olabilmek için yeni teknolojik ordular kurarken, mevcut savunma doktrinlerini ve organizasyonlarını yenilemektedir. Bu konuda başı çeken ülkelerden ABD ve Çin arasında siber casusluğu da içeren bir siber savaş sürmektedir. Bugün dünyanın iki büyük gücü olan ABD ve Çin askeri, siyasi, ekonomik, teknolojik ve kültürel alanlarda başat güç olmak için mücadele içine girmişlerdir. 2016'da dünyanın birinci ekonomik gücü olan, ekonomik üstünlüğünü teknoloji ve internet gibi güçlerle birleştirmeye çalışan Çin, 21. yüzyılda ABD'nin yeni rakibi ve potansiyel dünya gücü olarak değerlendirilmektedir. Bu çalışmada, günümüzün en önemli uluslararası güvenlik sorunlarından biri haline gelen siber savaş konusu Amerikan-Çin rekabeti bağlamında ele alınacaktır.

ABSTRACT

Warfare can be defined as the use of force and violence by the opposing parties against each other to achieve certain goals. Planned attack over the information systems and critical infrastructures of countries is called "cyber warfare". Throughout history, scientific and technological advances have been used in wars. The worldwide spread of information technology in virtue of globalization has led the countries to prepare their defense strategies on the political and economic struggles in the international arena by taking this new kind of warfare into account. Computers have replaced the weapons in this new kind of warfare, which is taken into account as the fifth dimension of war. While the countries are establishing new technological structures in order to be prepared for this new situation, they are also renewing their doctrines and organizations. There is a cyber-war including cyber spying between the United States of America and the People's Republic of China (PRC), the prominent countries in this regard. The United States of America and China, which are the two great powers of the world, are struggling to be the dominant power in military, political, economic, technological and cultural fields. China, the prominent economic power of the world in 2016, is striving to combine its economic superiority with other fields such as technology and Internet and it is seen as the new rival of the USA and potential dominant power in the 21th century. In this study, cyber warfare, becoming one of today's most important international security issues will be discussed in the context of US-China rivalry.

1. GİRİŞ

Savaş, en basit tanımıyla belli amaçların elde edilmesi için tarafların birbirleri üzerine güç ve şiddet kullanmaları durumudur. Taraflar bir devlet veya devletler topluluğu olabileceği gibi, değişik

niteliklerde örgütlü gruplarda olabilir. Savaşın en yakın amacı rakibini alt etmek, yıkmak ve böylece tüm direnişini yok etmektir. (Clausewitz, 1975:13).

Günümüzde ise savaşlar konvansiyonel savaş yöntemlerinin çok ötesinde başka boyutlara taşınmış durumdadır. Bilgi teknolojisindeki gelişmeler hava, deniz, kara ve uzaydan sonra savaşın beşinci boyutu olarak adlandırılan siber uzaya taşınmış durumdadır. Ordular bilgi teknolojilerine bağımlı hale gelmiştir. Komuta kontrol sistemleri, silah sistemleri, istihbarat, keşif ve gözetleme sistemleri, muharebe sistemleri gibi sistemlerin çoğu elektronik ortamda ve iletişim altyapısı üzerinde çalışmaktadır. Söz konusu ortam ve altyapının korunması ise devletler için hayati önem teşkil etmektedir. Nükleer tesisleri, bilgisayar sistemlerini, elektrik santrallerini ve hava sistemlerini kapatma kabiliyetleri siber saldırıları ulusal güvenlik için ciddi tehdit haline getirmektedir. Uluslararası sistemi savaş haliyle bağdaştıran realistler güce ve silahlanmaya özel bir önem vermişlerdir. Uluslararası politikada devletler çıkarlarını kazanacakları güce göre tanımlarken, güç her zaman diğer devletlerin gücüyle kıyaslanmalıdır. (Morgenthau, 1993:29). Uluslararası ölçekte bir güç olma niteliğinin sürdürülmesinin en önemli unsurları teknoloji üretme yeteneği, coğrafi büyüklük ve nüfustur. Bunların arasında sürekli geliştirilen ve yenilenen teknoloji önemli bir faktör olarak karşımıza çıkmaktadır. Amerika, araştırma ve geliştirmeye ayırdığı kaynaklar sayesinde yeni teknolojik buluşlar yaratmada en önde olmuş bu küresel gücünün en önemli faktörü olmuştur. (Demir, 2012:50-52).

Dünya tarihi bazı devletlerin belirli dönemlerde başat güç konumuna yükselmeleri ve daha sonra bu statülerinden düşmeleri şeklinde günümüze kadar sürmüştür. Hobsbawm I. Dünya Savaşı için sınırları önceden çizilmemiş ve ne zaman biteceği belirsiz sıfır toplamlı bir oyun benzetmesi yapmıştır. Savaş sonrasında küresel bir işsizlik ve akabinde ise 1929 Ekonomik Bunalımı çıktı. Savaştan galip çıkan ABD, Fransa, Britanya, İtalya gibi başlıca güçlerin Almanya'ya dayatmaya çalıştıkları Versailles Antlaşması sorunlara çözüm bulmak bir yana daha da büyütmüştür. Fransa'nın Almanya'yı güçsüz kılmak arzusu ve savaş borçları Alman halkında tepkilere ve sonrasında faşizme temel olarak Almanya'da Nazilerin iktidara gelmesine ve 2. Dünya Savaşı'na neden olacaktı. Milletler Cemiyeti (MC) kurma çalışmalarının başarısız olması da ikinci bir dünya savaşını adeta tetiklemiştir. (Hobsbawm, 2006:35).

İkinci Dünya Savaşı'nın 1945'te sona ermesiyle dünya politikasına iki yeni süper güç, Amerika Birleşik Devletleri (ABD) ve Sovyet Sosyalist Cumhuriyetler Birliği (SSCB) hâkim olmuştur. İkinci Dünya Savaşı sonunda başlayıp 1990'lara kadar gelen ve dünya politikasına hâkim olan bu iki devletin oluşturduğu sisteme "İki Kutuplu Sistem" veya "Soğuk Savaş Dönemi" denir. (Sönmezoğlu, 2000:674). İngiltere, I. ve II. Dünya Savaşları sonucunda zayıf düşmüş ve süper güç olma özelliğini kaybetmiştir. SSCB'yi ise tarihin sonu çığlıkları arasında kapitalizmin dayanılmaz rekabeti yıkmıştır. Şimdi de ABD ekonomisi askeri harcamalar, küresel siyasi uyanış, tüketim ve yatırım tercihlerinin, bütçe krizlerinin kıskacına girmiş durumdadır. Bu zinciri kırmak içinde dünyada yeni açılımlar yapmak zorundadır. Diğer taraftan önümüzdeki yılarda ABD'nin ekonomik bir rakibi imkânsız gibi görünse de Çin'in ABD 'nin ekonomik gücünü tehdit etme olasılığı çok yüksektir.

