Siber Savaş ve Siber Ortamdaki Kötü Niyetli Hareketlerden Farkı

Hakemli Makale

Mehmet YAYLA
Dr., Askeri Yargıtay Başsavcı Yardımcısı (meh_yayla@yahoo.com)

ÖZET

Günümüzde, bilgisayar, iletişim araçları ve internet gibi bilgi teknolojilerinin neredeyse tüm organizasyonlar ve devletler tarafından önemli derecede kullanıldığı açıktır. Dünya, internet ve iletişim sistemlerine gitgide daha bağımlı hale gelirken yasal kurumların yanında yasadışı kurumlar, suç organizasyonları ve hatta devletlerde siber ortamı ve araçları kendi yararları için kullanmaktadırlar.

Teknoloji lideri ülkeler, ordularını siber savaş için hazırlamaktadırlar. Siber savaş ulusal güvenlik için en önemli tehditlerden biri olmuştur.

Siber ortamın sınıra sahip olmaması yargılama konularını önemli bir ilgi alanı yapmaktadır. Hukuk sistemi, bu yeni savaş alanına uyum sağlamaya çalışırken siber ortamdaki kötü niyetli diğer hareketler arasındaki fark da ortaya konmaya çalışılmaktadır. Bu makalede, siber savaş hukuki açıdan tartışılmış, siber savaşın siber ortamdaki kötü niyetli diğer hareketlerden farkının neler olduğu incelenmiştir.

Anahtar Kelimeler: Siber savaş, siber saldırı, siber suç, siber terörizm, siber casusluk.

ABSTRACT

Cyber War and its Differences From Malicious Acts in Cyber Space*

Today, it is considerably clear that information technologies, such as computers, telecommunication devices, and the internet have been used by almost all organizations and goverments. As the world has become more and more reliant on technology and networked systems, not only have legitimate entities benefited from this trend, but also illegal groups, criminal entities and even goverments have been using cyber space and tools for their own benefits.

Governments which are the leaders of technology has been equiping their armies for cyber war. Cyber war has been one of the most important threat against national security.

Cyber space, which has no border, makes jurisdictional issues an important area of concern. While the legal system is trying to adapt to this battleground, its differences from other malicious acts in cyber space are tried to express. In this article, "cyber war" has been discussed from the legal perspective and its differences from other malicious acts in cyber space has been examined.

Keywords
Cyber war, cyber attack, cyber crime, cyber terrorism, cyber espionage.

Giriş

Yeni geliştirilen teknolojinin ilk kullanıldığı alanlardan biri olan, bilginin ve hızlı karar almanın önem taşıdığı savaş ortamında bilgisayar ve iletişim teknolojileri yoğun olarak kullanılmaktadır. Günümüz savaş sahasında siber ortamın güvenliğini sağlamak, aynı zamanda bu alanı kullanarak düşmanın silah sistemlerini etkisiz hale getirmek için devletler önemli çalışmalar yürütmektedirler. Uluslararası ilişkilerde bilgisayar ve iletişim teknolojisini saldırı ve savunma amaçlı olarak kullanılması olarak tanımlanabilecek "siber savaş", günümüzde ulusal ve uluslararası güvenlik açısından en tartışılan kavramlardan biri haline gelmiştir. Savaşı önlemeyi amaçlayan veya savaş kurallarını düzenleyen hukuk kurallarının siber savaşa adapte edilmesine çalışılırken siber ortamdaki kötü niyetli hareketlerin benzeşen ve farklı yönleri de tartışılmaktadır.

Bu kapsamda çalışmanın ilk bölümünde, siber ortamın savaş hukuku açısından ortaya çıkardığı sorunlara değinilecek; ikinci bölümde siber tehdide karşı strateji geliştirme çabalarından örnekler verilerek siber ortamda silah kavramının neyi ifade ettiği üzerinde durulacak; üçüncü bölümde ise siber savaş, siber saldırı, siber suç siber casusluk ve siber terörizm arasındaki ilişki incelenecektir.

