

HUKUKİ BİR TERİM OLARAK “SİBER SAVAŞ”

“CYBER WAR” AS A LEGAL TERM

Mehmet YAYLA**

Özet: Siber güvenlik, 21. yüzyılda ulusal güvenliğin en yeni sorunudur. “Siber savaş”, uluslararası ilişkilerde bilgisayar ve iletişim teknolojilerini saldırı ve savunma amaçlı olarak kullanmaktadır. Şu ana kadar, siber savaş teriminin anlamı ve bu savaşı düzen altına alan kurallar konusunda fikir birliğine varılamamıştır.

Uluslararası hukuk sisteminin, bu yeni savaş alanı ile ilgili düzenlemeler yapması gerekmektedir. Fakat, siber savaş konusunda ulusal ve uluslararası kural ve stratejinin ne olacağını tartışmadan önce, siber savaş teriminin bir hukuk terimi olarak açıklanması önem arz etmektedir. Çünkü, kelimeler hukuk biliminin vazgeçilmez malzemesidir. Bundan dolayı, hukuki ve etimolojik bakış açılarıyla üzerine düşünülmesi en az bilimin içeriği kadar hak etmektedir. Bu çalışmada, siber savaş bir hukuk terimi olarak incelenmiştir.

Anahtar Sözcükler: Siber savaş, uluslararası hukuk, siber güvenlik, siber suç, siber terörizm, siber casusluk.

Abstract: Cybersecurity is the newest national security issue in the twenty-first century. Cyber war uses computer and telecommunications technologies as defensive and offensive weapons in international relations. Until now, neither its meaning nor the international laws that govern the concept of cyber war have been discussed.

The international legal system must adapt to this battleground. But, before discussing what national and international rules and strategy should be developed, It is important to explain “cyber war” as a legal term. Because words are inevitable instruments of jurisprudence. So, they merit to be thought with legal, etymological perspectives at least as contents of sciences. In this study; cyber war as a legal term has been examined.

Keywords: Cyber war, international law, cyber security, cyber crime, cyber terrorism, cyber espionage.

* Bu makale, TÜBİTAK tarafından sağlanan destek kapsamında 2012-2013 döneminde ABD The City University of New York John Jay College’da yürütülen çalışmalar kapsamında hazırlanmıştır.

** Dr., Askeri Yargıtay Başsavcı Yardımcısı

I. Giriş

Sosyal bilimlerin her dalında olduğu gibi, hukukta da bazı temel kavramların etimolojik, tarihi ve sosyal kökeninin araştırılması, daha sağlıklı tespitler yapmak bakımından büyük bir ihtiyaçtır.

İnsanlar, yeryüzünde kullanılan kelime ve terimleri, yaşanan olayların günlük hayatta yarattığı ihtiyaç ve değişikliklerden ötürü oluşturmuştur. Bu değişimi toplumsal yapılarda adlandırma çabaları, Sanayi Toplumu’ndan Bilgi Toplumu’na geçiş biçiminde yoğunlaşmaktadır.¹ Teknoloji ile ilintili olan kelime ve terimler, en çok değişim geçirmeye elverişli olanlardandır.

İnsanoğlu teknolojik alanında son çeyrek asırda yaşanan devrim niteliğindeki gelişmelerle birlikte, hayal bile edemeyeceği bir yaşam standardına ve tarzına ulaşmıştır. Bilgisayarlar küçülmüş, cep telefonları neredeyse bilgisayar halini almış ve bu iki cihazın götürülemediği veya kullanılmadığı yaşam alanı yok denecek kadar azalmıştır. Bu gelişmeler, hukuk alanında da önemli birtakım sorunlara neden olmuş, yeni kavramlar ortaya çıkmış, bu kavramların tanımları tartışılmaya ve hukuki açıdan sonuçlar doğurmaya başlamıştır.

Konuyla uluslararası hukuk ve ceza hukuku bakımından bakılacak olursa, bilişim alanındaki saldırılar ve suçlar en güncel ve en hızlı değişim gösteren konulardandır. Nitekim teknolojik alanda yaşanan gelişmelere bağlı olarak, daha önceden siber ortamda hiç öngörülemeyen bir takım yeni fiiller ortaya çıkabildiği gibi, bazı fiillerin yeni yöntemlerle işlenmesi de söz konusu olabilmektedir. Bu nedenle, uluslararası ortamda düzenlemeler yapılmakta, bunlara bağlı olarak da devletlerin mevcut düzenlemelerini değiştirmesi ya da yeni düzenlemeler yapması gerekmektedir. Aksi takdirde ortaya çıkabilecek hukuki boşluklar, sosyal hayatta önemli sorunların yaşanmasına neden olmaktadır.

Düzenleme yapılmadan önce, bilişim alanındaki değişimlerin yakından takip edilerek, bunlara yönelik terimlerin doğru bir şekilde tanımlanması zorunluluğu da ortaya çıkmaktadır. Ancak, bu alanda gelişmeleri takip etmek ve uygun tanımları ortaya koymak, uluslararası alanda uzlaşma ve ulusal alanda düzenleme yapmak hukukçuların

¹ Güney Nair, “Bilgi’nin Değişen Anlamı ve Kavram Tartışmaları” C.Ü. İBF Dergisi Doç. Dr. Feramuz Aydoğan’ın Anısına, s.329.

karşılaştığı zorluklardandır. Ayrıca, bu alanda çalışan bir hukukçunun, sadece iyi bir hukukçu kimliğine sahip olması, bu alanda uzmanlaşabilmesi bakımından yeterli olmamakta; bunun yanında bilişim sistemlerine, bu sistemlere bağlı olarak kullanılan teknolojik ürünlere ve internete ilişkin oldukça kapsamlı bilgilere de sahip olması gerekmektedir. Bunun yanında, yeni gelişen teknolojinin bilişim ortamındaki imkânları genişletmesi, terimleri tanımlamada en büyük sorun olarak hukukçuların karşısına çıkmaktadır.

Hukukta terimlerin ne anlama önem taşımaktadır. Eskilerin deyişiyle, hukukta her kavram “*efradını câmi, ağıyarını mâni*” olmalı, yani içermesi gereken tüm unsurlarını içermeli ve içermemesi gereken hiçbirini bünyesinde barındırmaması gerekmektedir. Aksi takdirde, hukuk dünyasında doğacak kavram karmaşası hukukun nesnelliğini yok ederek anarşinin yolunu açacaktır. Bu bağlamda, hukukun ‘endemik’ nitelikteki zorlayıcılık özelliği göz önünde tutulduğunda; hukukta meydana gelebilecek bir keşmekeşin, diğer alanlarda olabilecek sorunlardan çok daha fazla tehlikeye yol açabileceği söylenebilecektir.²

Günümüzde bilim ve teknolojiye baş döndürücü tarzda hızlı gelişmeler görüldüğünden hukuk ve bilim birlikte çalışmalı ve birbirleriyle ilişki kurmalıdır. Siber savaş terimi ve önemi üzerine yapılacak olan bir analiz kavramın somutlaştırılmasına hukuk dünyasında daha anlaşılır hale gelmesine faydalı olacaktır.

II. Siber Savaş Terimi

1. Dilbilgisi Bakımından

Türk Dil Kurumu Büyük Türkçe Sözlüğü’ne bakıldığında siber savaş tanımlanmış değildir. Siber savaş, iki isimden oluşan bir isim tamlamasıdır. Dilbilimsel açıdan incelendiğinde görülecektir ki; isim tamlamalarında asıl ifade edilmek istenen, temel, geniş kavram ikinci sözcükte yer alır. Birinci sözcük ise ikinci sözcüğün bir türünü, dalını veya yönünü oluşturur. İlk sözcük ikinci sözcüğü anlamsal olarak sınırlar ve ayırır.³

² Faruk Y. Turinay, “Bir Kelime Olarak Anayasa’nın Tarihsel Yolculuğu Üzerine Düşünceler”, Türkiye Barolar Birliği Dergisi, sayı 95, 2011, s.271.

³ Turinay, s.278.

Siber savaş terimi, İngilizce “*cyber war*” (siber savaş) teriminden dilimize çevrilerek kullanılmaya başlamıştır. İngilizce’de “*cyber*” kelimesi “*siber*”, “*war*” kelimesi ise savaş anlamına gelmektedir.⁴ Bu kapsamda “*siber savaş*” kavramını tanımlamaya, “*siber*” ve “*savaş*” kelimelerini tanımlayarak başlamak gerekmektedir.

a. “Siber”

Yalın olarak Türkçe sözlüklerde yer almayan “*siber*” kelimesi, sibernetik⁵ kavramından türetilmiş olup günümüzde bilişim ve iletişim ağlarının şekillendirdiği uzayı ifade etmektedir. Sibernetik, ilk olarak Norbert Wiener’in “*Sibernetik*” isimli kitabında, “*hayvanlarda ve makinelerde kontrol ve iletişim*” olarak tanımlanmıştır.⁶ “*Siber uzay*” terimi ise ilk olarak 1984 yılında “*Neuromancer*” adlı bilim kurgu romanında William Gibson tarafından kullanılmış olup, etimolojik açıdan siber ve uzay kelimelerinin bir araya gelmesinden oluşmaktadır.⁷ Sonrasında, siber uzay terimi akademik ortamda da kullanılmaya başlanmış ve teknolojinin gelişmesi ile birlikte tanımı da değişmiştir.

Bilgisayar kullanımındaki artış benzeri görülmemiş toplumsal değişimlere yol açmış ve insan hayatını inanılmaz derecede kolaylaştırmıştır. İnternetin yaygın olarak kullanılmaya başlanması ile coğrafi kısıtlamalar ortadan kalkmış, insanların her türlü elektronik bilgi hizmetine erişimini mümkün kılan yeni bir dünya oluşmuştur. Bu dünya zamanla siber uzay olarak tanımlanmıştır.⁸

⁴ Cambridge Dictionaries Online, <http://dictionary.cambridge.org/dictionary/turkish/cyber?q=cyber>, <http://dictionary.cambridge.org/dictionary/turkish/war?q=war>, erişim tarihi:12.11.2012; Resuhi Akdikmen, Langenscheidt Standart Sözlüğü, İnkilap Kitapevi, İstanbul, 1992, s.599.