1972'deki Mao-Nixon karşılaşmasından ve 1979'da kapsamlı diplomatik ilişkiler kurulmasından bu tarafa ABD-Çin ilişkileri istikrarlı bir biçimde gelişmiştir. Deng'in dış dünya ile sorunsuz ve barışçı bir ortam yaratarak, ekonomik kalkınma stratejisi izlemesi çerçevesinde Çin dış politikasında ABD baş köşede yer almaktadır. İki ülke Askeri, siyasi, ekonomik, teknolojik ve kültürel alanlarda başat güç olmak için mücadele etmektedir. Barack Obama döneminde çıkarılan 2012 tarihli ABD savunma stratejisi ABD-Çin rekabetine ışık tutar içeriktedir. Raporda savunma değerlendirilmesi yapılırken güç ağırlığı Ortadoğu'dan Asya-Pasifiğe kaydırılmıştır. Dengeleri değiştiren Çine'e karşı Hindistan ve Japonya dengeleyici ülkeler olarak saptanmıştır. Savunma konseptini Çin merkezli yeni bir paradigmaya oturtan raporda siber alem ve siber ağlarda ilk defa ciddi bir mücadele alanı olarak tespit edilmiş ve siber güvenlik konusunda gerekli hazırlıkların yapılması istenmiştir.(Örmeci, 2013:7).

ABD Soğuk Savaş döneminden sonra adeta rakipsiz kalmış ve uluslararası politikaya hegemonik bir güç olarak damgasını vurmuştur. Çin ise küreselleşme süreciyle bölgesel ve küresel arenada bir yıldız olmuştur. Çin 1.3 milyar nüfusuyla dünyanın en büyük ordusuna, nükleer silahlarına sahiptir ve Birleşmiş Milletler (BM) Güvenlik Konseyi üyesidir. Bu haliyle yalnızca ekonomik değil stratejik bir güç olarak ta tanımlanabilir. Şanghay İşbirliği Örgütü (ŞİÖ) , Güneydoğu Asya Uluslararası Birliği (ASEAN) gibi içinde yer aldığı örgütlerle Çin çok büyük bir bölgede etkin olabilecektir. (TASAM, 2005:13). Çin

artık giderek güçlenen ekonomisi ve gelişen nükleer gücüyle ABD 'nin rakipleri arasındadır. Bu durum ise iki ülke çıkarlarının bölgesel ve küresel düzlemlerde çatışma alanları oluşturmasına neden olmuştur.

Çin'in 2015 Büyüme hızı yüzde 6.9'dur. (Deutsche Welle, 2016). Çin, ABD ve Sovyetlerden sonra Aralık 2013'te ayın yüzeyine araç indiren üçüncü ülke olmuştur. Stockholm Uluslararası Barış Araştırmaları Enstitüsü (SIPRI) Askeri Harcamalar Veritabanı göre, ABD'nin askeri harcamaları 2015 yılında 595 milyar doları bulurken Çin'in harcamaları yüzde 7.4'lük artışla 215 milyar dolara yükseldi. (Deutsche Welle, 2016). Ayrıca BRICS (Brezilya, Rusya, Hindistan, Çin ve Güney Afrika Cumhuriyeti) ülkelerinin en önemli ayağı olan Çin hem bölge hem dünya siyasetinde önemli bir güç olma yolunda ilerlemektedir. ABD'nin kendisine yönelik çevreleme politikasına karşı da önlemler almaktadır. Bu yüzyılda Çin, ABD'nin yeni rakibi ve potansiyel dünya gücü olarak görülürken, iki devlet askeri, siyasi, ekonomik, teknolojik ve kültürel alanlarda rekabet halindedir.

Tablo 1. ABD ve Çin'in Sosyo-Ekonomik Yapısı

	ÇİN	**ABD**
Nüfusu	1.373.541.278 (Temmuz 2016)	323.995.528 (Temmuz 2016)
Yüzölçümü	9.596.960 km^2 (Dünya ülke karşılaştırmasında 4. Sırada)	9.833.517 km^2 (Dünya ülke karşılaştırmasında 3. Sırada)
GSMH	21.27 trilyon dolar (2016) (Dünya ülke karşılaştırmasında 1. Sırada)	18.56 trilyon dolar (2016) (Dünya ülke karşılaştırmasında 3. Sırada)
Askeri Harcamalar	215 milyar dolar (2015) (Dünya ülke karşılaştırmasında 2. Sırada)	596 milyar dolar (2015) (Dünya ülke karşılaştırmasında 1. Sırada)

Kaynak:https://www.cia.gov/library/publications/resources/the-world-factbook/geos/us.html; http://www.sipri.org/media/pressreleases/2016/milex-apr-2016, Erişim tarihi 05.01.2017.

Hedef seçilen şahıs, şirket, kurum, örgüt, gibi yapıların bilgi sistemlerine veya iletişim altyapılarına yapılan planlı ve koordineli saldırılara 'siber saldırı' denilmektedir. Bunlar, ticari, politik veya askerî amaçlı olabiliyor. Aynı saldırıların ülke veya ülkelere yönelik yapılmasına ise 'siber savaş'deniyor. En genel ifadeyle siber savaş "bilgi teknolojilerini korumak için siber alanda savunma yapmak veya saldırmak ya da rakip saldırıları engellemek için yapılan faaliyetlerin tümü" olarak tanımlanabilir. 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. (Gürkaynak&İren, 2011:169). Devletlerarası uyuşmazlıklarda diğer ekonomik, askeri, siyasi ve ideolojik araçlarla birlikte siber savaş son on yıldır kullanılır olmuştur. Bir devlet diğer devlete karşı kendisini avantajlı duruma geçireceği için siber saldırılarda bulunabilir.

Rusya, yakın geçmişte Çeçenistan, Kırgızistan, Gürcistan, Litvanya, Estonya ve İnguşetya'ya yaptığı siber saldırılarla bu alandaki en aktif ülkelerden biri olarak görülmektedir. Körfez Savaşı esnasında Irak güçlerinin, Çin ve Rus yapımı silahlarla savaşması ve ABD'nin siber savaşa maruz kalmasıyla dikkatleri üzerine çeken Çin bu alanda çalışmalar yapmaya başlamıştır. ABD ve NATO sistemlerine yapılan saldırıların büyük bir kısmının Çin kaynaklı olduğuna bakılırsa, Çin siber saldırılar konusunda sürekli bir çalışma içindedir. ABD'nin ise siber alandaki en önemli aktörlerden biri olduğu şüphesizdir. Kara, Deniz ve Hava kuvvetlerinin siber savaş birliklerinden meydana gelen ve Birleşik Devletler Stratejik Komutanlığı(U.S Strategic Command) adı altında kurulan Birleşik Devletler Siber Komutanlığı (U.S. Cyber Command) 31 Ekim 2010'da çalışmaya başlamıştır.(Lord, 2009:3)

ABD ve Çin arasında 2000'li yıllardan beri başat güç olma mücadelesinin sürdüğü söylenmektedir. Bu mücadeleden galip çıkan gücün ise 21. Yüzyılın süper gücü olacağı öngörüleri yapılmaktadır. Bu çerçevede, yapacağımız çalışmada 21.yüzyılda ABD'nin yeni rakibi ve potansiyel dünya gücü olarak görülen Çin arasında yaşanan ilişkiler siber savaş düzleminde analiz edilecektir.

2. SİBER SAVAŞ: KAVRAMSAL ÇERÇEVE

Soğuk Savaş'ın sona ermesiyle birlikte başlayan dönemde yaşanan gelişmeler güvenlik çalışmaları alanında da değişikliklerin yaşanmasına neden olmuştur. Bilim ve teknoloji alanındaki ilerlemelere küreselleşmenin getirdiği birtakım gelişmelerde eklendiğinde ortaya karmaşık ve çok boyutlu bir güvenlik ortamı çıkmıştır. Yeni dönemde güvenlik ile ilgili sorunların azalacağı beklentileri boşa çıkmıştır. Bu sebeple güvenlik alanında teorik çalışmalar ivme kazanmış ve güvenlik uluslararası ilişkiler teorileri arasında farklı bakış açılarıyla değerlendirilmiştir.