* Bu makale, 5. Uluslararası Terörizm ve Sınıraşan Suçlar Sempozyumuna (UTSAS 2013)'de sunulan sözlü bildirinin gözden geçirilmiş ve geliştirilmiş versiyonu olup, TUBİTAK tarafından sağlanan destek kapsamında 2012-2013 döneminde ABD The City University of New York John Jay College'da yürütülen çalışmalar kapsamında hazırlanmıştır. Makalede yayımlanan görüş ve düşünceler tamamen yazarın kişisel fikirlerini yansıtmakta olup, çalışma gizlilik dereceli doküman kullanılmadan açık kaynaklardan yararlanılarak yapılmıştır.

1. SİBER SAVAŞ VE HUKUK

Bilim dünyası, insanlık tarihi kadar eski olan savaşın sebepleri, niteliği ve kapsamı hususunda tam olarak görüş birliğine varmış değildir. Savaş kavramı, kural olarak devlet veya ulus içerisindeki rakip siyasal güçler arasında gerçekleşen, açık ve ilan edilmiş silahlı çatışmaları ifade etmek için kullanılmaktadır. Açıkça ilan edilmiş olsun veya olmasın, bütün savaşları düzenlemeyi amaçlayan savaş hukuku, savaşan ülkelerin birbirleriyle ve savaşa katılmayan ülkelerle olan ilişkilerini düzenlemekte, ayrıca bireylerin savaştaki hak ve sorumluluklarını belirtmektedir. Savaş hukukunun faydası, savaş sebebiyle yapılması gereken askeri eylemler ile insancıl gereklerin bağdaştırılmasına çalışılmasıdır. Savaş hukukunun amacı ise, savaşın sebep olduğu vahşeti olabildiğince en az düzeye indirmektir.[1]

Savaşı önlemeyi amaçlayan veya savaş kurallarını düzenleyen hukuk kurallarının, bilgisayar ve iletişim teknolojisi gelişmeden önce belirlenmiş olması nedeniyle, mevcut kuralların siber saldırılara uyarlanması konusunda yapılacak çalışmalar zor olmaktadır.

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 bir saldırı ile aynı sonucu doğuracağını ve konvansiyonel anlamda silahlı kuvvet kullanılmayacağını savunmaktadırlar[2]. Buna karşın, Estonya[3], Gürcistan[4] ve İran'a[5] karşı yapılan saldırılar siber savaşın

---

1 Savaşların bir kurala bağlanması gerektiği düşüncesi eski çağlardan bu yana mevcut olmakla birlikte, uluslararası hukukta bu konudaki ilk ciddi adımların on dokuzuncu yüzyılda atıldığı görülmektedir. Günümüz dünyasına hâkim olan kurallar ise İkinci Dünya Savaşı'ndan sonra belirlenmiştir. ASLAN, Yasin, "Savaş Hukukunun Temel Prensipleri", **Türkiye Barolar Birliği Dergisi**, 2008, Sayı 79, s.235,236.

2 RID, Thomas, "Cyber War will not Take Place in", **Strategic Studies**, 2012, V.35, I.1, s.5-32; SINGEL, Ryan, "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); DEIBERT, Ronald, "Tracking the Emerging Arms Race in Cyberspace", **Bulletin of the Atomic Scientists,** Ocak/Şubat 2011, s.1-8.

3 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. BAKIR, Emre, "İnternet Güvenliğinin Tarihçesi", **TUBİTAK Bilgem Dergisi**, 2011, Cilt 3, Sayı 5, s.16; TRAYNOR, Ian, "Russia Acccused of Unleashing Cyberwar to Disable Estonia", **The Guardian**, http://www.guardian.co.uk/world/2007/may/17/topstories3.russia (erişim tarihi 10.1.2013).

4 Rusya'nın 8 Ağustos 2008'de Gürcistan'a saldırısının ardından, Gürcistan'a ait internet sitelerine hizmet engelleme saldırıları düzenlenmiştir. Fiziki saldırılarla eş zamanlı olarak gerçekleştirilen siber saldırılar gerçek dünyada meydana gelen sorunların anında sanal dünyaya da yansıyabileceğini göstermektedir. GÜRKAYNAK, Muharrem / İREN, Adem Ali. "Reel Dünyada Sanal Açmaz: Siber Alanda Uluslararası İlişkiler", **Süleyman Demirel Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi**, Yıl 2011, Cilt 16, s.271, http://iibf.sdu.edu.tr/dergi/files/2011-2-13.pdf (erişim tarihi 28.02.2012).