⁵ Sibernetik; Türk Dil Kurumu Sözlüğünde “*güdümbilimi*” olarak tanımlanmaktadır. <http://tdkterim.gov.tr/bts/>, erişim tarihi:30.10.2012. Sibernetik sistemleri, “*algılayıcılarından aldığı bilgilerle geri besleme sağlayan ve kendi kendine işleyen otomatik sistemler*” şeklinde tanımlamak mümkündür.

⁶ Norbert Wiener, *Cybernetics: or Control and Communication in the Animal and the Machine*. Paris, (Hermann & Cie) & Camb. Mass., 1948.

⁷ Jason Whittekar, *The Cyberspace Handbook*, Oxon, Routledge, 2004, s.4; “*Siber uzay*” terimi ilk defa, 1982 yılında William Gibson tarafından “*Burning Chrome*” isimli kısa hikâyede kullanılmıştır. Ancak Gibson’ın bu terimi “*Neuromancer*” isimli romanında kullanmasıyla popüler hale gelmiştir. Vassily Fourkas, *What is cyberspace?*, <http://www.waccglobal.org/en/20043-communication-rights-unfinished-agenda/495-What-is-cyberspace.html>, erişim tarihi:13.11.2012.

⁸ Rich Gibson, Schuyler Erle, *Google Maps Hack*, U.S.A., O’Reily Media Inc., 2006, s.97.

Birleşmiş Milletler Terimler Sözlüğü siber uzayı, net olarak bilinen internete, iletişim altyapısına, online konferans kuruluşlarına, bilgi depolama ve işleme aygıtlarına bağlı global sistem olarak tanımlarken⁹, Amerikan Savunma Bakanlığı'nın Askeri Terimler Sözlüğü ise; internet, telekomünikasyon ağları, bilgisayar sistemleri, gömülü işlemci ve kontrol sistemleri gibi birbirine bağlı bilgi teknolojileri altyapılarını kapsayan bilgi ortamı olarak tanımlamaktadır.¹⁰

Siber uzay, günümüzde tek bir homojen uzaydan oluşmamaktadır. Çok sayıda, hızla genişleyen, her biri farklı bir sayısal etkileşim ve iletişim yöntemi sağlayan uzayların bir birleşimidir.

Siber uzayın gayri merkezi, sınırları olmayan, ağ biçimindeki yapısı onun herhangi bir devletin, dolayısıyla herhangi bir hukuk düzeninin yek egemenliği altına sokulmasına engel olmakta ve aynı zamanda hangi fiillerin siber suç olduğu tanımını da zorlaştırmaktadır. Vatandaşlık, ulusal sınır gibi kavramların çok da anlam taşımadığı siber uzayda, ülkelerin egemenlik yetkilerini meşrulaştırmasına, başka bir deyişle hukuk kuralı koyma ve uygulama haklarını sağlam temeller üzerine oturtulmasına ihtiyaç duyulmaktadır. Siber uzayın yeni bir hukuk alanı olduğu genel kabul görmekle birlikte asıl üzerinde uzlaşmaya varılamayan konu, hukukun kim tarafından konulacağı ve nasıl uygulanacağı sorunudur. Her ne kadar siber uzay, ulusal devletlerin fiziki sınırları içinde bir kısım dijital alanı kapsıyorsa da aynı zamanda farklı ülkelerin de ulusal alanını işgal etmektedir.

Gerçek dünya, insanlar tarafından binlerce yılın sonunda ulusal ve uluslararası hukuk kuralları ile yönetilirken siber uzay yapısı gereği yeterince bu hukuk kurallarından nasibini alamamaktadır.

b. "Savaş"

Savaşın tarihi, insanlık tarihi kadar eskidir. Devletler, çıkarlarını korumak ve hayat alanlarını genişletmek amacıyla düzenli ordular

⁹ United Nations, UN Terms, <http://unterm.un.org/dgaacs/unterm.nsf/WebView/99B98BDBCBAB096185256E620052EFD3?OpenDocument>, erişim tarihi:31.10.2012.

¹⁰ Department of Defence Dictionary of Military and Associated Terms (Joint Publications 1-02), http://www.dtic.mil/doctrine/new_pubs/jp1_02.pdf, erişim tarihi:30.10.2012.

kurmuşlar, iktidarı elinde tutan kimseler ise iktidarlarını pekiştirmek ve güçlendirmek amacıyla silahlı güç kullanılması yöntemlerine sıkça başvurmaktan çekinmemişlerdir. Uluslararası düzenin en başta gelen süjeleri olan devletler bakımından, savaşa başvurulmasında amaç ulusal çıkarların korunmasıdır.¹¹

Savaşın tanımlanması hukuksal, ideolojik, felsefi, siyasal, ekonomik, sosyolojik ve psikolojik boyutlarıyla yakından ilgilidir. Uluslararası hukukta savaşın herkes tarafından kabul edilmiş bir tanımı yapılamamıştır. Bunun sebebi, bir silahlı çatışmanın veya eylemin savaş sayılıp sayılmayacağı hususunda uluslararası hukukta objektif bir ölçütün benimsenememiş olmasıdır. Herhangi bir silahlı çatışma eyleminin savaş sayılıp sayılmayacağı hususundaki temel ölçüt ilgili devletlerin amacı olarak değerlendirilmektedir. Bu sebeple, savaşan taraflardan herhangi birisinin savaş amacıyla hareket etmesi durumunda, söz konusu silahlı çatışmaların savaş olarak değerlendirilmesi gerekmektedir.¹² Dolayısıyla, taraflardan en az birisi tarafından savaş değerlendirilmesi yapılmadıkça, bütün silahlı çatışma türlerinin savaş niteliğini taşımayan silahlı “zararla karşılık” veya silahlı “karışma” şeklinde değerlendirilmesi uygun görülmektedir.¹³

Savaş; “bir toplumun, bir ulusun veya devletler topluluğunun isteklerini diğer bir ulus ve devletler topluluğuna zorla kabul ettirmek amacıyla giriştikleri bir mücadele” şeklinde tanımlanmasının yanında¹⁴, “uluslararası hukuk kurallarına uygun şekilde devletlerarasında yürütülen silahlı bir çatışma, bir çekişmedir”¹⁵ şeklinde de tanımlanmaktadır.¹⁶

¹¹ Funda Keskin, *Uluslararası Hukukta Kuvvet Kullanma: Savaş, Karışma ve Birleşmiş Milletler*, Ankara, Öteki Matbaası, 1998, s.15.

¹² Yasin Aslan, “Savaş Hukukunun Temel Prensipleri”, *Türkiye Barolar Birliği Dergisi*, Sayı 79, 2008, s.249.

¹³ Seha L. Meray, *Devletler Hukukuna Giriş*, Ankara Üniversitesi Siyasal Bilgiler Fakültesi Yayınları, 1962, s.407-456.

¹⁴ Yoram Dinstein, *War, Aggression and Self-Defence, Second Edition*, Grotius Publications, Cambridge: Cambridge University Press, 1995, s.15.

¹⁵ Meray, *Devletler Hukukuna Giriş*, s.469.

¹⁶ Türk hukukunda, 2941 sayılı Seferberlik ve Savaş Hali Kanunu’nun 3. maddesinin 5. fıkrasında savaş, “devletin bekasını temin etmek, milli menfaatleri sağlamak ve milli hedefleri elde etmek amacıyla, başta askeri güç olmak üzere, Devletin maddi ve manevi tüm güç kaynaklarının, hiçbir sınırlamaya tabi tutulmadan kullanılmasını gerektiren silahlı mücadele” olarak tanımlanmaktadır. Bakınız 8 Kasım 1983 tarih ve 18215 sayılı Resmi Gazete.

Tarih boyunca, bir devletin silahlı kuvvet kullanmaya başvururken haklı bir sebebe dayanması büyük önem taşımıştır. Savaşa başvurmanın ve saldırının uluslararası hukukta yasaklanmasıyla birlikte, devletler yine de silahlı kuvvet kullanma hakkından vazgeçmiş değillerdir. Artık bunu savaş değil de, başka isim ve yöntemler kullanarak yapmaya başlamışlardır. Günümüzde uluslararası silahlı çatışma, uluslararası uyuşmazlıkların barışçı yöntemlerle çözülememesi durumunda, devletlerin isteklerini zorla kabul ettirmek amacıyla, silahlı kuvvetlerin kullanılması da dâhil olmak üzere, ulusal güçlerinin tamamını veya bir kısmını kullanarak yaptıkları mücadele anlamına gelmektedir.¹⁷

2. Siber Savaş Teriminin Anlamı ve Genel Kullanımı

İnsanoğlu ilk başlarda bir birinden çok farklı özellikler gösteren iki alanda savaşmıştır; “kara” ve “deniz”. Yüzyıl öncesinde ise hava teknolojisinin gelişmesi ile birlikte üçüncü savaş ortamı “gökyüzü” olmuştur. 1957 tarihine gelindiğinde ise dördüncü savaş ortamı “uzay” olarak kabul edilmiştir. Bu dört savaş ortamının da kendine has özellikleri ve gereklilikleri bulunmaktadır. 21. yüzyıla gelindiğinde bu dördüne beşinci savaş ortamı eklenmiştir; “siber ortam”.¹⁸

Askeri doktrinde, siber ortamın beşinci savaş ortamı olduğu kabul edilmektedir. Ordular da kendilerini bu yeni ortamda savaşacak imkân ve kabiliyetleri kazandırmak maksadıyla hazırlıklar yapmaktadırlar. Ülkeler arası ilişkilerde olduğu kadar, savaşta ve düşük yoğunluklu çatışmada da siber ortam, saldırı ve savunma amaçlı olarak kullanılmaya başlanmıştır.

Neredeyse tüm bilginin siber ortamda depolandığı ve işlendiği, cihazların siber ortamda yönetildiği, orduların operasyonel üstünlüğünün, elektronik haberleşme, görüntü alma, uzaktan algılama gibi taktiklere dayandığı günümüzde, beşinci savaş alanı olan siber ortama göre saldırı ve savunma strateji ve taktikleri geliştirilmektedir. Uluslararası ilişkilerde, ülkeler arası anlaşmazlıkların çözülmesi için

¹⁷ Aslan, s.250.

¹⁸ Beyaz Saray tarafından 2003 yılındaki “Siber Ortamın Güvenliği için Ulusal Strateji” belgesinde “siber ortam, ülkenin kontrol sistemidir... kritik altyapıların çalışmasını sağlayan birbirine bağlı bilgisayarlar, servis sağlayıcılar, fiber kablolar, elektronik anahtar ve yönlendiriciler oluşur.” şeklinde tanımlanmıştır.

orduların caydırıcı bir güç olarak kullanılmasına, siber orduların ve saldırıların da dahil edildiği bir zamana gelinmiştir.