Uluslararası ilişkiler alanında ilk kuramsal yaklaşım, Birinci Dünya Savaşı sonrasında on yıl kadar egemen bir görüş olarak kabul edilen idealizmdir. İdealistlere göre insan doğası itibariyle iyidir ve işbirliğine yatkındır. İnsanların kötü davranışlarda bulunmasına ise kötü kurumsal ve yapısal düzenlemeler neden olmaktadır. Uluslararası toplum, savaş ve adaletsizlik gibi sorunları önlemek için kurumsal düzenlemelere gitmesi gerekir. (Arı, 2013:24). Barış temasını temel alan ve barışçıl bir dünya düzeninin oluşturulmasını hedefleyen İdealizm ekseninde kurulan Milletler Cemiyeti İkinci Dünya Savaşı'nın çıkmasını engelleyemedi. (Eralp, 2006:45).

Realist güvenlik anlayışı Uluslararası İlişkiler (Uİ) disiplinine ilişkin temel teorik yaklaşımlardan birisidir. 1930'lardan günümüze kadar etkili konumunu sürdüren realizmin ilk özgün kullanımı Morgenthau ile başlamış ve 'ulusal çıkar', 'güç' gibi kavramlar uluslararası sistemi açıklamada kullanılan kavramlar olmuştur. (Sönmezoğlu, 1996:370).

Güvenliğin sağlanması için askeri güce ve silahlanmaya özel bir önem veren realistler, uluslararası sistemi savaş haliyle bağdaştırmışlardır. Hobbes'a göre insanlar bir toplum haline gelmeden önce doğa halinde yaşamaktaydı. Doğa durumu herkesin herkesle savaştığı, korku, kuşku ve şiddetin bulunduğu son derece güvensiz bir ortamdır. Bu durumdan kurtulmak için insanlar her çeşit yetkilerinden vazgeçerek bunları Leviathan'a (En üstün yönetici veya devlet otoritesi) devir ederek bir toplumsal sözleşme oluşturdular. Bir Leviathan'ın hegemonik bir gücün ya da dünya devletinin bulunmadığı uluslararası ilişkilerde doğa durumu sürmekte olduğundan anarşi devam etmektedir. Hobbes'a göre böyle bir ortamda çatışma, kuşku, güvensizlik ve savaş kaçınılmaz olgulardır.Bu sebepten dolayı bir toplumsal sözleşmenin olmadığı uluslararası ilişkilerde hiçbir moral ve ahlaki sorumluluğun devletlerarası ilişkilerde istenen seviyede sağlayamayacağını öne sürmektedir. (Karabulut, 2011:54).

Morgenthau ise realizm çerçevesinde 6 temel ilke belirlemiştir. Bunlar:

1. Realizm, genel olarak toplum gibi, siyasetin de, kökleri insan doğasında bulunan objektifliğine yöneltildiğine inanır.
2. Siyasal realizme yolunu bulmakta yardım eden uluslararası politika denen geniş alanda en önemli "odak noktası" ise güç terimi ile ifade edilen çıkar kavramıdır.
3. Realizmin en temel kavramı olan güç şeklinde tanımlanan çıkar kavramı hiç değişmeyen ve sabit bir anlam içinde ifade edilemez. Çıkar fikri gerçekten de politikanın özüdür ve zaman ve mekâna bağlı değildir, onlardan etkilenmez.
4. Siyasal realizm siyasal eylemin moral öneminin farkındadır. Fakat çoğu zaman başarılı bir politikanın gerekleriyle ahlakın emirleri arasında giderilmesi güç bir gerilim olduğu görülmektedir. Realizm, evrensel moral ilkelerinin, evrensel soyut formüller biçimi içinde, devletlerin eylemlerine uygulanamayacağı görüşündedir ve bu ilkelerin zaman ve yer konusundaki somut şartlara göre ayıklanması gerektiğini savunur.
5. Siyasal realizm, belli bir ulusun ahlaki hareket edip etmediğini belirleyip anlamakta dünya çapındaki moral yasaların temel ölçüt olarak alınması görüşünü kabul etmez. Gerçek ile kanaat arasında bir ayırım ve benzemezlik olduğuna inandığı gibi, gerçek ile gerçek yerine konan şeylere tapınma arasında da ayrım olduğuna inanır.
6. Siyasal realizm ile diğer düşünce ekolleri arasında gerçek ve önemli bir fark vardır. (Morgenthau, 1970:1-18).

Bir devletin diğerlerine göre daha gelişmiş silahlara sahip olması, diğer devletlerinde bu sistemlere sahip olma arayışlarına itmekte ve güvenlik ikilemindeki bu döngü kendini silahlanma girişimlerinde göstermektedir. Realizmin temel tezlerini şu şekilde sıralayabiliriz: Birincisi, uluslararası sistemin temel aktörü egemen devletlerdir. Devletler rasyonel karar alıcıları ve kurumlarıyla kendi başlarının çaresine bakmak zorundadırlar. Bunlar sadece kendi çıkarlarını savunurlar. İkincisi, uluslararası sistemin üyeleri kim olursa olsun yapısı anarşiktir. Anarşi burada bir kaos ve belirsizlik durumundan

ziyade uluslararası sistemi oluşturan devletlerin davranışlarını disipline edecek ya da düzenleyecek üst bir otoritenin olmaması durumunu ifade eder. Üçüncüsü, anarşik bir sistemde varlığını sürdüren egemen devletlerin çıkarlarını gerçekleştirmek için davranışlarını seçme özgürlükleri vardır fakat bu özgürlüğü adalet ve hukuk gibi soyut değerler değil, yalnızca diğer devletlerin çıkarları ve davranışları kısıtlayabilir. Dördüncüsü, devletlerin söz konusu çıkarları arasında herhangi bir uyum beklenmeyeceği gibi görecelidir. Başka bir ifadeyle devletler bir diğerinin sahip olduğu kazançların kendisininkinden azlık ve çokluğunu sürekli kontrol etmek durumundadır. Realist güvenlik anlayışının beşinci tezi tarihsel olarak en sık rastlanan devlet davranışı olan savaşlardır. Savaşlar, uluslararası anarşik sistemde 'güç' ve 'güvenlik' için yapılır devlet siyasetinin devamı niteliğindedir. Devletlerarası anlaşmazlıkları çözmede en etkili araç olarak kabul edilen savaşlar yıkıcı, bencil insan doğasının ve bunlara engel olacak bir üst otorite ve yönetim eksikliğinin sonucudur. (Kardaş, 2007:127).

1980'li yıllardan itibaren iletişim ve ulaşım teknolojilerindeki gelişmeye bağlı olarak hızlı bir değişim yaşanmaktadır. Küreselleşme ile ifade edilen bu değişimde ülkeler birbirlerine başta ekonomi, güvenlik, enerji, kültür gibi çeşitli alanlarda birbirlerine daha bağımlı hale gelmişlerdir. Yine bu dönemde eskinin askeri odaklı tehditlerine ek olarak siber saldırılar gibi yeni tehditler ortaya çıkmıştır. "siber savaş" ve saldırılar güvenliğe yönelik güncel risk ve tehditlerin başında gelmektedir. (Karabulut, 2011:91).