5 İlk kez Haziran 2010'da ortaya çıkarılan Stuxnet isimli solucan Windows tabanlı işletim sistemleri üzerinde yayılmış olan bir endüstriyel virüstür. Kötü maksatlı yazılımların karşılaşılan en gelişmişi olan Stuxnet'in en belirgin özelliği, kendisini otomatik olarak kopyalayabilmesidir. İçerisine girdiği ağı işlevsiz hale getirene

ciddiyetini ortaya koymakta, uluslararası hukuk ve savaş hukuku açısından konu değerlendirilmekte, düşman devlet veya devlet güdümlü alt gruplar tarafından gerçekleştirilecek bir siber saldırı durumunda, saldırıya uğrayan devlet tarafından Birleşmiş Milletler (BM) Antlaşması'nın 51. maddesindeki "meşru müdafaa hakkı"nın kullanılabileceği savunulmaktadır.

Siber saldırılar, ekonomik, fiziksel yıkımlara sebep olmasının yanında, yaralanmalara, ölümlere ve büyük yıkımlara sebep olabilecek kabiliyetlere ulaşmıştır. Bir yandan teknolojinin ulaştığı imkânlar göz önüne alınarak siber saldırı senaryoları üretilip, devletler bu saldırılara karşı strateji geliştirme arayışına girmekte iken diğer yandan da hukuk dünyasında ortaya çıkması muhtemel sorunlar tartışılmaktadır.

Uluslararası çatışmaların doğasında meydana gelen iki önemli değişim; BM Antlaşması'nda öngörülmeyen önemli sorunlar ortaya çıkarmıştır. İlk değişim, teknolojinin ilerlemesi ile birlikte silah sistemlerinin ve silah kavramının değişmesidir. Nihayetinde BM Antlaşması, bilgi çağı öncesi bir belgedir ve siber uzayın imkân ve kabiliyetlerini öngörmemiştir. Bilgisayar ve iletişim teknolojisindeki gelişmeler, bazı hukuk kurallarında olduğu gibi BM Antlaşması'nı da çağ dışı olma tehlikesiyle kar**şı karşıya bırakmıştır.**

İkinci değişim, siber tehdidin farklılaşan doğası ve bunun uluslararası toplum tarafından algılanmasıdır. Siber tehdit, artık ülkesel çapta değerlendirilecek boyutu aşmış uluslararası tehdit oluşturmaktadır. Siber uzayın mekân tanımayan yapısı gereği, devlet dışı aktörler küresel öl**çekte örgütlenebilmekte, eşzamanlı olarak değişik ülkelere ya da organizasyonlara siber saldırılar gerçekleştirebilmek**tedir. Daha da önemlisi, bu saldırıların sonuçlarının artık fiziksel zararlara veya can kayıplarına ya da büyük yıkımlara sebep olabilecek imkân ve kabiliyetlere ulaşmasıdır.

Bu gelişmeler, siber saldırılarla etkin şekilde mücadele etmek için uluslararası antlaşmaların yeterli olup olmadığı sorusunu akla getirmektedir. Aynı zamanda, kavramsal düzeyde devlet merkezli bir hukuk olan uluslararası hukuk hakkındaki geleneksel yargılara da meydan okumaktadır. Diğer yandan devletler tarafından, kuvvet kullanılmasını sınırlandırmak için tasarlanmış BM sistemi, devlet dışı aktörler tarafından gerçekleştirilen kuvvet kullanma sorunuyla etkin şekilde ilgilenmede dikkate değer zorluklarla karşılaşmaktadır.

Bu bağlamda çözüm bekleyen başlıca önemli sorunlar arasında şunlar bulunmaktadır:

- Siber saldırıların silahlı kuvvet kullanma eşiğine gelmesi söz konusu olabilir mi? Bu eşiğin standartları nelerdir?
- Siber saldırılar, 51. madde kapsamında meşru müdafaa hakkının doğmasına yol açabilir mi?
- Devletler, silahlı saldırı seviyesine varmayan siber saldırılara karşı ne gibi yasal tedbirlere başvurulabilir?
- Devletlerin, başka bir devlet tarafından yönlendirilen siber saldırılara karşı kuvvet kullanması meselesine ilişkin olarak BM Antlaşması nasıl yorumlanmalıdır?