11 Eylül 2001 günü İkiz Kuleler ile birlikte tehdit konusundaki geleneksel anlayış da yıkılmış, elli yıldan fazladır dünyaya hâkim olmuş olan Soğuk Savaş senaryosu tam anlamıyla ve geri dönülemez biçimde değişmiştir. Tehdidin açık bir "gönderici adresi" olmadığı, devletlerin toprak sınırlarının yanı sıra askeri mekân ve zaman kurallarının da anlamsız hale geldiği anlaşılmıştır. Sivil uçakların bir terör saldırısı aracı olarak kullanılması hemen hemen her şeyin her an silaha dönüşebileceğini göstermiş ve hiçbir şeyin imkânsız olmadığı ortaya çıkmıştır. Siber tehdit için de durum aynı gözükmektedir.¹⁹ Yeni teknolojik gelişmeler siber uzaydaki imkânları arttırarak bireyleri, organizasyonları ve devletleri tehdit etmektedir. Bu tehditlerin en önemlisi siber savaş olarak değerlendirilmektedir.

Kamuoyu, siber saldırı ve siber suç terimleri ile çokça aşına olmasına rağmen, son on yıllık zaman zarfında siber savaş terimi gündemi daha fazla meşgul etmeye başlamış ve devletler siber savaşı, taktikleri ve doktrinlerine almaya başlamışlardır.²⁰ Siber savaş için yapılmış uluslararası anlaşma olmadığı için bu terimin tanımlanması ve neyin siber savaş oluşturduğu tartışma konusudur. Diğer bir tartışma konusu ise siber savaşın gerçek bir savaş olup olmadığı ve silah kullanımına ilişkin uluslararası kuralların ve teamüllerin siber savaşa uygulanıp uygulanamayacağıdır. Bu belirsizlik siber savaş teriminin tanımlanmasını zorlaştırmaktadır.

Birleşmiş Milletler Terimler sözlüğünde, siber savaş (cyber war) bilgi savaşı (information warfare) ile birlikte aynı anlamda "bilgisayar sistemlerinin düşman sistemlerine zarar vermek veya yok etmek amacıyla kullanıldığı savaş tipidir" şeklinde tanımlanmaktadır.²¹

¹⁹ Olaf Theiler, "Yeni Tehditler:Siber Boyut", NATO Dergisi On Yıl Sonra Alınan Dersler, <http://www.nato.int/docu/review/2011/11-september/Cyber-Threads/TR/index.htm>, erişim Tarihi: 3.11.2012.

²⁰ Aslında "siber savaş" terimine medyatik olarak 1983 yapımı "Savaş Oyunları (War Games)" isimli Amerikan yapımı film ile aşına olunmuştur. Bu filmde bir çocuğun askeri network ağına girerek kaza ile üçüncü dünya savaşını başlatması konu edilmiştir. Siber savaşa ilişkin olarak yapılan ve popüler olan diğer filmler ise, 1992 yapımı "Sneakers (Şifreciler)" ve 2007 yapımı "Zor Ölümler 4 (Die Hard 4)" dır. Bunlar dışında, siber uzayın kötü amaçlar için kullanıldığı birçok film yapılmış ve kitap yazılmıştır.

²¹ United Nations, UN Terms, <http://unterm.un.org/dgaacs/unterm.nsf/Web->

“Cyberwar”, İngilizce bazı sözlüklerde de “*information war*” (bilgi savaşı) teriminin eş anlamlısı olarak kullanılmakta ve “*elektronik iletişim ve internetin bir ülkenin iletişim sistemi, güç kaynakları, ulaşım sistemi ve benzeri sitemlerini bozması veya çökertmesi*” olarak tanımlanmaktadır.²²

Konunun yeni yeni ortaya çıkmaya başladığı 1990’lı yıllarda bazıları tarafından siber savaş olgusu “*bilgi savaşı*” ile birlikte değerlendirilmiş ve askeri doktrinde siber savaş bilgi savaşı içinde icra edilen hareketlerden sayılmıştır.²³ Bilgi savaşı, siber savaş da kapsayacak bir üst terim olmasına rağmen günümüzde siber savaş ve bilgi savaşı terimleri birbirinin eş anlamlısı terimler olarak kabul edilememektedir.²⁴

Bilgi savaşı, bilginin yer aldığı ortamların ve bilginin kendisinin, düşman harp gücünü azaltmak ve yok etmek maksadıyla hedef alınması veya kendi lehte kullanılması faaliyetlerini içeren bir harekât türüdür. Bu harekâtın harp zamanında uygulanmasına ise bilgi savaşı denmektedir.²⁵

Siber savaş ise, “*devletler veya devlet benzeri aktörler tarafından gerçekleştirilen, kritik ulusal altyapıları, askeri sistemleri veya ülke için önemli*

View/E996B25EA7D3B36 E85256B090056D806?OpenDocument, Erişim tarihi: 31.10.2012.

²² Collins Dictionaries, <http://www.collinsdictionary.com/dictionary/english/cyberwar>, Free Dictionary, <http://www.thefreedictionary.com/cyberwar>, Oxford Dictionaries, http://oxforddictionaries.com/definition/american_english/cyberwar?region=us&q=cyber+war, Macnillan Dictionary, <http://www.macmillandictionary.com/dictionary/american/cyberwar>, erişim tarihi:11.11.2012.

²³ Thomas C.Wingfield, *The Law of Information Conflict: National Security Law in Cyberspace*, Aegis Research Corp., 2000, s.29; Bilgi savaşı; elektronik savaş, siber savaş, bilgisayar ağları harekâtı gibi alt kavramları içermektedir. Nafi Kaşıkçıoğlu, “Elektronik Harp”, *Siber Savunma Sempozyumu*, Askeri Müze ve Kültür Sitesi Komutanlığı, Harbiye, İstanbul, 24-25 Mayıs 2011; Martin C. Libicki, *What is Information Warfare?*, National Defence University, Washington, 1995, s.7, 75 vd; Siber savaşın açık tanımı verilmese de, Bilgi Savaşı, NATO Bilgi Harekâtı Konseptine göre; “*politik ve askeri hedefleri desteklemek maksadıyla, kendi bilgi ve bilgi sistemlerini etkili bir şekilde kullanarak ve korurken, hasmın bilgiye dayalı işlemlerini, komuta kontrol, muhabere ve bilgi sistemlerini etkileyerek karar vericilerin başarılı olmalarını sağlamak maksadıyla icra edilen faaliyetlerdir*” şeklinde tanımlanmaktadır.*Türk Silahlı Kuvvetleri Bilgi Harbine Nasıl Hazırlanmalıdır?*, Harp Akademileri Yayınları (Tasnif Dışı), İstanbul, 1999, s.1-14.

²⁴ *Cyber Space Operations* (US Air Force Doctrine Document 3-12, 15.6.2010), s.2, <http://www.e-publishing.af.mil/shared/media/epubs/AFDD3-12.pdf>, Erişim tarihi: 15.11.2012.

²⁵ *Joint Doctrine for Information Operations* (Joint Pub 3-13), 9.10.1998, s.I-1, http://www.c4i.org/jp3_13.pdf, Erişim Tarihi:2.11.2012.

endüstriyel yapıyı tehdit eden, simetrik veya asimetrik, saldırı veya savunma maksatlı dijital ağ faaliyetleri"dir.²⁶ Diğer bir siber savaş tanımı ise savaş tanımından yola çıkılarak, "ülkelerin ulusal güçlerinin tamamını veya bir kısmını kullanarak siber ortamda gerçekleştirdikleri mücadele" olarak yapılabilir. Burada gözden kaçırılmaması gereken nokta, mücadele siber ortamda gerçekleştirilse de sonuçlarının siber ortamda olduğu kadar fiziksel ortamda da görülebilecek olmasıdır. İşte bu nokta siber savaş, klasik anlamda bir savaş ile kıyaslar hale getirmekte ve uluslararası hukuk ve silahlı çatışma hukuku açısından önemli kılmaktadır.

Siber savaşın tarihçesi, ABD tarafından Irak'ın sistemlerinin havadan etkisiz hale getirilmesinin planlandığı Körfez Savaşı zamanlarına kadar geri götürülmektedir.²⁷ Bu savaşın hemen ardından ABD Hava Kuvvetlerinde, Bilgi Savaşı Merkezi (Info War Center) kurulmuştur. 1995 yılında ise ABD Ulusal Savunma Üniversitesi siber savaşa komuta edecek olan ilk subaylarını mezun etmeye başlamıştır.

ABD'de George Bush'un ikinci döneminde bu yeni savaş alanının önemi çok açık hale gelmiş ve yeni ortaya çıkan bu alanı kimin kontrol etmesi gerektiği tartışılmaya başlanmıştır. Bu gelişmelerin sonucunda Uzay Komutanlığı (Space Command), Stratejik Komutanlığa (Strategic Command-STRATCOM) dönüştürülmüş ve bu komutanlığa siber savaşa komuta etme yetkisi verilmiştir. 2008 yılına ABD, siber savaşın önemi konusunda ikna olmakla kalmamış aynı zamanda ayrı bir siber komutanlık kurulmasının gerekliliğine inanmaya başlamıştır.²⁸ Bu gelişmelerin devamında 23 Haziran 2009 tarihinde Stratejik Komutanlığa, Siber Komutanlık kurulması emri verilmiş, 21 Mayıs 2010 tarihinde itibaren de Siber Komutanlık (CYBERCOM) kurulmuştur.²⁹

²⁶ Shane M. Coughlan, *Is There a Common Understanding of What Constitutes Cyber Warfare?*, (Yayınlanmamış Yüksek Lisans Tezi), The University of Birmingham 2003, s.2, <http://citeserx.ist.psu.edu/viewdoc/download?doi=10.1.1.102.1876&rep=rep1&type=pdf>, erişim tarihi: 15.05.2012

²⁷ Shitanshu Mishra, "Network Centric Warfare in the Context of Operation Iraqi Freedom" *Strategic Analysis*, V.27, I.4, s.546-547. http://www.idsa.in/strategicanalysis/NetworkCentricWarfareintheContextofOperationIraqiFreedom_smishra_1003, erişim tarihi: 5.11.2012.

²⁸ Clarke, a.g.e., s.6,3-21.