Siber Savaş Bush'ın siber güvenlik danışmanı Clarke'a göre "Bir devletin, başka bir devletin bilgisayar sistemlerine veya ağlarına zarar vermek ya da kesinti yapmak üzere gerçekleştirilen sızma faaliyetleridir" Bir devlet, diğer devlete karşı kendini avantajlı duruma geçirdiği için saldırıda bulunabilir. Siber savaşın harici amacı, siber savaşın asıl amacı olarak sayılabilir. Karşı tarafa boyun eğdirmeyi, bilgilerini çalmayı, sistemlerini belirli bir süre devre dışı bırakmayı veya tamamen bozmayı içerir. Dahili amacı ise, siber savaş uygulamasının nasıl yapılacağını (saldırıları durdurma, kapsamı sınırlandırma, karşı tarafın sağlıkla ilgili sistemlerine saldırmama v.b.) ve gerginliğin tırmandırılmasından nasıl kaçınılacağını içerir. (Çiftçi, 2013:3-7).

Siber savaşı cazip kılan avantajları:

1. Klasik yöntemlere göre çok ucuz olmaları
2. Ani ve beklenmedik saldırı ile düşmanı hazırlıksız yakalar ve savunma imkânı vermez
3. Tanınma, bilinme olasılığı nerdeyse yok
4. Sınırlar, kıtalararası ulaşım
5. Çok az riskli

İstendiği takdirde can kaybı hiç olmayabilir, kamuoyu açısından bilgisayarların oluşturacağı kaos daha etkili olur. (Şeker, 2015). Bilgi teknolojilerinin doğası gereği; bilgi çağının tehditleri, endüstri çağının tehditlerine nazaran daha dağınık, yayılmış, çok boyutluluk ve belirsizlik gibi özellikler taşımaktadır. Bilgi teknolojilerindeki gelişme, devletler ya da terör örgütleri tarafından kullanılan silah ve teknikleri de değiştiriyor. Bu bağlamda ifade edilen siber savaş kavramı ise bilgi teknolojilerinde meydana gelen gelişme neticesinde ortaya çıkan yeni bir çatışma ve suç modeli ortamını ifade etmektedir. (Arquilla&Ronfeldt, 2001).

Bilgisayarın ve internetin 20.Yüzyılda ortaya çıkışı ile birlikte devletlerin savaş, saldırı ve savunma teknikleri değişiklik göstermiştir. Artık ülkeler geleneksel savaş stratejilerinin yanında siber savaşa da hazırlık yapmaktadır. Çünkü gelişmiş ülkelerin kritik altyapıları ileri düzey bilgi teknolojileri ile korunmaktadır bu da onları siber saldırı tehdidi altında bırakmaktadır. Teknolojiyi verimli kullanarak rakiplerine üstünlük sağlayan ülkelere enerji, finans, temel altyapı hizmetleri, elektrik, savunma gibi alanlarda siber saldırı kaçınılmaz olmakta ve bu ülkeler açısından zafiyet yaratmaktadır. Siber savaşın gelecekte en önemli üstünlük mücadelesi olacağını öngören devletler bu alanda çalışmaktadırlar. ABD 11 Eylül 2001 terör saldırılarının ardından siber savunmaya yönelik yatırımlarını artırmıştır. Askeri Haber Alma Ajansı'nın (NSA) yanı sıra dijital savunmaya yönelik 14 farklı birim oluşturmuştur. Yıllık en az 50 milyar dolarlık bir bütçeyle çalışan bu kuruluşlar bireysel internetin kontrolünden sanayi casusluğuna, dijital savaştan tüm iletişim ağlarının kontrolüne kadar sanal dünyanın mutlak hâkimiyeti için çalışmaktadır. Ancak ABD bu alandaki faaliyetleriyle yalnız değildir. ABD'nin haricinde Çin, Hindistan, Rusya, Kuzey Kore, İran, İsrail ve İngiltere başta olmak üzere çok sayıda ülke sanal savaşlar için büyük harcamalar yapmaktadır. (Onar, 2016:32).

Çin, Rusya ve Kuzey Kore gibi ülkeler siber savunma alanına önemli yatırımlar yapan ülkelerin başında gelmektedirler. Çin 2050 yılına düşmanlarının önemli altyapılarını hedefleyen bir siber doktrin benimsemiştir. (Menon, 2013). Çin rakiplerine karşı siber saldırı kapasitesini artırarak yalnızca fiziki dünyada yapılan savaşların üstünlük için yeterli olmadığını kabul etmiştir. Özellikle ABD ve Rusya gibi güçlü rakipleriyle siber alanda mücadele edebilmek için önemli çalışmalar yapmaktadır. Güçlü virüsler ve kötü amaçlı yazılımlar (malware) oluşturarak düşmanlarının kritik alt yapılarını çökertmeyi amaçlamaktadır. Çin siber savaşa karşı aldığı bu önlemlerinde yalnız değildir. Diğer gelişmiş teknolojiye sahip devletler de kendi önlemlerini almaktadırlar. Rusya'nın da diğer ülkelerin sahip olduğu gibi ileri düzey siber saldırı silahları ve gelişmiş stratejileri bulunmaktadır Kuzey Kore'nin teknolojisi de daha önce bahsedilen devletlerin sahip olduğu siber saldırı kapasitesinden düşük değildir. Kuzey Kore ordusu ise Unit 121 adında siber savaşa odaklı ve olası bir savaşa karşı kapasitesini geliştirmeye çalışan bir birim kurmuştur. Siber savaşa önem veren diğer bir devlet de Hindistan'dır. Pakistan'la yaşadığı Keşmir sorunu ve nükleer silah denemelerinde maruz kaldığı siber saldırılara önlem almak amacıyla sanal dünyada yaşanan rekabete tepkisiz kalamamıştır. Hindistan, 1998 yılından itibaren siber savaşı da içine alan yeni güvenlik doktrini çerçevesinde hareket etmektedir. İran ise siyasi ve ekonomik açıdan savunma sistemlerinin korunmasına yönelik teknolojik yatırımlara ağırlık vermektedir.Ayrıca İran, dışarıdan bilgi teknolojileri satın almakta, askeri alanda teknik yardım aramakta, Rusya ve Hindistan gibi ülkelerden de eğitim desteği almaktadırlar. (Onar, 2016:31).