---

kadar çoğalıp, yayılabilmektedir. New York Times, BBC ve Guardian gibi gazeteler bu virüsün ABD veya İsrail tarafından İran hedef alınarak geliştirildiğini düşünmektedir. Çünkü Stuxnet'in zarar verdiği sistemlerin %60'ı İran'da yer alan bilgisayarlardır. GÜRKAYNAK / İREN, a.g.m., s.273.

- Devletlerin, devlet dışı aktörler tarafından yönlendirilen siber saldırılara karşı kuvvet kullanması meselesine ilişkin olarak BM Antlaşması nasıl yorumlanmalıdır?
- BM Antlaşması'nda öngörülen kolektif güvenlik sistemi, siber saldırıları ele almada başarısız mıdır?
- Siber saldırılara karşı kuvvet kullanma konusunda BM Antlaşması'nın etkin bir yorumuna ulaşmak için fiili devlet uygulamalarına veya stratejilerine mi bakılmalı mıdır?
- BM Antlaşması'nın devletler merkezli bir Antlaşma olduğu göz önünde bulundurulursa, siber saldırılarla ilgili sorunlara etkin şekilde yanıt vermek için kuvvet kullanma konusunda, uluslararası hukukun yeniden gözden geçirilmesi gerekli midir?
- Siber saldırı yapan devlet dışı aktörler, bir devletin siyasal bağımsızlığını ve ülkesel bütünlüğünü tehdit etmek amacıyla bir başka devlet tarafından desteklenebilir mi?

2. SİBER TEHDİT VE STRATEJİ GELİŞTİRME ÇABALARI

2.1. Genel

Uluslararası hukuk ve savaş hukuku kapsamında siber ortamdaki saldırılara karşı çözüm arayışları, hukuk kamuoyunun dikkatini 1990'ların sonlarında çekmeye başlamıştır. Konuyla ilgili en önemli hukuk konferansı ilk olarak, 1999 yılında Amerika Birleşik Devletleri (ABD) Deniz Harp Akademisi'nde (Naval War College) düzenlenmiştir[6]. 11 Eylül saldırıları konuyu siber terörizm boyutuna taşımış, 2007 yılında Estonya[7], 2008 yılında Gürcistan'a[8] yapılan siber saldırılar ve 2010 yılındaki Stuxnet[9] vakası konunun üzerindeki tartışmaların giderek artmasını sağlamıştır.

Saldırıların açmış olduğu zararlar ve teknolojinin ilerlemesine bağlı olarak saldırı potansiyelinin artması devletlerin siber kabiliyetlerini geliştirmelerine, aynı zamanda da bu saldırılara karşı önlem almalarına ve doktrin üretmelerine sebep olmuştur.

İngiltere'nin 2010 tarihli "Ulusal Güvenlik Stratejisi"nde, gelecek beş yılda güvenlik açısından önlem alınması gereken en önemli dört konudan biri, devlet, organize suç örgütü ve terörist grup tarafından yapılacak siber saldırılar olarak kabul edilmektedir[10].

---

6 SCHMITT, Michael N. / O'DONNELL, Brian T. (Editörler), **Computer Network Attack and International Law**, V.76, Naval War College International Law Studies, Rhode Island: William S. Hein & Co.,Inc, 2002, https://www.usnwc.edu/getattachment/95012329-e379-4341-bd1d-a4764c84dd4c/Vol--76--Computer-Network-Attack-and-Internation.aspx (erişim tarihi 10.1.2013).

7 Ayrıntılı bilgi için bkz. dipnot 5.

8 Ayrıntılı bilgi için bkz. dipnot 6.

9 Ayrıntılı bilgi için bkz. dipnot 7.

10 İngiltere'nin güvenlik konusundaki diğer üç önceliği, uluslararası terörizm, uluslararası askeri kriz, doğal felaket veya büyük çaplı kazalardır. **A Strong Britain in an Age of Uncertainty: The National Security Strategy**, 2010, (Başbakan tarafından Kraliçe adına Parlamento'ya Ekim 2010 tarihinde sunulan rapor), http://www.direct.gov.uk/prod_consum_dg/groups/dg_digitalassets/@dg/@en/documents/digitalasset /dg_191639.pdf (erişim tarihi 10.1.2013).