²⁹ US Department of Defence, *US Cyber Command Fact Sheet*, 25.5.2010, http://www.defense.gov/home/features/2010/0410_cybersec/docs/cyberfactsheet%20updated%20replaces%20may%2021%20fact%20sheet.pdf, erişim tarihi: 8.11.2012.

ABD Siber Komutanlığının görevi; Savunma Bakanlığının bilgi ağını korumak üzere operasyonlar düzenlemek, görev verildiğinde tüm alanlarda kapsamlı askeri siber alan operasyonları gerçekleştirmek, siber alanda ABD/müttefik özgürlüğünü sağlarken düşman faaliyetlerini kısıtlamak maksadıyla faaliyetler planlamak, koordine etmek, bütünleştirmek, senkronize etmek olarak tanımlanmıştır.³⁰

Teknoloji lideri ülke olarak bilişim ortamını en etkin kullanan Amerika'nın, siber tehdit ve siber savaşa karşı yaklaşım tarzını görmek için aşağıdaki açıklama önem arz etmektedir.³¹ Amerika Savunma Bakanı Leon Panetta'nın 11 Ekim 2012 tarihinde New York'ta işadamları ile yaptığı toplantıda, Amerika'nın "*Siber-Pearl Harbor*"³² ihtimali ile karşı karşıya olduğunu, düşman devletlerin ya da radikal grupların siber aletleri Amerika'nın kritik altyapılarının kontrolünü ele geçirmek için kullanabileceğini, bunların enerji kaynaklarını ele geçirebileceklerini, su kanallarını kirletebileceklerini, bir treni kimyasal madde ile doldurup saldırı amaçlı yönlendirebileceklerini belirtmiş, ayrıca en kötü ihtimalin kritik altyapı sistemlerine karşı yapılacak koordineli bir saldırı olduğunu, bu saldırıda insanların hayatlarını kaybedebilecekleri gibi, halkı şok edecek fiziksel zararlar meydana gelebileceğini belirtmiştir. Leon Panetta konuşmasında, böyle ciddi sonuçlar doğuracak bir saldırı tehdidi aldıklarında ulusun güvenliği için bu saldırılara karşılık verebileceklerini vurgulamıştır.³³ Hemen

³⁰ *US Cyber Command Fact Sheet.*

³¹ Kara, deniz, hava ve uzaydan sonra siber uzayı yani tüm sanal ortamı beşinci askeri kuvvet olarak belirleyen ABD, "*Aktif Milli Strateji*"yle siber kuvvetlerinin altyapısını kurmuş, Pentagon'u da devreye sokarak Ulusal Güvenlik Bürosu'nun (NSA) başkanı General Keith Alexander'ın komutasında ordular arası siber savaş projesi olan "*Siber Kuvvet Stratejisi (Cyber-Command Strategy)*"ni başlatmıştır. ABD'nin bu yeni siber savaş kuvvetlerinin görevi, askeri şebekeleri korumak ve gerektiğinde diğer ülkelerin her türlü sistemlerine saldırılar düzenlemektir.

³² Japon İmparatorluk Deniz Kuvvetleri'nin 7 Aralık 1941 Hawaii adalarının Oahu adasında bulunan Pasifik Filosu ve Pearl Harbor askeri üslerine karşı düzenlediği beklenmedik saldırıdır. Saldırı sonucu, 12 Amerikan savaş gemisi ciddi şekilde hasara uğramış veya batmış, 188 savaş uçağı imha olmuş ve 2.403 Amerikan askeri ile 68 sivil ölmüştür. Leon Panetta'nın yapmış olduğu "*Pearl Harbor*" benzetmesi, siber saldırıların her an gerçekleşebileceğini ve ne kadar büyük zararlar verebileceğini anlamak için önemlidir.

³³ Elisabeth Bumiller, Thom Shanker, "*Panetta Warns of Dire Threat of Cyberattack on U.S.*", *The New York Times*, 11 Ekim 2012, http://www.nytimes.com/2012/10/12/world/panetta-warns-of-dire-threat-of-cyberattack.html?pagewanted=all&_r=0, Erişim Tarihi:3.11.2012; ABD Ulusal Güvenlik Bürosu'nun (NSA) başkanı General

belirtmek gerekir ki, Savunma Bakanı'nın vurguladığı husus, saldırı olduğunda değil, saldırı tehdidi doğduğunda Amerikan hükümetinin buna karşılık verme hakkını kendinde görmesi ve bu saldırının siber ortamda yapılacak bir saldırıyı kapsadığı gibi, klasik anlamda silahlı bir saldırıyı da kapsamasıdır. Bu açıklama, Amerika Birleşik Devletlerine siber 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 ve silahlı çatışma hukuku açısından ne sonuçlar doğuracağını akla getirmektedir.

Konuya hukuki açıdan bakıldığında bazı yazarlar; siber savaşa gerektiğinden fazla önem verildiğini, gerçekleşecek bir siber saldırının, savaş nedeni olamayacağını, devlet kaynaklı politik bir siber saldırının, savaş kadar eski olan sabotaj, casusluk ya da tahrip amaçlı olabileceğini savunmaktadırlar.³⁴ Buna karşın, bugüne kadar yaşanan Estonya, Gürcistan ve İran'a karşı yapılan saldırılar siber savaşın ciddiyetini ortaya koymakta, uluslararası hukuk ve silahlı çatışma hukuku açısından konu değerlendirilmekte, düşman devlet veya devlet güdümlü alt gruplar tarafından gerçekleştirilecek bir siber saldırı durumunda, saldırıya uğrayan devlet tarafından Birleşmiş Milletler Şartı'nın 51. maddesindeki "*meşru müdafaa hakkı*"nın kullanılabileceği savunulmaktadır. Tabii olarak siber savaşın tanımı ve içeriği konusunda uluslararası ortamda fikir birliğine varılmadığı gibi bu konuda da tartışma devam etmektedir.

General Keith Alexander ise Başkan Obama'nın konuya verdiği önemi şu şekilde dile getirmektedir: "*Milli ve askeri güç bakımından siber uzay kritik öneme kavuşmuştur. Başkan Obama'nın ulusal güvenlik stratejisine göre, dijital altyapımız, ulusal varlığımızdır, kişi hak ve özgürlüklerini ihlal etmeden onu korumak milli güvenlikte önceliğimizdir.*" Donna MILES, "*New Cyber Chief: People Key in Meeting Cyberspace Challenge*", *The Official Website of U.S. Air Force*, <http://www.af.mil/news/story.asp?id=123207676>, erişim Tarihi:6.12.2011; Brian Krebs, "*Obama: Cyber Security is a National Security Priority*", *Washington Post*, 29.5.2009, http://voices.washingtonpost.com/securityfix/2009/05/obama_cybersecurity_is_a_natio.html, erişim tarihi: 7.11.2012

³⁴ Thomas Rid, "*Cyber War Will Not Take Place In*", *Strategic Studies*, Volume 35, Issue 1, 2012, s.5-32; Ryan Singel, "*White House Cyber Czar: There is no Cyber War*", *Wired*, 3.4.2010, <http://www.wired.com/threatlevel/2010/03/schmidt-cyberwar/>, erişim tarihi:10.11.2012; Ronald Deibert, "*Tracking the emerging arms race in cyberspace*", *Bulletin of the Atomic Scientists*, January/February 2011, 67 s.1-8.

Siber savaş, savunan açısından dijital ağlar ve altyapılar arasında yüksek seviyede birbirine bağımlılık ve saldırgan açısından da teknolojik yeterlilik gerektirdiğinden NATO, siber savaşa göre doktrinini değiştirmiş ve konunun teknik ve hukuki boyutunu tartışmak üzere çalışmalarına başlamıştır.

11 Eylül’den bir yıl sonra NATO, Kasım 2002’de kabul edilen “*Prag Yetenek Taahhütleri*”nin bir parçası olarak yeteneklerin siber saldırılara karşı koruyabilecek şekilde geliştirilmesi konusunda önemli bir çağrıda bulunmuş, 2002’den sonraki yıllarda İttifak öncelikli olarak askeri kanadın talep ettiği pasif koruma önlemlerinin uygulanması üzerinde odaklanmıştır.³⁵

2007 ilkbaharında Estonya’nın maruz kaldığı siber saldırı ise hazırlık boyutunu farklı bir seviyeye taşımıştır.³⁶ Tarihinde ilk defa İttifak, siber uzay politikasının üç temel ayağını belirleyen resmi bir “*NATO Siber Savunma Politikası*” hazırlamış ve Ocak 2008’de kabul etmiştir.³⁷

2010 yılındaki Lizbon zirvesinde ise siber savunmanın sürekli olarak NATO gündeminde bulunması yönünde temel bir karar alınmıştır.³⁸ Haziran 2011 tarihinde NATO Savunma Bakanları gözden

³⁵ Theiler, a.g.m.

³⁶ Rusya, İkinci Dünya Savaşında Estonya’da Estonya’nın Nazi istilasından korunması için verilen mücadeleyi simgeleyen bir heykel dikmiştir. Bu heykel 26 Nisan 2007 tarihinde Estonya tarafından yerinden kaldırılmıştır. Daha sonraki günlerde daha organize bir şekilde gerçekleştirilen ve Rus Hackerlar tarafından yapıldığından şüphelenilen saldırılar sonucu ülkenin ulusal bilgi sistemleri, internet hizmet sağlayıcıları ve bankaları çok büyük zarar görmüştür. Ülkenin internet sistemi çökme tehlikesiyle karşı karşıya gelmiştir. Estonya’nın 1,3 milyon olan nüfusunun 1 milyondan fazlası sayısal kimliğe sahiptir. Nüfusunun %66’sının internet kullanıcısıdır. Evlerin %55’inde internet bağlantısı vardır ve vergi beyanlarının %80’i internet üzerinden yapılmaktadır. Bankacılık işlemlerinin %97’sinin çevrim içi olarak gerçekleştirildiği, sağlık kayıtlarının tamamının sayısal ortamda tutulduğu da göz önünde bulundurulduğunda Estonya’ya verilen zararın boyutları tahmin edilebilecektir. Emre Bakır, “*İnternet Güvenliğinin Tarihçesi*”, TUBİTAK Bilgem Dergisi, 2011, Cilt 3, Sayı 5, s.16.