Siber güç kapasitesi değerlendirildiğinde ABD, Rusya ve İngiltere birinci, Çin ikinci, İran ve Kuzey Kore ise üçüncü kademe ülkeler olarak değerlendirilmektedir. Bilgi güvenliği uzmanı Bruce Schneir'a göre, herhangi bir siber saldırının siber savaş olarak değerlendirilebilmesi için ortada gerçek bir savaş olması gerekir. 2011 yılında Rusya ile Gürcistan arasındaki savaşta Gürcistan'a karşı yürütülen siber saldırılar bu kapsamda değerlendirilmektedir. Bir devletin ulaşım, haberleşme, finans, enerji ve su gibi temel kritik altyapılarını işlevsiz hale getiren siber saldırlar siber savaş olarak tanımlanmaktadır. Küçük maliyetlerle büyük etkiler yaratma potansiyeline sahip siber savaşta daha az maliyetli bilgisayar teknolojisi varken neden yüksek maliyetli füze kullanılacağı temel motivasyondur. ABD 'dijital Pearl Harbor' olarak değerlendirilen böyle bir saldırı durumunda, bunun savaş nedeni sayılacağını ve bunu yapan düşmana siber ve kinetik boyutta her türlü araçla karşılık verileceğini belirtmiştir. (Pehlivan, 2013:32). Amerikan hükümeti¬nin siber saldırılara karşılık verme hakkını kendinde görmesi, siber ortamda yapılacak bir saldırıyı kapsadığı gibi, klasik anlamda silahlı bir saldırıyı da kapsamaktadır. Bu açıklama, ABD'ye saldırı tehdidinde bulunan devlete klasik anlamda savaş açma hakkını kendinde görmesi açısından dikkat çekici olduğu kadar, siber saldırıya klasik anlamda silahlı karşılık verme hakkının uluslararası hukuk açısından ne sonuçlar doğuracağını akla getirmektedir. (Yayla, 2013:188).

3. SİBER SAVAŞIN HUKUKİ BOYUTU

Savaş süresince uyulması gereken kurallar bütünü savaş hukukunu ifade etmektedir. Bu kurallar önceleri, uyulması ve uyulmaması konusunda hukuki zorunluluğu bulunmayan savaş kararları şeklinde iken sonraları yapıla geliş kuralları halini almıştır. 20. Yüzyılın ikinci yarısından itibaren ise bu kurallar derlenmiştir. (Sönmezoğlu, 1996:383). Avrupa Konseyi'nin 2001 tarihli Siber Suçlar Sözleşmesi, siber suçlara karşı ortak mutabakat ve uluslararası işbirliği için hazırlanan bir belgedir. Sözleşme değişik maddelerinde bilgisayarlara yönelik saldırılar, hacklemek, kişisel verilerin korunması, izinsiz dinleme gibi bilgisayar suçlarını düzenlemektedir. (Önok, 2013). BM'de ise siber suçlarla ilgili 2000, 2002 yılında kararlar alınmış, 2005 yılında ise siber güvenlikle ilgili karar alınmıştır. Ayrıca 2011'de siber suçlara dair BM' de Hükümetler arası uzmanlar grubu kurulmuştur. (BTK, 2013).

BM Şart ile belirlenen karşılık verme konusu da dikkat çeken diğer bir noktadır. BM Şartı kuvvet kullanımını sınırlandırırken Güvenlik Konseyi kararı ile meşru müdafaa başlığı altında bu hakka izin vermektedir. BM Antlaşması'nın 51. Maddesinde ferdi ve kolektif meşru müdafaa düzenlenmiştir. Buna göre; BM Teşkilatı üyelerinden her hangi birisine karşı silahlı saldırıda bulunulduğunda Güvenlik Konseyi'nin milletlerarası barışı ve güvenliği korumak amacıyla toplanıp gerekli tedbirleri alıncaya kadar, tek başına veya toplu meşru müdafaa hakkının her zaman saklı olduğu ve bunun BM Antlaşmasında hiçbir tahdide tabi tutulamayacağı yer almaktadır. (Bozkurt, 1996:21).

Siber alandaki hangi saldırılar kuvvet kullanımı olarak algılanacak sorusuna henüz cevap veremeyen BM, siber uzayda kuvvet kullanımı konusunda yetersiz durumdadır. Enerji nakil hatları, haber sitesi gibi yerlere saldırı durumunda nasıl karşılık verileceği konusunda ciddi boşluklar bulunmaktadır. Rusya tarafından siber savaşın tüm çeşitlerinin, kısıtlanması uzun dönemde yasaklanması önerilmiştir. Çin ve ABD ve diğer güçlü ülkelerle mücadele edebileceği ve maksimum kazançlar sağlayacağı bu kozu elinden çıkarmak istememiş ve reddetmiştir. Ayrıca yapılan antlaşmalara uyulup uyulmadığının kontrolü zorluk içermektedir. Devlet dışındaki birey ve grupların uyması beklenmezken, bir devlette gizlice bu grupları destekleyebilir. Özellikle ABD gibi güçlü devletler BM Antlaşması'nın 2(4). Maddesinin daha geniş yorumlanmasını ve siber saldırıları da kapsayacak biçimde genişletilmesi yönünde görüş bildirmektedirler. Söz konusu maddeye göre; "Teşkilatın tüm üyeleri, uluslararası ilişkilerinde gerek herhangi bir başka devletin toprak bütünlüğüne ya da siyasal bağımsızlığa karşı, gerek Birleşmiş Milletler'in Amaçları ile bağdaşmayacak herhangi bir biçimde kuvvet kullanma tehdidine ya da kuvvet kullanılmasına başvurmaktan kaçınırlar." (Orallı, 2014). Fakat söz konusu madde halen klasik anlamda silahlı kuvvet kullanmayı yasaklamaktadır. Son yıllarda özellikle Estonya, Gürcistan, İran'ın nükleer tesislerine karşı Stuxnet olaylarındaki siber saldırılar geleneksel uluslararası hukuk normu olan "müdahale yasağı" kuralını da ihlal etmektedir. Fakat devletler ya bu saldırıları devlet dışı aktörlere yaptırarak kendilerini gizlemekte ya da teknolojik imkânlar sayesinde saldırıların kimler tarafından yapıldığı tespit edilememekte ve resmi bir kanıt ortaya konamamaktadır.(Yayla, 2013:9).

4. ABD ve ÇİN ARASINDA YAŞANAN SİBER SALDIRI ÖRNEKLERİ

- ✓ Kosova Savaşı'nda Çin'in Belgrad Büyükelçiliği'nin Bombalanması
  1999 yılında bir NATO jeti Kosova Savaşı sırasında Çin büyükelçiliğini bombaladı. En az 12 saat sonra Çin'in Kızıl Hackerlar Birliği ABD web sitelerine karşı binlerce siber saldırı başlattı. (Platov, 2013).
- ✓ Birinci Dünya Siber Korsan Savaşı
  2001 yılında bir Amerikan casus uçağı ile Çin jeti pasifikte çarpışmıştır. Çin jeti düşünce Çinli hackerler Beyaz Saray'ın sitesine saldırmıştır. (Nytimes, 2001).
- ✓ Casusluk, Titan Rain

Çinli hackerlar 1998 yılında Pentagona saldırı başlattılar ve ABD askeri bilgisayarlarından veri çaldılar. Pentagon yayınladığı yıllık raporunda resmi olarak ilk kez Çin'i ve ordusunu siber saldırılar konusunda 2013 yılında uyardı. Çin'in başta ABD olmak üzere ülkelerin savunma, diplomasi, askeri ve ekonomik bilgilerini sızdırdığını açıkladı. Obama Çin Başbakanıyla görüşmesinde aynı uyarıyı tekrarladı fakat Çin suçlamaları reddetti. Yine Mandiant şirketi Şubat 2013 tarihli raporunda, Şanghay'da Çin ordusuna bağlı gizli bir askeri birliğin ABD şirketlerine casusluk amaçlı saldırılarda bulunduğunu ve 140 şirkete yönelik saldırının Çin Halk Kurtuluş Ordusu ile bağlantısının olduğunu belirtmiştir. (İnternethaber, 2013). Yeni savunma stratejisiyle Asya-Pasifiği ilk sıraya koyan ABD Çin'i niyeti belli olmayan şüpheli olarak nitelendirmiştir. (Dünya, 2012). Yine Türkiye'nin Çin'den almak istediği füze sistemleri Çin ile NATO ve ABD arasında gerilime neden olmuştur. NATO Genel Sekreteri Rasmussen, Türkiye'nin Çin'den ithal edeceği füze sisteminin NATO standartlarına uymadığını ileri sürmüştür. Çin'e duyulan güvensizlik Çin'in bununla NATO içinde virüs etkisi sağlayarak kritik bilgilerini elde edebileceği yorumlarına neden olmuştur. (Diplomatik Gözlem, 2013).