Amerika Birleşik Devletleri'nin 2010 tarihli "Ulusal Güvenlik Stratejisi"nde siber tehdit, en ciddi ulusal güvenlik, kamu güvenliği ve ekonomik mücadele konularından kabul edilmiş[11], Savunma Bakanlığı tarafından hazırlanan 2011 tarihli "Siber Uzay Operasyon Stratejisi"ne göre siber ortam, savaş alanı olarak kabul edilerek strateji geliştirilmiştir[12]. Bu gelişmelere paralel olarak ABD, 23 Haziran 2009 tarihinde Stratejik Komutanlığa verilen emir gereği, 21 Mayıs 2010 tarihinde siber ortamdaki operasyonları yönetmek üzere "Siber Komutanlık" (CYBERCOM) kurmuştur[13].

ABD, 2011 tarihli "Siber Uzay için Uluslararası Strateji" belgesinde siber saldırılara karşı uluslararası işbirliğine ilişkin strateji geliştirmiştir. Bu belgede, "Siber uzaya hâkim olacak normlar, ne geleneksel uluslararası hukuk kurallarını yeniden geliştirmeye gerek duyar, ne de mevcut normları anlamsız kılar. Uzun süredir, barışta veya savaşta, devletlerin hareketlerine yön veren normlar siber uzay için de uygulanabilir." diyerek siber uzaya uygulanacak uluslararası hukuk normları hakkında ulusal görüşünü dile getirirken, "network teknolojisinin kendine has özelliklerine göre normların nasıl uygulanacağını ortaya koymak gerekmektedir" şeklindeki ifadeyle mevcut normların siber uzayın ve gelişen teknolojinin özellikleri göz önüne alınarak yorumlanması gerektiğini vurgulamaktadır[14].

Kanada, "Kanada'nın Siber Güvenlik Stratejisi"[15], Birleşik Krallık, "Birleşik Krallık Siber Güvenlik Stratejisi: Dijitalleşen Dünya'ya Birleşik Krallığı Taşımak ve Korumak"[16] belgeleri ile strateji oluştururken, Rusya, "Silahlı Kuvvetleri'nin Bilgi Ortamındaki Aktivitelerine İlişkin Konsept"[17] hazırlamıştır.

NATO ise, konuya ilişkin çalışmalarını 2002 yılından itibaren sürdürmekle birlikte, 2010 yılındaki Lizbon Zirvesi'nde siber savunmanın sürekli olarak NATO gündeminde bulunması yönünde temel bir karar almıştır[18]. Haziran 2011 tarihinde NATO Savunma Bakanları, "Gözden Geçirilmiş NATO Siber Savunma Politikası"nı kabul etmişlerdir. Bu politika, siber savunma konusunda gerçekleştirilecek olan topluluk bazındaki çabaları

---

11 The White House **National Security Strategy**, 2010, http://www.whitehouse.gov/sites/default/files/rss_viewer/national_security_strategy.pdf (erişim tarihi 11.1.2013).

12 U.S. Department Of Defence, 2011, **Department of Defence Strategy For Operating in Cyberspace**, http://www.defense.gov/news/d20110714cyber.pdf (erişim tarihi 10.1.2013).

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

14 Department of Defence Strategy For Operating in Cyberspace, 2011, s.9.

15 Government of Canada, 2010, **Canada's Cyber Security Strategy**, http://www.publicsafety.gc.ca/prg/ns/cybr-scrty/_fl/ccss-scc-eng.pdf (erişim tarihi 8.11.2012).

16 **The UK Cyber Security Strategy: Protecting and Promoting The UK in a Digital World**, 2011, http://www.carlisle.army.mil/dime/documents/UK%20Cyber%20Security%20Strategy.pdf (erişim tarihi 11.1.2013).

17 Russain Federation, 2011, **Conceptual Views Regarding the Activities of the Armed Forces of the Russian Federation in Information Space**, http://pircenter.org/media/content/files/9/13480921870.pdf (erişim tarihi 10.1.2013).

18 **Lisbon Summit Declaration,** 20.11.2010, http://www.nato.int/nato_static/assets/ pdf/pdf_publications/20120207_strategic-concept-2010-tur.pdf (erişim tarihi 3.1.2013).

içermektedir. Ekim 2011 tarihinde Bakanlar tarafından, "Siber Savunma Eylem Planı"nın detayları üzerinde görüş birliğine varılmıştır. 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, istihbarat paylaşımı ve durumsal farkındalık için bir "Siber Tehdit Farkındalık Birimi" vücuda getirilmiştir[19]. 2012 Chicago Zirvesi Sonuç Bildirisi'nde de sürekli gelişen ve karmaşıklaşan siber tehditlerle etkin biçimde ve işbirliği içinde mücadele edilmesi gerektiği vurgulanmıştır[20].