³⁷ Estonya’nın maruz kaldığı saldırı örneğinden sonra NATO’nun 2008 Bükreş Zirvesi’nde siber saldırılar ve kritik altyapıların güvenliği gibi bazı sorunlara çözüm arayışları konusu gündeme gelmiş, siber savunmada işbirliği için birimlerin kurulması kararı alınmıştır. Bu karar neticesinde Savunma Yönetim Otoritesi ile Siber Savunma Mükemmeliyet Merkezi kurulmuştur. NATO Cooperative Cyber Defence Centre of Excellence Tallinn, Estonia, <http://www.ccdcoe.org/>, erişim tarihi: 12.11.2012

³⁸ http://www.nato.int/nato_static/assets/pdf/pdf_publications/20120207_strategic-concept-2010-tur.pdf, erişim tarihi: 3.11.2012.

geçirilmiş NATO Siber Savunma Politikasını kabul etmişlerdir. Bu politika, siber savunma konusunda gerçekleştirilecek olan topluluk bazındaki çabaları içermektedir. Ekim 2011'de Bakanlar tarafından, Siber Savunma Eylem Planı'nın detayları üzerinde görüş birliğine varılmıştır. Siber Savunma Politikası'nda siber tehditler, yeni Stratejik Kavram doğrultusunda 5. maddede ifade edilen toplu savunma görevini yerine getirmesi için potansiyel kaynak olarak tanımlanmaktadır. Şubat 2012'de NATO Bilgisayar Olayları Karşılama Kapasitesi'nin (NATO Cyber Incident Response Capability - NCIRC) 2012 yılı sonunda tamamen operasyonel hale gelebilmesi için 58 milyon Avroluk bir kontrat imzalanmıştır. Ayrıca, bunun yanında istihbarat paylaşımı ve durumsal farkındalık için bir Siber Tehdit Farkındalık Birimi vücuda getirilmiştir.³⁹

2012 Chicago Zirvesi Sonuç Bildirisi'nde de sürekli gelişen ve karmaşıklaşan siber tehditlerle etkin biçimde ve işbirliği içinde mücadele edilmesi gerektiği vurgulanmıştır.⁴⁰

NATO siber güvenlik konusunda önemli mesafe almış olmakla birlikte, konuyla ilgili temel sorun ortak savunma koşulunu kapsayan 5. maddenin siber saldırıyı kapsayıp kapsamayacağıdır. Yani üye ülkelerden birinin silahlı saldırı yerine siber saldırıya uğraması halinde, anlaşmanın bu maddesinin geçerli olup olmayacağı, saldıran ülkenin en kısa sürede nasıl ortaya çıkarılacağı ve bu ülkeye nasıl karşılık verileceği halen belirsizliğini korumaktadır.⁴¹

³⁹ http://www.nato.int/cps/en/natolive/events_78665.htm?selectedLocale=en, erişim tarihi:3.11.2012

⁴⁰ http://www.nato.int/cps/en/SID-D71112AD-6BB73526/natolive/events_84074.htm, erişim Tarihi: 3.11.2012.

⁴¹ Washington'da 4 Nisan 1949 tarihinde imzalan NATO Anlaşması'nın 5. Maddesi; "Taraflar, Avrupa veya Kuzey Amerika'daki üyelerinden biri ya da daha fazlasına karşı silahlı bir saldırıyı, anlaşma taraflarının tümüne yapılmış sayacakları konusunda mutabık kalmışlar ve sonuç olarak ta böyle bir silahlı saldırı gerçekleştiği taktirde, taraf devletlerin her biri, BM Şartının 51. maddesinde belirtilen toplu veya bireysel savunma hakkının kullanılmasında saldırının muhatabı olan taraf ya da taraflara derhal karşı saldırı konumuna geçerek yardım edecek, ve diğer taraflarla iş birliği içersinde silahlı güç kullanımı, Kuzey Atlantik Bölgesinin güvenliğinin devamının sağlanması da dahil olmak üzere gerekli görülen eylemleri düzenleyeceklerdir..." şeklindedir. <http://translate.google.com/translate?hl=tr&langpair=en%7Ctr&u=http://www.nato.int/docu/basics.htm&ei=I86dULifEtK80AHP-oHYAw>, erişim tarihi:11.11.2012.

Diğer uluslararası örgütler ve devletler de buna ilişkin hazırlıklar yapmakta ve ordularını siber savaşa karşı teşkilatlandırmaktadırlar. Uluslararası ortamda da silahlı çatışma hukuku kuralları ve savaş hukukuna ilişkin uluslararası hukuk kurallarının siber savaşta uygulanıp uygulanamayacağı tartışılmaktadır.

Siber alanda meydana gelen ve bazıları siber savaş olarak tanımlanan saldırı ve savunma olaylarından aşağıdaki şekilde sonuçlar çıkarılmıştır:⁴²

- Siber alanda şimdiye kadar gerçekleşen vakalar göstermiştir ki; siber savaş gerçektir ve şimdiye kadar ilkel siber silahlar kullanılmış olup taraflar gerçek yeteneklerini ve silahlarını devreye sokmamışlardır. Bunun nedeni, tarafların ellerinde bulundurdıkları yetenekleri henüz göstermek istememeleridir. ABD ve diğer tarafların sahip oldukları gerçek yetenekler kullanıldığında bu saldırıların bir ulusun sonunu getirebileceği konusunda yorumlar yapılmaktadır.
- Siber savaşta, saldırı zamanı ile bu saldırının karşı tarafta yaratacağı etki neredeyse aynı anda gerçekleşmektedir. Bu durum aynı zamanda kriz yöneticilerinin karar alma süreçlerini ve ellerinde bulundurdıkları zamanı önemli ölçüde zora sokmaktadır.
- Siber ortamın yapısı ve kullanılan tekniklerin karmaşıklığı, herhangi bir siber anlaşmazlık durumunun kolaylıkla küresel hale gelebileceğini ve birçok devleti bu savaşın içersine çekeceğini göstermektedir.
- Bankalardan savunma radarlarına kadar insanların ihtiyaç duyduğu ve güvendiği sistemler siber ortamdan erişilebilir durumdadır ve bu sistemler hiç kullanılmaya fırsat verilmeden devre dışı bırakılabilmekte ya da kullanılamaz hale getirilebilmektedir.

Siber savaşın tanımlanması konusunda problem oluşturan konulardan en başta geleni savaş konusu sayılabilecek saldırıların neler olduğu ve saldırı kaynağının tespittir.⁴³ Siber ortamda, iz sürmenin zor

⁴² Richard A. Clarke, Robert K. Knake. *Cyber War : The Next Threat to National Security and What to do About It* (1. Baskı), New York, 2010, s.5,83,93.

⁴³ Alexander Klimburg. "Building Confidence in Cyberspace", *Cyber Security, New Europe* (Special Edition), Sayı: Mayıs-Haziran 2011, <http://www.scribd.com/>

olması nedeniyle, gerçekten saldırı kaynağı olan devlet, bunu kolaylıkla reddedebilirken aynı zamanda devlet dışı aktörleri de bu saldırılarda aracı olarak kullanabilmektedir.

Başka bir zorluk ise, “*kazara savaş*” tır. Gerçek saldırı kaynağı, saldırıyı bir devlet üzerinden sistemli yapılan bir saldırı gibi gösterip gerçek problemlere sebep olabilmektedir.

Siber alandaki her saldırı veya kötü niyetli faaliyet siber savaşın kapsamına girmemektedir. Siber savaşı tanımlarken, siber ortamda en çok kullanılan ve bazen karıştırılan terimleri de açıklamak konunun daha iyi kavranması için faydalıdır. Bu nedenle, siber uzayda gerçekleştirilen kötü niyetli siber hareketlerden olan siber suç, siber casusluk ve siber terörizm terimlerinin ne anlama geldiğini açıklamanın siber savaş teriminin farkını kavramak açısından önemli olduğu değerlendirilmektedir.

3. “Siber Suç”, “Siber Casusluk” ve “Siber Terörizm” Kavramları

a. Siber Suç

Siber suç teriminin kullanımı, siber saldırı ve siber savaş teriminden daha eskiye dayanmaktadır. Siber suç terimi uluslararası belgelerde yer almasına rağmen hangi eylemlerin siber suç olarak kabul edileceği açıkça belirtilmemiştir.⁴⁴ Çoğunlukla, siber suç denildiğinde bilgisayar ve iletişim sistemleri kullanılarak işlenen yasadışı fiiller anlaşılmaktadır. Siber suçun tipik tanımını, bilgisayar veya bilgisayar ağları ve donanımları kullanılarak işlenen suç şeklinde yapmak mümkündür.⁴⁵ Fakat, literatürde net bir tanım üzerinde fikir birliğine varılamamış ve hangi fiillerin suç siber suç kapsamına girdiği açıkça sayılmamıştır.

Literatürdeki birçok tanıma karşın; herhangi bir suçun siber uzay içinde işlenebilme imkânı bulunuyor ve bu ortam içersinde gerçekleş-

doc/56702531/Cyber-Security-2011, erişim tarihi:10.11.2012.
⁴⁴ Sarah Gordon, Richard Ford, “On the Definition and Classification of Cybercrime”, *J. Computer Virology*, no:1, 2006, s.13; Sylvia Mercado Kierkegaard, “International Cybercrime Convention”, <http://www.igi-global.com/viewtitlesample.aspx?id=7486> Erişim Tarihi:2.11.2011; Debra Littlejohn Shinder, *Scene of the Cybercrime: Computer Forensic Handbook*, Ed Tittel, Syngress Publishing Inc., 2002, s.16..
⁴⁵ Gordon, Ford, a.g.e., s.14.

tirilen fiil hukuka aykırı veya suç olarak tanımlanabiliyorsa, bu suç “siber suç” olarak tanımlanabilmektedir.

“Bilgisayar suçu” terimi bazı zamanlar “siber suç” teriminin yerine kullanılsa da, “siber suç” denildiğinde bilgisayarı da kapsayan ancak sadece bilgisayarlarla kısıtlı olmayıp siber alandaki bütün cihaz, araç ve sistemlere karşı veya bunlar marifetiyle işlenen suçlar kastedilmektedir. Türkiye’de “siber suç” terimi yerine daha çok “bilgişim suçu” terimi kullanılmaktadır.