Bazı uzmanlar, Çinlilerin dünyada saldırgan siber saldırıları yapan bilgisayar korsanlarının ülkesi olarak anılması ve bundan dolayı, NATO ile Çin sisteminin entegre edilmesi halinde, Çinli program yazılımcılarının NATO bilgi sistemine sızma ihtimali tehlikesine dikkat çekmişlerdir. (BBC, 2013).

- ✓ Dünya Birinci Siber Savaşı

Dünya Birinci Siber Savaşı'nda ortak saldırı merkezi hedefi olarak ABD yer aldı. Büyük hack saldırıları sonucu Amerika'nın servis sağlayıcıları zor durumda kalmıştır. ABD ve Çin arasında yaşanan yoğun siber saldırılar sonucu Dünya Birinci Siber Savaşı çıktığı iddia edilmektedir. (Yeniakit, 2015).

2014 yılında Kuzey Kore'nin Sony Pictures'ın Kuzey Kore lideri Kim Jongun'a yönelik suikast sahnelerinin yer aldığı The Interview adlı film yüzünden Sony Pictures'e düzenlenen saldırılarla başlayan siber savaş, ABD'nin Kuzey Kore'nin internetini bir süreliğine kesmesine neden olmuştur. ABD'ye yapılan bu saldırılara tüm dünyadan hackerler destek vermiştir. ABD' li yetkililer Kuzey Kore internetinin servis sağlayıcısı Çin Unicom'dan bu ülkenin hizmet ve servis sağlayıcılarının

kapatılmasına yardım etmesini ve hackerların saptanmasını istemiştir. ABD'nin taleplerine doğrudan yanıt vermeyen Pekin Kuzey Kore'nin sorumlu olduğuna dair kanıt bulunmadığını ama her türden siber saldırıya karşı olduğunu duyurdu. (Cumhuriyet, 2014).

5. ABD ve ÇİN'İN SİBER SAVAŞ STRATEJİLERİ

Ülkeler, güvenli bir siber ortam sağlayabilmek için siber ortamın parçası olan elemanları siber saldırılara karşı muhafaza etmek, saldırılara karşı müdahale etmek için gerekli yasal oluşturmak üzere politika ve stratejiler geliştirmişlerdir. Bu bölümde ABD ve Çin'in siber stratejileri ele alınmıştır.

Amerika, siber güvenliğe yönelik ilk belgesi 2003 tarihli The National Strategy to Secure Cyberspace adlı belgedir. Geniş kapsamlı olan belgede öncü rol üstlenecek devlet kurumları belirlenmiştir. Siber ortama yönelik tehditlerden söz edilmiş ve özellikle 11 Eylül'e reaksiyon olarak hazırlanmıştır. Obama siber güvenliği. ABD'nin karşılaştığı en ciddi ekonomik ve milli güvenlik konularından biri olarak tanımlanmıştır.2011 yılında ise 'Siber Uzay İçin Strateji Belgesi' hazırlanmıştır. İçinde beyaz Saray'ın siber ortamda başarmak istediği amaçlar vardır. Belgede siber saldırılara karşı askeri güç kullanımının göz ardı edilemeyeceği belirtilmiştir. Çin tarafından belgeye üç eleştiri getirilmiştir:

Stratejinin aslında askeri yetenek ve caydırıcılıkla ilgili olduğu ve hem kendini hem müttefiklerini korumak için gerekli tüm yolları uygulayacağı ifadesi bun örnek verilmiştir.

İş birliği çağrısına rağmen ABD'nin teknolojik liderlik çabasında olduğu belirtilmiştir.

İnternet özgürlüğünü zorlamanın daha fazla çatışmalara neden olacağı. Bu eleştiri elektronik bilgi akışının serbest olması maddesiyle ilgili Arap Baharı olaylarına atfen yapılmıştır.

2008 yılında ABD'nin Ortadoğu'daki üslerinden USB bellek yoluyla gizli iletişim ağına ve Merkezi Komutanlığı'na bulaşmıştır. Bu olay ABD siber savunma stratejinde dönüm noktası olmuş ertesinde ABD Siber Komutanlığı kurulmuştur.

30 Mayıs 2011 tarihinde ise, Pentagon tarafından, siber saldırılara cevap vermek için yalnızca siber saldırı değil, mümkün olan tüm seçeneklerin kullanılacağı, bunların içinde askeri güç kullanımının da olduğu ilan edilmiştir. (Çiftçi, 2013:66-73).

ABD, yeni savaş konseptine bilgisayar korsanlarıyla mücadeleyi ekledi Pentagon, ordunun "Savaş Kitabı"nı güncelleyerek, kendilerine siber saldırıda bulunan kişi ve gruplara karşı, gerek görüldüğünde askerî operasyon dâhil her türlü karşılığı vermeye izin verecek şekilde genişletti. Sanal düşmana ekonomik ambargo uygulanması veya aynı şekilde internet üzerinden cevap verilmesi de seçenekler arasında görülürken ABD'nin belirlediği siber saldırı odaklarının birinci sırasında Çin bulunmaktadır. Uzmanlar, Çin'in, internet üzerinden birbirine bağlı federal ağlarda arıza meydana getirebilecek teknolojiye şimdiden ulaştığına inanıyor. Ulusal elektrik hizmetlerinin çökertilmesi gibi, ABD'de gündelik hayatı menfi şekilde etkileyebilecek saldırılara maruz kalınması, söz konusu tehditler arasında sayılıyor. ABD ayrıca İran ve Rusya'yı da, siber saldırılar kapsamında büyük tehlikeler olarak tanımlamaktadır. (Sondevir, 2013).

Dünyada pek çok devlete ve şirketlere ait bilgisayar sistemlerine 2000 yılında girilmiş ve bu girişlerin başlangıç noktasının Çin olduğu belirlenmiştir. Ünlü Çinli stratejist Sun Tzu tarafından M.Ö. 6.Yüzyılda kaleme alınan Strateji Sanatı adlı kitabında savaşmadan savaşı kazanmanın zekice bir stratejiyle mümkün olduğunun altını çizmektedir ve şunları söylemektedir "muktedir olan, muktedir değilmiş gibi görünür. Yakında iken uzaktaymış gibi görünür. Hasmın hazırlıksız olduğu bir anda saldırır ve hiç beklenilmeyen yerden aniden ortaya çıkar" Bu bir stratejinin zafere ulaşma şeklidir. (Wing, 1995:15).

Çin'in 2010 yılı Savunma Raporu'nda da, Çin'in milli savunmasında siber güvenliğin önemi açık bir şekilde vurgulanmaktadır. Buna göre siber savaş kabiliyetleri, Çin'in askeri harekâtına üç temel alanda hizmet edecektir:

Siber casusluk ile başka ülkelerden veri çalınmasına hâlihazırda izin vermektedirler.