1.2. Siber Ortamda Silah Kavramı

Bilgi çağıyla birlikte silahın tanımı da değişmeye başlamıştır. Günümüzde ordular amaçlarını elde etmek için sadece top, tüfek, füze ya da bomba gibi fiziksel anlamda silah kullanmamaktadırlar. Diğer anlamda, bilgisayar ve iletişim teknolojisi savaş gereksinimlerini değiştirmiş ve silah teriminin tanımını evrime uğratmıştır.

Bilgi çağındaki silah teriminin anlamını vermek için geleneksel anlamda silahın ne anlam ifade ettiğine bakmakta fayda vardır. Bir silah ateşlendiğinde mermi, yolunu izleyerek bir hedefe çarpar ve zarar verir. Silahın kendisi tek başına zararlı değildir, onun rolü mermiyi hedefe göndermekten ibarettir. Mermi de tek başına zarar verme kabiliyetine sahip değildir, ancak yüksek hızda bir silah aracılığıyla hedefe yönlendirildiğinde zarar verici özelliğinden bahsedilebilir. Mermi, bir kullanıcı tarafından silaha konup hedefe doğru ateşlenmedikten sonra, silah da mermi de zarar verici değildirler.

Yukarıdaki anlatımdan yola çıkarak siber ortamdaki silah tanımına bakıldığında, zararlı bir kod, sistemlere zarar verici komutlar veya bilgi mermi olarak algılanabilir. Kod, kendi kendini yazmaz ya da hedefe yönlendirmez. Kod yazmak, komut vermek veya onları başka bir sisteme transfer etmek için bilgisayar veya iletişim teknolojilerine ihtiyaç vardır. En önemli ihtiyaç ise bir kullanıcıdır. Yani geleneksel anlamda mermiyi silaha koyup ateşleyecek bir kullanıcı gereksinimi vardır, bu da bilgisayar veya sistem kullanıcısıdır. Bu açıklamadan yola çıkarak siber anlamda bir silah için üç gereksinim vardır: kod, bilgisayar veya iletişim teknolojisi ve sistem kullanıcısı.

Siber savaşın silahları ise üç kategoriye ayrılabilir: sentaktik saldırılar, semantik saldırılar ve karışık saldırılar[21]. Sentaktik saldırıların hedefi bilgisayar işletim sistemleri olup,

---

19 **NATO Rapid Reaction Team to Fight Cyber Attack**, 13.3.2012, http://www.nato.int/cps/en/natolive/news_85161.htm (erişim tarihi 3.1.2013).

20 **Chicago Summit Declaration**, 20.5.2012, http://www.nato.int/cps/en/SID-D43E0787-B3987422/natolive/official_texts_87593.htm?mode=pressrelease (erişim tarihi 3.11.2012).

21 BRENNER, Susan W. / GOODMAN, Marc D., "In Defense of Cyberterrorism: An Argument for Anticipating Cyber Attacks", **University Of Illionis Journal of Law, Technology and Policy**, Bahar 2002, s.27-42.

zararlı kodlar/yazılımlar[22], hizmet engelleme saldırıları[23] ve sisteme girmek (hack)[24] olarak sayılabilir.

Semantik saldırılar, bilgisayarın işletim sistemini hedef almazlar, bunun yerine bilgisayar kullanıcısının ulaştığı bilginin doğruluğunu hedef alırlar. Sistem sorunsuz bir şekilde çalışmasına rağmen içerdiği bilgiler doğru değildir[25]. Bu saldırılar, özellikle resmi internet sitelerinin ya da kritik altyapı tesislerinin sistemlerini hedef aldığında ciddi sonuçlar doğurabilir. Nükleer tesisteki bir sistemin hatalı olarak deprem algılaması ve uyarı vermesi sonucunda elektriğin kesilmesi ya da havaalanında kullanılan trafik kontrol sisteminin uçakların inişi ile ilgili doğru bilgi vermemesi sonucu meydana gelebilecek hatalı yönlendirmeler örnek olarak gösterilebilir[26].