Avrupa Konseyi Sibera suç Sözleşmesinde de siber suç tanımı yapılmış değildir. Sözleşmede siber suçlar; yetkisiz erişim, sisteme ve veriye müdahale, bilgişim sistemi aracılığıyla sahtekârlık ya da dolandırıcılık suçları ile sınırlı tutulmamaktadır. Söz konusu suçlar, bilgişim sistemlerinin ceza hukukuna etkisi bakımından belirli dönemlerde ortaya çıkan niceliksel ve niteliksel etkilere bir tepki olarak gündeme gelmiştir. Siber suçların, sadece bilgisayar ve veriye yönelik fiilleri esas almadığı bilgişim sistemlerinin kullanılmasıyla ve özellikle internetin yaygınlaşması ile birlikte niceliksel olarak ortaya çıkan sorunları da kapsadığı görülmektedir.⁴⁶ Bu açıdan çocuk pornografisi, telif haklarına ilişkin ihlaller ve son olarak Sözleşmeye yapılan ek protokolle kapsama alınan, yabancı düşmanlığının ve ırkçılığın önlenmesine ilişkin hükümler de siber suç kapsamındadır.⁴⁷ Sözleşmede bu suçların minimum bir uzlaşmayı temsil ettiği ve taraf devletlerin kendi mevzuatlarında başka suçları da düzenleyebilecekleri belirtilmiştir.

Siber suç fiilleri bir asayiş olayı olup, kişi, grup veya organizasyonlar tarafından farklı saiklerle işlenebilir. Ancak, siber savaş nedeni olabilecek fiiller, aleyhine işlenen devletin hukukunda suç olsun veya olmasın, devletin güvenliğine ve siyasal yararlarına, siber ortamda veya fiziksel ortamda ciddi zararlar veren eylemlerdir.

⁴⁶ Muammer Ketizmen, *Türk Ceza Hukukunda Bilgişim Suçları*, Ankara Üniversitesi Sosyal Bilimler Enstitüsü Kamu Hukuku Anabilim Dalı Doktora Tezi, Ankara, 2006, s.61.

⁴⁷ Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems, Strasbourg, 28.1.2003, <http://conventions.coe.int/Treaty/en/Treaties/Html/189.htm>, erişim tarihi:16.11.2012.

b. Siber Casusluk

Casusluk, çok eski çağlardan beri varlığını koruyan, tarihi gelişimi içinde giderek kurumsallaşıp uzmanlaşmış son derece teknik ve kendine özgü şartları olan bir meslektir. Devlet güvenliğine karşı işlenen suçların en önemli, en tehlikeli ve en eskilerinden biri casusluk suçudur. Devletlerin müstakil siyasi yapısının oluşumu harp sanatı kadar eskidir. Casusluk, tarihe bakıldığında savaşta başarı vasıtalarından biri olarak anlaşılmış ve bu gayeye hizmet için her zaman kullanılmıştır.

Casusluk, düşman menfaatine gözetlemek, gizli şeyleri bulmak ve sağlamak için araştırmalar yapmak ve gerektiğinde istenilen yere ulaştırmaktır.⁴⁸ Nitekim batı dillerinde⁴⁹ casusluk, gözetlemek anlamına gelen “*spigare*”, “*epier*” fiilinden alınmış bir kelimedir.⁵⁰

1889 Lahey Antlaşması’nın 29. maddesinde casus; “*gizlice veya sahte kimlikle, muharip bir devletin harekât sahasında bilgi elde eden veya etmeye çalışan kimse*” olarak tanımlanırken,⁵¹ 1907 Lahey Konferansı’nda casus; “*gizli bir surette veya sahte bahanelerle hareket ederek hasım tarafa bildirmek üzere muhariplerden birinin hareket mıntıkası hakkında malumat alan veya almaya çalışan kimsedir*” şeklinde tanımlanmıştır.⁵² Bu tarifler, daha çok savaş zamanında yapılan askerî casusluğa ait olup, konunun muhtelif şekillerini kapsayacak bir kapsam taşımamakta, mesela barış

⁴⁸ Askerî Yargıtay 3. Dairesinin 25.1.1972 gün ve 1972/5-21 E.K. sayılı kararı. (Askerî Yargıtay Kütüphanesi 3. Daire 1972 yılı kararlar klasörü); Askerî Yargıtay 3. Dairesinin 21.3.1972 gün ve 1972/93-102 E.K. sayılı kararı. (Askerî Yargıtay Kütüphanesi 3. Daire 1972 yılı kararlar klasörü); Casus ve casusluğun Arapça bir kökene sahip olduğu görülür. “*Câsûs*”, Arapça bir isim olarak anlamı, “*çaşıt*” (*Türk Dil Kurumu Türkçe Sözlük*, 10. Baskı, 4. Akşam Sanat Okulu Matbaası, Ankara, 2005, s.399); “*hafiye*”; “*gizli haberler öğrenerek veya sırları çözerek haber veren*”; “*düşmanın askerliğe dair haberlerini öğrenip bildiren kimse*” dir. (Ferit Develioğlu, *Osmanlıca-Türkçe Ansiklopedik Lûgat*, 24. Baskı, Aydın Kitabevi, Ankara, 2007, s.20).

⁴⁹ Casusluk: Fransızca Espionage; İngilizce Espionage; Almanca Spionage; İtalyanca Spionaggio; İspanya Espionaje; Rusça Şpionstvo; bunların kökü İtalyanca spia (casus) kelimesinin abartılı şekli olan “*spione*” kelimesinden gelmektedir. “*spiare*” (Eski Fransızca “*ipier*”, Modern Fransızca “*ipier*”) gizli bakmak; Hind-Avrupa kökü “*spek*”, tetkik etmek; Latince “*specere*”, görmek; Yunanca “*skeptesthein*”, gizli bakmak. *Türk Ansiklopedisi*, Cilt 9, Maarif Basımevi, Ankara, 1958, s. 490.

⁵⁰ Abdullah P. Gözübüyük, *Alman, Fransız, İsviçre ve İtalyan Ceza Kanunlarıyla Mukayeseli Türk Ceza Kanunu Açıklaması*, Cilt 1, 3. Baskı, Kazancı Yayınevi, Ankara, s. 509.

⁵¹ *Türk Ansiklopedisi*, s. 490.

⁵² Atıf Akgüç, “*Casusluk Suçu*”, *Siyasi İlimler Mecmuası*, Yıl 10, Sayı 118, 1941, s. 478.

zamanında yapılan askerî (plan, v.b.), siyasi (belge, haber, gizli anlaşma, v.b.), iktisadi (mali, ticari, iktisadi durum, v.b.), ilmi (atom sırrı, gizli silâh, keşif, v.b.) casusluk bu tariflere girmemektedir.

5237 sayılı TCK'nın "Devlet sırlarına karşı suçlar ve casusluk" başlığı altındaki suçlara bakıldığında çıkarılan casus tanımı; "devletin güvenliği veya iç veya dış siyasal yararları bakımından, niteliği itibarıyla, gizli kalması gereken bilgileri veya yetkili makamların kanun ve düzenleyici işlemlere göre açıklanmasını yasakladığı ve niteliği bakımından gizli kalması gereken bilgileri siyasal veya askerî casusluk maksadıyla temin etmek veya açıklamak" şeklindedir.⁵³

Teknolojinin büyük bir hızla geliştiği günümüzde yeni buluşlar yapılmakta ve bu buluşlar öncelikle ülkelerin güvenliği ya da menfaatleri için kullanılmaktadır. Yeni gelişen teknolojinin, egemenlik ve bağımsızlığı doğrudan etkilediği, dünyada gücü belirleyen en önemli unsur haline geldiği çağımızda, teknolojik ve ekonomik istihbarat çok daha önemli duruma gelmiştir. Casusluk faaliyetlerinin geçmişte sadece askerî ve siyasi alanlara yöneldiği, bugünün dünyasında ise telekomünikasyondan bilgisayar teknolojisine, genetikten havacılık endüstrisine, lazer teknolojisinden optik alanındaki araştırmalara kadar her alanda etkisini hissettirdiği ortadadır.⁵⁴

Teknolojik gelişmeler bilgiyi depolamayı ve korumayı kolaylaştırırken aynı zamanda casusluk faaliyetlerini de kolaylaştırmaktadır. Günlük yaşamın internet ile iç içe geçtiği günümüzde, internet üzerinden şahısların ve küçük ölçekli şirketlerin kimlik bilgilerinin, kul-

⁵³ Askerî Yargıtay Daireler Kurulunun 02.10.1997 gün ve 1997/98-114 E.K. sayılı kararında casusluk şöyle tarif edilmektedir: "Casusluk, sözlük anlamıyla; gözetlemek amacıyla düşman içine sızmak, yabancı bir devletle ilgili sırları öğrenmeye çalışmaktır. Hukuki kavram olarak casusluk; bir devlet menfaatine bir başka devletin askerî, siyasi ve iktisadi durumuna ilişkin gizli bilgilerin veya belgelerin araştırılması, sağlanması ve yabancı devlete ulaştırılmasıdır. Dolayısıyla casusluk, casus ile casusluğu talep eden arasında, talep edilen kimsenin devleti için "sır" niteliği taşıyan bilgi ve belgelerin karşı tarafa aktarılmasına yönelik bir anlaşmanın bulunmasını gerekli kılar." Askerî Yargıtay Kütüphanesi Daireler Kurulu 1997 yılı kararlar klasörü.

⁵⁴ "Titan Rain", 2002 yılında başlayan ve ABD Savunma Bakanlığı'nı hedef alan ve Çin tarafından gerçekleştirildiği belirtilen siber casusluk vakalarına verilen gayri resmi isimdir. Bu saldırılarda Çinliler tarafından NIPRNet sunucularından 10-20 terabayt veri indirildiği düşünülmektedir. Bu faaliyetlerin sonrasında gerçekleşmiş olan vakalar da bu isimle anılmaya devam edilmiştir. Jeffrey Carr, Lewis Shepherd, *Inside Cyber Warfare* 1. Baskı, Sebastopol, Calif., O'Reilly Media, Inc., 2010, s.4.

lanıcı hesaplarının ele geçirilmesi artık çok sık yaşanan vakalar haline gelmiştir. Özellikle, kendilerini zararsız, faydalı programcılar olarak gösterip gerçekten de bu şekilde işlev gören ancak içlerine kullanıcı faaliyetlerini kaydeden programcılara gizlenen yazılımlar bu maksat için kullanılan en yaygın yöntemdir.