Hasımların özellikle internet tabanlı lojistik, iletişim ve ticari faaliyetlerini kısıtlayabilirler. Siber savaşı, konvansiyonel bir savaşta kuvvet çarpanı olarak kullanabilirler. (Çiftçi, 2013:81-82).

Çin ordusunun resmi bildirilerinde, siber savaş kapasitesinin geliştirilmesine yönelik bir stratejinin benimsendiği görülmektedir. Çin ordusu, çatışma anında istihbarat toplama ve düşmana karşı bilgi

üstünlüğü sağlama amacıyla çeşitli siber araçların kullanılması için eğitim görmektedir. Çin'in bilgisayar ağ sistemlerinin zamanlı ve karmaşık saldırılar yaparak ABD ve gelişmiş ülkelere yönelik istihbarat amaçlı kullandığı iddia edilmektedir. ABD'den çalındığı iddia edilen belgelerin çoğu ise stratejik önemdedir. ABD 'li uzmanlar, ABD ve Çin arasındaki bir çatışmada askeri ve müttefik ülkelerdeki iletişim ağlarına saldırı düzenleyeceğini öngörmektedir. Bu saldırılarsa ABD'nin intikalini geciktirirken çatışma sahasındaki birliklerinin etkinliğini azaltmayı amaçlamaktadır. Yine Çin'in Küba'da iki adet casus ağ istasyonu kurduğu, birisinden ABD'nin internet trafiği izlenirken diğerinden ABD Savunma Bakanlığı'na ait iletişim ağlarının dinlenildiği iddia edilmektedir. (Sondevir, 2013). Çin Devlet Konseyi ise dünyadaki değişen dengeler ve tehlikelere karşı ülkesini korumak gerekçesiyle Mart 2015'te "Beyaz Kitap"ı yayınlamıştır. Özellikle ABD'nin Asya- Pasifik'te "yeniden dengeleme" stratejisiyle bölgedeki askeri varlığını ve ittifaklarını artırması Çin ve bölge ülkelerinde endişelere sebep olmuştur. Beyaz Kitap'a göre Çin, "kara denizden üstündür" ilkesini terk ederek okyanusları kritik güvenlik alanlarına eklemektedir. Uzay, siber dünya ve nükleer güç okyanuslarla birlikte tanımlanan Çin'in diğer kritik güvenlik alanları olmuştur. (Turkishny, 2015).

Dünyada meydana gelen siber saldırıların pek çoğundan sorumlu tutulan Çin'in muhtemel saldırıları önlemek için Mavi Ordu isimli birlik kurduğu söylenmektedir. Çin'in en yetenekli beyinlerinden oluşan Mavi Ordu'nun, halk kurtuluş ordusunda görev alan askerlerden ve üniversite öğrencilerinden seçildiği ve amacının mevcut askeri kuvvetlerin güvenliğini artırmak olduğu söylenmektedir. (Milliyet, 2011).

6.SONUÇ

İletişim çağındaki hızlı gelişmeler geleneksel savaş metotlarında da dönüşüm gerçekleştirmiş ve savaşlar muhabere alanlarından bilgisayar alanlarına kaymıştır. Kara, deniz, hava ve uzaydan sonra savaşın beşinci cephesi olan siber uzayda başarılı olmak için siber saldırıları ve maliyetlerini inceleyip uygun stratejiler geliştirmek gerekmektedir. Hasım olarak görülen hedefe saldırıda bulunmak, savunma yapmak ve istihbaratla ilgili bilgiler toplamak siber savaş faaliyetlerini oluşturmaktadır. Siber saldırıların hukuki boyutunda ise ciddi boşluklar söz konusudur. Realizmin anarşik uluslararası ortamda bir üst otorite olmaması tezini doğrulamaktadır. Siber savaşın ana hedefi ise devletlerin haberleşme, enerji, savunma, sağlık gibi kritik alt yapılarıdır. Çatışma potansiyeli yüksek anarşik bir uluslararası sistemde varlığını sürdürmek durumunda olan devletler kendi egemenliklerini ve güvenliklerini korumak için her türden silaha ve savaş yöntemine başvurmaktadırlar. Bu bağlamda, siber savaş ülkelerin milli güvenliğini sağlama ve dış tehditleri bertaraf etme amaçlarına ulaşmak için etkili araçlardan biri olarak görülmektedir.Devletler siber güçlerini maksimize etmek için rekabet içindedirler.

Soğuk Savaş'tan sonra Çin yükselen bir güç olarak ABD'ye rakip olarak gösterilmiştir. ABD'nin devlet kurumlarına ve şirketlerine saldırının ardında Çin'in olduğu düşünülmektedir. ABD ise gerek savunma doktrinlerinde gerekse siber güvenlik belgelerinde Çin'i rakip olarak gördüğünün ve çevrelediğinin işaretlerini vermektedir. Şu an Çin'in orta vadede bir bölgesel güç olduğu tartışılmazdır. Uzun vadede ise ekonomik ve askeri gücüne ek olarak siber savaş alanındaki manevra kabiliyetini de artırıp bir dünya gücü olma potansiyeline sahip olduğu ileri sürülebilir. Siber saldırı konusunda ABD tarafından Çin'in doğrudan suçlanmasına karşılık Çin'den de ABD'yi aynı şekilde suçlayan bir açıklama gelmiştir. Yani iki gücün rekabet alanına artık siber uzay da eklenmiştir.Bu güvenlik sorununun çözümü içinse ilk olarak konunun taraflar tarafından bütüncül bir şekilde ele alınması gerekmektedir.İkinci olarak ise ortak hukuki bir zeminin ve küresel bir siber güvenlik standardının oluşturulması için çalışmalara başlanmalıdır. Ancak devletlerin kendi çıkarlarını ön planda tutan politikalarına ve bilgi teknolojilerinde yaşanan gelişmelerle ağ kontrolünün de zorlaşmasına bağlı olarak bu konuya ilişkin kalıcı bir çözümün sağlanabilmesi şimdilik pek mümkün görünmemektedir.

KAYNAKÇA

"ABD ile Çin Arasında Siber Başladı", (2015). http://www.yeniakit.com.tr/ haber/abd-ile-cin-arasinda-siber-savas-basladi-48099.html , (Erişim tarihi 22.12.2015).

Arquilla, J., & Ronfeldt, D. (2001). Networks and Netwars: The Future of Terror, Crime, and Militancy, http://faculty.cbpp.uaa.alaska.edu/afgjp/padm610/networks%20and%20netwar.pdf , (Erişim tarihi 15. 10. 2013)

Arı, T. (2013), Uluslararası İlişkilere Giriş, MKM, Bursa.

"Askeri Harcamalar Yükselişte", (2016). http://www.dw.com/tr/askeri-harcamalar-y%C3%BCkseli%C5%9Fte/a-19163891, (Erişim tarihi 24.04.2016).

Bozkurt, E. (1996). BM Sisteminde Kuvvet Kullanımı ve Körfez Krizi Örneği, Atlas Kitabevi, Konya.

BTK, Bilgi Teknolojileri ve İletişim Kurumu, http://www.cybersecurity.gov.tr/publications/uksgf.pdf , (Erişim tarihi 15. 12. 2013).

China - The World Factbook, https://www.cia.gov/library/publications/resources/the-world-factbook/geos/ch.html, (Erişim tarihi 24.04.2016).