Karışık saldırılar, sentaktik ve semantik saldırıların birlikte yapılmasıdır. Kritik işletim sistemlerinin hatalı bilgi ile beslenerek etkisiz hale getirilmesi karışık saldırıya örnek olarak gösterilebilir[27].

Siber ortamdaki silah kavramının ve bu silahların neler olduğu yukarıdaki açıklamalar ile ortaya konulmasına rağmen geleneksel anlamda bile silahlı saldırı kavramının tanımına BM Antlaşması'nın hükümlerinde yer verilmemiş olması, siber ortamda neyin silah olduğu konusundaki sorunun çözümünü zorlaştırmaktadır.

"Silahlı saldırı" terimi diğer terimlerin aksine BM Antlaşması'nda dar yorumlanmaktadır[28]. Örneğin Antlaşma'nın 2(4). maddesini ihlal eden bazı tehdit veya kuvvet kullanımları, 51. madde anlamında silahlı saldırı teşkil etmemektedir. Bu durumda silahlı saldırı olarak değerlendirilemeyecek olan siber saldırılar, dolayısıyla 51. madde uyarınca meşru müdafaa hakkı doğurmamaktadır.

BM Antlaşması'nın 51. maddesinde, meşru müdafaa hakkının kullanılabilmesinin ön şartı olarak "saldırının" değil bir "silahlı saldırı"nın gerçekleştirilmiş olması kabul edilmiştir. Ancak, silahlı saldırı kavramının tanımına ne bu maddede ne de diğer madde hükümlerinde yer verilmemiştir. Saldırı ve silahlı saldırı kavramları,

---

22 Bilgisayar ortamına kullanıcının bilgisi/onayı dışında aktarılmış, mevcut dosyaları, yazılım ve/veya işletim sisteminin bütünlüğünü, erişilebilirliğini, tehdit eden yetkisiz kod parçaları ve yazılımlar genel olarak zararlı kod/yazılım olarak tanımlanmaktadır. Zararlı kodlar/yazılımlar, virüsler, solucanlar, zararlı mobil yazılımlar, truva atları, casus yazılımlar olarak alt başlıklar halinde sayılabilir. ÖZDEMİR, Battal, **Zararlı Yazılıma Karşı Korunma Klavuzu**, Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü Doküman Kodu:BGT-1004, Kocaeli, 2007, s.8-14.

23 Hizmet engelleme saldırıları (Denial of Service Attack), karşı sistemde çalışan servisin durdurulmasını amaç edinir. Web sunucuları artık http servisi veremez, e-posta sunucuları posta gönderip alamaz hale gelir. ÖZDEMİRCİLİ, Özgür, **Denial of Service Saldırılarının Önlenmesi**, http://www.enderunix.org/docs/dos-saldirilari.pdf (erişim tarihi 12.1.2013).

24 Bilgisayara sistemine girmek ve değiştirmek hack'lemek olarak tanımlanmaktadır. BRENNER/GOODMAN, **Bahar 2002**, s.22,31.

25 BRENNER/GOODMAN, **Bahar 2002**, s.31,32.

26 BRENNER/GOODMAN, **Bahar 2002**, s.36,37.

27 BRENNER/GOODMAN, **Bahar 2002**, s.40,41.

28 DINSTEIN, Yoram, "Computer Network Attack and Self-Defense", **Computer Network Attack and International Law, V.76. Naval War College International Law Studies**, Rhode Island, William S. Hein & Co.,Inc., 2002, s.100, https://www.usnwc.edu/getattachment/95012329-e379-4341-bd1d-a4764c84dd4c/Vol--76--Computer-Network-Attack-and-Internation.aspx (erişim tarihi 13.1.2013).

belli ölçüde birbiriyle örtüşen kavramlar olmalarına rağmen; tam olarak aynı şey değildirler. Daha da önemlisi bunların hukuksal anlamları farklı olup pratikte farklı sonuçlar doğurmaktadırlar.