Bu kapsamda siber casusluk, bir ülkenin, kurumun, organizasyonun ya da kişinin hassas bilgilerini, siber ortamı araç olarak kullanıp gizlice ele geçirmektir. Bu eylem, bireysel veya kolektif olarak parasal kazanç elde etmek veya çıkar sağlamak saiki ile yapılıyor olabilir. Bir devlet tarafından organize olarak başka bir devlete zarar vermek saikiyle icra edilen siber casusluk faaliyetleri siber savaşın nedeni olabileceği değerlendirilmektedir.

Teknoloji lideri ülkeler, özellikle teknolojik alandaki yeni buluş ve gelişmeleri askeri teknolojilerine uyarlamaktadır. Siber casusluk faaliyetlerinin hedefi de günümüzde devlete ilişkin sırların yanında endüstriyel sırlar da olmaktadır. Büyük emek, mesai ve kaynak harcanarak yapılan buluşların gizlenmesi ve yanlış kişilerin eline geçmesi veya kullanılmaması devlet güvenliği için büyük önem arz ettiği kadar şirketlerin başarısı ve bekası içinde önem arz etmektedir.

Değişik casusluk türleri, bin yıllardır görülüyor olsa da artan küresel rekabet, bilgi teknolojilerinde yaşanan gelişmeler ve küçük fakat çok yüksek kapasitelere sahip depolama cihazlarının ortaya çıkması siber casusluk faaliyetlerinin yaratmış olduğu tehlikeyi ciddi anlamda artırmıştır.⁵⁵

c. Siber Terörizm

Sözlük anlamı olarak terör, “*korkutma, yıldırma*”, terörizm ise “*yıldırıcılık*” anlamına gelmektedir.⁵⁶ Terörizm, uluslararası ve ulusal güvenlik ortamını ciddi derecede tehdit eden bir olgu olarak yoğun incelemelere konu olmaktadır. Terörizm konusunda uluslararası alanda halen ortak bir anlayışa bağlı olarak tek bir tanım geliştirilememiş

⁵⁵ 2006 yılında İnternet sitesi ismini kaydettiren ve 2007 yılı Ocak ayında, elinde yayınlanmak üzere 1,2 milyon doküman olduğunu bildiren Wikileaks dünya üzerinde çok ses getirmiş bir sitedir. Birçok ülkeye ait gizli belgeleri bu tarihten itibaren yayınlamaya başlamıştır ve büyük yankı uyandırmıştır. Bu siber casusluğa ilişkin en çarpıcı örneklerden birisidir.

⁵⁶ Türk Dil Kurumu Büyük Türkçe Sözlük, <http://tdkterim.gov.tr/bts/>, erişim tarihi:30.10.2012

olması önemli bir eksiklik olarak karşımıza çıkmaktadır. Doktrinsel tartışmada, terörizm ile “*yabancı işgaline karşı*” ve “*kendi kaderini tayin amaçlı meşru mücadele*” arasında bir ayrıma gidilmesi hususunda mutabakat yoktur. Ülkelerin yaklaşımındaki farklılıklar tanımı zorlaştıran en önemli etkenlerin başında gelmektedir.⁵⁷

Her devlet, terörizmin tanımını, kendi siyasi bakış açısına göre değerlendirmektedir.⁵⁸ Buna göre her devlet, uluslararası terör eylemlerini tanımlarken, kendisini hedef alan eylemleri içine alacak şekilde ve halen gelen veya gelebilecek iç ve dış düşmanlarının olası eylemlerini, uluslararası hukuka göre hukuk dışı saymak istemektedirler. Bunun yanında her devlet, herhangi bir biçimde egemenliklerini olumsuz yönde etkiyebilecek tanımlardan uzak durmaya çalışmaktadır. Netice olarak, bir devlet tarafından terörist olarak nitelendirilen kişi veya kişiler, diğer bir devlet tarafında da “*özgürlük savaşçısı*” olarak nitelendirilmektedir.⁵⁹ Bu nedenle siber terörizmin tek bir tanımının kabul edilmesi de beklenmemelidir.

Siber terörizm, terörist faaliyetlerin siber alan kullanılarak gerçekleştirilmesi olarak ya da terör örgütlerinin siber alanı araç olarak kullanmaları olarak tanımlanabilir.⁶⁰

Başka bir tanıma göre de siber terörizm, siber alan ve terörizmin bir araya gelmesidir. Politik veya sosyal hedeflerin gerçekleştirilmesi için bir devleti veya vatandaşlarını aşağılamak veya korkutmak üzere bilgisayarlara, ağlara veya bilgilerin depolandığı yerlere gerçekleştirilen kanunsuz saldırı veya saldırı tehditlerine siber terörizm denir.⁶¹

⁵⁷ Dışişleri Bakanlığı Resmi İnternet sitesi, “*Terörizmle Mücadelede Uluslararası İşbirliği ve Tanım Sorunu*”, http://www.mfa.gov.tr/terorizmle-mucadelede-uluslararası-isbirligi_-ve-tanim-sorunu_.tr.mfa, erişim tarihi: 12.11.2012.

⁵⁸ Türk Hukukunda Terör, 3713 sayılı Terörle Mücadele Kanunu’nun 1. maddesinde, “*cebir ve şiddet kullanarak; baskı, korkutma, yıldırma, sindirme veya tehdit yöntemlerinden biriyle, Anayasada belirtilen Cumhuriyetin niteliklerini, siyasi, hukuki, sosyal, laik, ekonomik düzeni değiştirmek, Devletin ülkesi ve milletiyle bölünmez bütünlüğünü bozmak, Türk Devletin ve Cumhuriyetin varlığını tehlikeye düşürmek, Devlet otoritesini zaafa uğratmak veya yıkmak veya ele geçirmek, temel hak ve hürriyetleri yok etmek, Devletin iç ve dış güvenliğini, kamu düzenini veya genel sağlığı bozmak amacıyla bir örgüte mensup kişi veya kişiler tarafından girişilecek her türlü suç teşkil eden eylemlerdir*” şeklinde tanımlanmıştır.

⁵⁹ Çitlioglu, Ercan. *Gri Tehdit Terörizm*, (1. Baskı), Ankara, Destek Yayınları, 2008, s.17.

⁶⁰ Serge Krasavin, “*What is Cyber Terrorism?*”, <http://www.crime-research.org/library/Cyber-terrorism.htm>, Erişim Tarihi:4.11.2012.

⁶¹ Dorothy E. Denning, “*Cyberterrorism*”, <http://www.cs.georgetown.edu/~den>

Bu iki tanım bir araya getirildiğinde siber terörizm, bilgisayar ve iletişim teknolojisi kabiliyetlerinin politik olarak motive olmuş ulus-altı gruplar veya gizli ajanlar tarafından şiddet, bir toplumu etkilemek veya bir hükümetin politikalarını değiştirmek maksatlı olarak silah veya hedef olarak kullanılması şeklinde tanımlanabilir.⁶² Siber terörizmi ircaa eden ulus-altı gruplar iken siber savaşı icra eden kişi grup veya organizasyonların bir devlet tarafından yönlendirilmesidir. Sorun, siber savaş nedeni sayılabilecek saldırının gerisindeki saldırgan devleti tespit edebilmektir.

III. Sonuç

Hukukun vazgeçilmez aracı dil olduğundan, siber savaş gibi teknolojik gelişmelere bağlı olarak anlamı değişen ve gün geçtikçe hukukçular için daha çok önem teşkil edecek bir terimi açıklama ihtiyacı vardır. Tabii, pek çok ülkenin hukukunda olduğu gibi Türk Hukuku’na yeni giren terimlerin gelişmelerden ilham alınarak yaratıldığı göz ardı edilmeyerek, yabancı diller bilimsel incelemelere dâhil edilmelidir. Hukuk alanındaki çalışmalara derinlik kazandıran, resmin tamamını görmeyi sağlayan bu yaklaşım hukukun dilbilgisiyle bağını sağlamlaştırmaktadır.

Siber savaş, bilimsel eserlerde artık yaygın şekilde kullanılmaya başladığından bu çalışmada, siber savaş bir hukuk terimi olarak incelenmiştir. Silahlı çatışma hukuku kuralları ve savaş hukukuna ilişkin uluslararası hukuk kurallarının siber savaşta uygulanıp uygulanamayacağı başka bir çalışmanın konusu olacaktır.

Yakın bir gelecekte siber silahlarla gerçekleştirilebilecek saldırıların, sonuçları açısından klasik savaşları aratmayacağı ve elektrik santrallerinin devre dışı bırakılması, nükleer santrallerin kontrollerinin ele geçirilerek potansiyel birer atom bombasına dönüştürülmesi, basıncın artırılarak doğal gaz borularının havaya uçurulması, baraj kapakları açtırılarak şehirlerin sular altında bırakılması, iletişim ağlarının devre dışı bırakılmasıyla haberleşmenin sekteye uğratılması ve hava, kara ve deniz trafiğinin aksatılması gibi sonuçlar doğuracağı beklenmektedir.

ning/infosec/ cyberterror-GD.doc, Erişim Tarihi:07.11.2012.
⁶² Jason Andress, Steve Winterfeld, *Cyber Warfare*, Elsevier, 2011, s. 198.

Uluslararası hukuku önümüzdeki günlerde daha fazla meşgul edecek olan siber savaş konusunda, hukukçuların da konuya eğilmesi ve gelişmeleri takip ederek Türkiye özelinde yapılması gereken düzenlemeleri tartışmaya açmaları faydalı olacaktır.