Clausewitz,C. V. (1975). Savaş üzerine, (Çev.: Şiar Yalçın), Eriş Yayınları, Ankara.

Çifci, H. (2013). Her Yönüyle Siber Savaş, Tubitak, Ankara.

"Çin'den ABD ordusuna siber saldırı" , (2013), http://www.internethaber.com/cinden-abd-ordusuna-siber-saldiri-531441h.htm , (Erişim tarihi 10.12.2013)

"Çin Askeri Stratejisini Yeniledi", (2015), http://www.turkishny.com/headline-news/2-headline-news/181177-cin-askeri-stratejisini-yeniledi?utm_source=dlvr.it&utm , (Erişim tarihi 22.12.2015).

"Çin'in Büyüme Hızı Düşüyor", (2016), http://www.dw.com/tr/%C3%A7inin-b%C3%BCy%C3%BCme-h%C4%B1z%C4%B1-d%C3%BC%C5%9F%C3%BCyor/a-18988343, (Erişim tarihi 23.04.2016).

"Çin'in gizli 'Süper Ordu'su Ortaya Çıktı" , (2011), http://www.milliyet.com.tr/cin-in-gizli-super-ordu-su-ortaya-cikti/dunya/dunyadetay/27.05.2011/1395440/default.htm , (Erişim tarihi 22.12.2015).

"Çin de Ay'a Ayak Bastı", (2013). http://www.radikal.com.tr/hayat/cin_de_aya_ayak_basti-1166228 , (Erişim tarihi 29.12.2013).

Demir, S. (2012). Küresel Güvenlik Ortamının Analizi; Riskler, Aktörler, Beklentiler, Tedbirler. (Ed. Erol, M. S. Ve Efegil, E.) ,Türk Dış Politikasında Güvenlik Arayışları ss.31-65, Barış, Ankara.

"Devletler İçin Yeni Tehdit Algısı: Siber Savaş" , (2013), http://www.sondevir.com/analiz/113482/devletler-icin-yeni-tehdit-algisi-siber-savas.html , (Erişim tarihi 18.12.2013).

Dünya, "ABD'nin yeni savunma doktrini Çin'i kızdırdı" , (2012), http://www.dunya.com/abdnin-yeni-savunma-doktrini-cini-kizdirdi-143291h.htm , (Erişim tarihi 16.12.2013).

"Devletler İçin Yeni Tehdit Algısı: Siber Savaş", (2013), http://www.sondevir.com/analiz/113482/devletler-icin-yeni-tehdit-algisi-siber-savas.html , (Erişim tarihi 18.12.2013)

Eralp,A. (2006). Devlet, Sistem ve Kimlik, İletişim, İstanbul.

"Füze İhalesinde Türkiye'nin Çıkarı", (2013), http://www.diplomatikgozlem.com/TR,4497/fuze-ihalesinde-turkiyenin-cikari.html, (Erişim tarihi 24.04.2016).

Gürkaynak, M. & Adem, A. İ. (2011). "Reel Dünyada Sanal Açmaz: Siber Alanda Uluslararası İlişkiler" , Süleyman Demirel Üniversitesi İİBF Dergisi, C.16, S. 2.

Hobsbawm, E. (2006). Kısa 20. Yüzyıl, Everest, İstanbul.

Karabulut, B. (2011). Güvenlik, Barış Kitap, Ankara.

Kardas, T. (2007). "Güvenlik: Kimin Güvenliği ve Nasıl?". (Ed. Zeynep Dağı), Uluslararası Politikayı Anlamak: Ulus-Devletten Küreselleşmeye, Alfa, İstanbul.

Lord, W. T. (2009), "Cyberspace Operations: Air Force Space Command Takes the Lead", High Frontier, 5(3), ss. 3-5.

Menon, R. (2013). "Asya'da Yeni Güç dağılımı" , http://media.dunyabulteni.net/file/2013/asyada-yeni-guc-dagilimi.pdf , (Erişim tarihi 20. 12. 2013).

Morgenthau, H. (1993). Politics Among Nations, McGraw Hill, Boston.

Morgenthau, H. J. (1970). Uluslararası Politika, (Çev.:Baskın Oran &Ünsal Oksay), Sevinç Matbaası, Ankara.

"May 6-12; The First World Hacker War", (2001), http://www.nytimes.com/2001/05/13/weekinreview/may-6-12-the-first-world-hacker-war.html , (Erişim tarihi 30. 12. 2013).

Onar, A. (2016). "Siber Güvenlik, Siber Savaş ve Ulusal Güvenlik", http://www.medyapusula.com/files/uploads/siber.pdf , (Erişim tarihi 26.04.2016).

Orallı, L. E. . (2014). "Uluslararası Hukukta ve BM Sisteminde Askeri Müdahale Olgusu", http://tesamakademi.com/download/4.pdf , (Erişim tarihi 25.04.2016).

Önok, M. (2013). "Avrupa Konseyi Siber Suç Sözleşmesi Işığında Siber Suçlarla Mücadelede Uluslararası İşbirliği", http://edergi.marmara.edu.tr/maruhad/issue/download/5000001567/5000000648, (Erişim tarihi 20.12.2015).

Örmeci, O. (2013), "21.Yüzyılda ABD-Çin Rekabeti", SDÜ F en Edebiyat Fakültei Sosyal Bilimler Dergisi, (29), ss.1-14.

Pehlivan O. K. (2013). "Siber Güç Kapasitesi Asimetrik Savaşın Parametreleri" , Analist, ss. 62-67, USAK, Ankara.

Sandıklı, A. (2005). Geleceğin Süper Gücü Çin, Tasam, İstanbul.

"Siber Savaşta ABD İntikamı", (2014). http://www.cumhuriyet.com.tr/haber/dunya/170743/Siber_savasta_ABD_intikami.html , (Erişim tarihi, 14.02.2014)

"Siber Suçlar Sözleşmesi'nin bilinmeyen yüzü", (2010). http://ekonomi.haberturk.com/yazarlar/selin-kunt/581380-biz-neye-imza-attik , (Erişim tarihi 30.12.2013)

Sönmezoğlu, F. (1996). Uluslararası İlişkiler Sözlüğü, Der Yayınları, İstanbul.

Şeker, S. (2015). "Bilgi Çağının Değerlendirilmesi", ab.org.tr/ab05/tammetin/9.doc, (Erişim tarihi, 13.02.2015).

The 15 countries with the highest military expenditure in 2013, http://www.sipri.org/googlemaps/milex_top_15_2013_exp_map.html, (Erişim tarihi 13.02.2015)

United States - The World Factbook, https://www.cia.gov/library/publications/resources/the-world-factbook/geos/us.html , (Erişim tarihi 12.02.2015)

Vilidamir, Platov , "The USA and cyberwars", http://journal-neo.org/2013/10/15/rus-ssha-i-kibervojny-chast-1/ , (Erişim tarihi 26. 12. 2013).

Yayla, M. (2013). "Uluslararası Hukukta Siber Saldırılara Karşı Kuvvet Kullanma", TBB Dergisi, (107), ss.199-220.

Wıng, R. L. (1995). Strateji Sanatı, (Çev. M. S.Denker), Ezgi Kitabevi, Bursa.

"5 Apr. 2016: World military spending resumes upward course, says SIPRI", http://www.sipri.org/media/pressreleases/2016/milex-apr-2016, (Erişim tarihi 24.04.2016).