KAYNAKLAR

- Abdullah P. Gözübüyük, *Alman, Fransız, İsviçre ve İtalyan Ceza Kanunlarıyla Mukayeseli Türk Ceza Kanunu Açıklaması*, Cilt 1, 3. Baskı, Kazancı Yayınevi, Ankara, 1960.
- Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems*, Strasbourg, 28.1.2003, <http://conventions.coe.int/Treaty/en/Treaties/Html/189.htm>, erişim tarihi:16.11.2012.
- Alexander Klimburg, *"Building Confidence in Cyberspace"*, Cyber Security, New Europe (Special Edition), Sayı: Mayıs-Haziran 2011, <http://www.scribd.com/doc/56702531/Cyber-Security-2011>, erişim tarihi:10.11.2012.
- Atıf Akgüç, *"Casusluk Suçu"*, *Siyasi İlimler Mecmuası*, Yıl 10, Sayı 118, 1941, s. 477-484.
- Brian Krebs, *"Obama: Cyber Security is a National Security Priority"*, *Washington Post*, 29.5.2009, <http://voices.washingtonpost.com/securityfix/2009/05/obama-cybersecurity-is-a-natio.html>, erişim tarihi: 7.11.2012.
- Cambridge Dictionaries Online, <http://dictionary.cambridge.org/dictionary/turkish/cyber?q=cyber>, <http://dictionary.cambridge.org/dictionary/turkish/war?q=war>, erişim tarihi: 12.11.2012.
- Ceyda Karaaslan, *"Siber Ordunun İlk Timleri Hazır"*, *Sabah Gazetesi*, 9.5.2011, <http://www.sabah.com.tr/Gundem/2011/05/09/siber-ordunun-ilk-timleri-hazir>, erişim Tarihi:9.11.2012
- Collins Dictionaries*, <http://www.collinsdictionary.com/dictionary/english/cyber-war>, erişim tarihi:11.11.2012.
- Cyber Space Operations* (US Air Force Doctrine Document 3-12, 15.6.2010), s.2, <http://www.e-publishing.af.mil/shared/media/epubs/AFDD3-12.pdf>, Erişim tarihi: 15.11.2012.
- Çitlioğlu, Ercan. *Gri Tehdit Terörizm*, (1. Baskı), Ankara, Destek Yayınları, 2008.
- Debra Littlejohn Shinder, *Scene of the Cybercrime: Computer Forensic Handbook*, Ed Tittel, Syngress Publishing Inc., 2002.
- Department of Defence Dictionary of Military and Associated Terms (Joint Publications 1-02)*, http://www.dtic.mil/doctrine/new_pubs/jp1_02.pdf, erişim tarihi: 30.10.2012.

- Dışişleri Bakanlığı Resmi İnternet Sitesi, "Terörizmle Mücadelede Uluslararası İşbirliği ve Tanım Sorunu", <http://www.mfa.gov.tr/terorizmle-mucadelede-uluslararasi-isbirligi-ve-tanim-sorunu-.tr.mfa>, Erişim tarihi: 12.11.2012.
- Donna MILES, "New Cyber Chief: People Key in Meeting Cyberspace Challenge", *The Official Website of U.S. Air Force*, <http://www.af.mil/news/story.asp?id=123207676>, erişim tarihi: 6.12.2011.
- Dorothy E. Denning, "Cyberterrorism", <http://www.cs.georgetown.edu/~denning/infosec/cyberterror-GD.doc>, erişim tarihi: 07.11.2012.
- Emre Bakır, "İnternet Güvenliğinin Tarihçesi", *TUBİTAK Bilgem Dergisi*, Yıl 2011, Cilt 3, Sayı 5, s.6-17.
- Elisabeth Bumiller, Thom Shanker, "Panetta Warns of Dire Threat of Cyberattack on U.S.", *The New York Times*, 11 Ekim 2012, <http://www.nytimes.com/2012/10/12/world/panetta-warns-of-dire-threat-of-cyberattack.html?pagewanted=all&r=0>, Erişim Tarihi: 3.11.2012.
- Ferit Develioğlu, *Osmanlıca-Türkçe Ansiklopedik Lûgat*, 24. Baskı, Aydın Kitabevi, Ankara, 2007.
- Free Dictionary, <http://www.thefreedictionary.com/cyberwar>, erişim tarihi: 11.11.2012.
- Faruk Y. Turinay, "Bir Kelime Olarak Anayasa'nın Tarihsel Yolculuğu Üzerine Düşünceler", *Türkiye Barolar Birliği Dergisi*, sayı 95, 2011, s.269-312.
- Funda Keskin, *Uluslararası Hukukta Kuvvet Kullanma: Savaş, Karışma ve Birleşmiş Milletler*, Ankara, Öteki Matbaası, 1998.
- Güney Nair, "Bilgi'nin Değişen Anlamı ve Kavram Tartışmaları", *C.Ü. İBF Dergisi Doç. Dr. Feramuz Aydoğan'ın Anısına*, s.329-337.
- http://www.nato.int/nato_static/assets/pdf/pdf_publications/20120207_strategic-concept-2010-tur.pdf, erişim tarihi: 3.11.2012.
- http://www.nato.int/cps/en/natolive/events_78665.htm?selectedLocale=en, erişim tarihi: 3.11.2012.
- http://www.nato.int/cps/en/SID-D71112AD-6BB73526/natolive/events_84074.htm, erişim tarihi: 3.11.2012.
- <http://translate.google.com/translate?hl=tr&langpair=en%7Ctr&u=http://www.nato.int/docu/basics.htm&ei=I86dULifEtK80AHP-oHYAw>, erişim tarihi: 11.11.2012.
- Jason Andress, Steve Winterfeld, *Cyber Warfare*, Elsevier, 2011.
- Jason Whittekar, *The Cyberspace Handbook*, Oxon, Routledge, 2004.
- Jeffrey Carr, Lewis Shepherd, *Inside Cyber Warfare* 1. Baskı, Sebastopol, Calif., O'Reilly Media, Inc., 2010.
- Joint Doctrine for Information Operations (Joint Pub 3-13)*, 9.10.1998. http://www.c4i.org/jp3_13.pdf, erişim tarihi: 2.11.2012.
- Macnillan Dictionary*, <http://www.macmillandictionary.com/dictionary/american/cyberwar>, erişim tarihi: 11.11.2012.
- Martin C. Libicki, *What is Information Warfare?*, National Defence University, Washington, 1995.

- Muammer Ketizmen, *Türk Ceza Hukukunda Bilişim Suçları*, Ankara Üniversitesi Sosyal Bilimler Enstitüsü Kamu Hukuku Anabilim Dalı Doktora Tezi, Ankara, 2006
- Nafi Kaşıkçıoğlu, “Elektronik Harp”, *Siber Savunma Sempozyumu*, Askeri Müze ve Kültür Sitesi Komutanlığı, Harbiye, İstanbul, 24-25 Mayıs 2011.
- Norbert Wiener, *Cybernetics: Or Control and Communication in the Animal and the Machine*. Paris, (Hermann & Cie) & Camb. Mass., 1948.
- Olaf Theiler, “Yeni Tehditler:Siber Boyut”, NATO Dergisi On Yıl Sonra Alınan Dersler, <http://www.nato.int/docu/review/2011/11-september/Cyber-Threads/TR/index.htm>, erişim tarihi: 3.11.2012.
- Oxford Dictionaries, http://oxforddictionaries.com/definition/american_english/cyberwar?region=us&q=cyber+war, erişim tarihi:11.11.2012.
- Resuhi Akdikmen, Langenscheidt Standart Sözlüğü, İnkılap Kitapevi, İstanbul, 1992.
- Rich Gibson, Schuyler Erle, *Google Maps Hack*, U.S.A., O'Reily Media Inc., 2006.
- Richard A. Clarke, Robert K. Knake. *Cyber War : The Next Threat to National Security and What to do About It* (1. Baskı), New York, 2010.
- Ronald Deibert, “Tracking the Emerging Arms Race in Cyberspace”, *Bulletin of the Atomic Scientists*, January/February 2011, 67 s.1-8.
- Ryan Singel, “White House Cyber Czar:‘There is no Cyber War’”, *Wired*, 3.4.2010, <http://www.wired.com/threatlevel/2010/03/schmidt-cyberwar/>, erişim tarihi: 10.11.2012.
- Sarah Gordon, Richard Ford, “On the Definition and Classification of Cybercrime”, *J. Computer Virology*, no:1, 2006, s.13-20.
- Seha L. Meray, *Devletler Hukukuna Giriş*, Ankara Üniversitesi Siyasal Bilgiler Fakültesi Yayınları, 1962.
- Serge Krasavin, “What is Cyber Terrorism?”, <http://www.crime-research.org/library/Cyber-terrorism.htm>, erişim tarihi:4.11.2012.
- Shane M. Coughlan, Is There a Common Understanding of What Constitutes Cyber Warfare?, (Yayımlanmamış Yüksek Lisans Tezi), The University of Birmingham 2003. <http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.102.1876&rep=rep1&type=pdf>, erişim tarihi: 15.05.2012.
- Shitanshu Mishra, “Network Centric Warfare in the Context of Operation Iraqi Freedom” *Strategic Analysis*, V.27, I.4, s.546-547. http://www.idsa.in/strategicanalysis/NetworkCentricWarfareintheContextofOperationIraqiFreedom_smishra_1003, erişim tarihi:5.11.2012.
- Sylvia Mercado Kierkegaard, “International Cybercrime Convention”, <http://www.igi-global.com/viewtitlesample.aspx?id=7486>, erişim tarihi:2.11.2011.
- Thomas C.Wingfield, *The Law of Information Conflict: National Security Law in Cyberspace*, Aegis Research Corp., 2000.
- Thomas Rid, “Cyber War Will Not Take Place In”, *Strategic Studies*, Volume 35, Issue 1, 2012, s.5-32.

Türk Ansiklopedisi, Cilt 9, Maarif Basımevi, Ankara, 1958.

Türk Dil Kurumu Büyük Türkçe Sözlük, <http://tdkterim.gov.tr/bts/>, erişim tarihi: 30.10.2012

Türk Dil Kurumu Türkçe Sözlük, 10. Baskı, 4. Akşam Sanat Okulu Matbaası, Ankara, 2005.

Türk Silahlı Kuvvetleri Bilgi Harbine Nasıl Hazırlanmalıdır?, Harp Akademileri Yayınları (Tasnif Dışı), İstanbul, 1999, s.1-14.

United Nations, UN Terms, <http://unterm.un.org/dgaacs/unterm.nsf/WebView/E996B25EA7D3B36E85256B090056D806?OpenDocument>, erişim tarihi: 31.10.2012.

US Department of Defence, US Cyber Command Fact Sheet, 25.5.2010, http://www.defense.gov/home/features/2010/0410_cybersec/docs/cyberfactsheet%20updated%20replaces%20may%2021%20fact%20sheet.pdf, erişim tarihi: 8.11.2012.

Yasin Aslan, “Savaş Hukukunun Temel Prensipleri”, *Türkiye Barolar Birliği Dergisi*, Sayı 79, 2008, s.235-274.

Yoram Dinstein, *War, Aggression and Self-Defence, Second Edition*, Grotius Publications, Cambridge: Cambridge University Press, 1995.

Vassilys Fourkas, What is cyberspace?, <http://www.waccglobal.org/en/20043-communication-rights-an-unfinished-agenda/495-What-is-cyberspace.html>, erişim tarihi:13.11.2012.