Silahlı bir saldırının aynı zamanda bir saldırı olduğu söylenebilir fakat her saldırı bir silahlı saldırı değildir. Çünkü silahlı saldırı kavramı, saldırı kavramından daha dar bir anlam ifade etmektedir. Bir silahlı saldırı, saldırının bir alt kategorisi olduğu kabul edilmektedir. Ayrıca, bu iki kavram, doğurduğu sonuçlar itibariyle de birbirinden farklıdır. Silahlı saldırı, doğurduğu sonuçlar itibariyle, kabul edilmeyecek ölçülerde olduğu için; mağdur devlete; meşru müdafaa hakkına dayanarak münferiden kuvvet kullanma yetkisi verir. Bu husus silahlı saldırının ayırt edici nitelik ve fonksiyonunu ortaya koymaktadır. Saldırı kavramına giren diğer fiillerde ise bu nitelik yoktur; kolektif güvenlik sisteminin devreye girmesini sağlayan başka fonksiyona sahiptir.

Siber saldırılara karşı kuvvet kullanmanın ön şartı; 51. madde bağlamında "silahlı saldırı" olarak kabul edilmesidir. Dolayısıyla, askeri bir harekatın meşru olabilmesi için, saldırının silahlı saldırı boyutuna ulaşmış olması zorunludur.

1.3. Ortak Tanım Sorunu

Son on yıl içersinde birçok yazar, gerçekleşmesi muhtemel siber saldırıların sonuçları konusunda öngörü de bulunmaktadırlar. Bir virüsün finans kayıtlarını yok etmesi ve borsayı çalışamaz hale getirmesi[29], hatalı bir mesajın nükleer tesisisin çalışmasını durdurması[30], baraj kapaklarını açması, havaalanı trafik sisteminin karıştırılması sonucu uçak kazalarının yaşanması[31] gibi fiziksel ve ekonomik zararlar verecek, can kayıplarına neden olacak örnekler çoğaltılabilir. Bugüne kadar yaşanan Estonya[32], Gürcistan[33] ve Stuxnet[34] olayları siber saldırıların ciddiyetini göstermiştir. Ancak, bu saldırıların savaş nedeni olacak bir siber saldırı olup olmadığı konusunda gerek bilim dünyasında gerekse uluslararası kamuoyunda görüş birliği bulunmamaktadır.

Devletler, siber tehdide karşı strateji geliştirmekte ve hukuki anlamda siber saldırıları savaş hukuku kurallarına uydurmaya çalışmaktadırlar. Siber saldırılardan kaynaklanan tehditlerin anlaşılması konusunda, özellikle göze çarpan iki çalışma bulunmakta olup, bunlardan biri ABD'nin, diğeri Rusya ve Çin'in öncülük ettiği Şangay İşbirliği Örgütü'nün çalışmalarıdır.

---

29 HOLLIS, Duncan B, "Why States Need an International Law for Information Operations", **Lewis & Clark Law Review**, 2007, V.11, s.1023,1042.

30 ANTOLIN-JENKINS, Vida., "Defining the Parameters of Cyberwar Operations: Looking for Law in All the Wrong Places?", **Naval Law Review**, 2008, V.51, s.132,140.

31 GELLMAN, Barton, "Cyber Attacks by Al Qaeda Feared; Terrorists at Threshold of Using Internet as Tool of Bloodshed, Experts Say", **Washington Post**, 27.6.2002, s.A01, http://ellen-bomer.com/Osama/Cyber-Attacks.html (erişim tarihi 10.1.2013).

32 Ayrıntılı bilgi için bkz. dipnot 5.

33 Ayrıntılı bilgi için bkz. dipnot 6.

34 Ayrıntılı bilgi için bkz. dipnot 7.

ABD Ordusu, siber saldırı ve siber savaş konusunda resmi bir tanım yapılması için Kongre'ye öneride bulunmuş olmasına rağmen[35], ABD Genelkurmay Başkanlığı siber savaşa yakın bir anlam ifade eden tanımı talimnamelerinde bu öneriden önce yapmış olup, "bilgi savaşı" terimini kullanmış ve "düşmanın insan ve araç kaynaklı karar alma sistemlerini etkilemek, etkinliğini azaltmak, bozmak veya ele geçirmek buna karşın kendi sistemlerini korumak" olarak tanımlamıştır[36] Birleşmiş Milletler Terimler Sözlüğü'nde, siber savaş (cyber war) bilgi savaşı (information warfare) ile birlikte aynı anlamda, "bilgisayar sistemlerinin düşman sistemlerine zarar vermek veya yok etmek maksadıyla kullanıldığı savaş tipidir" şeklinde tanımlanmaktadır[37]. Siber savaşın, İngilizce karşılığı olan "cyberwar", bazı sözlüklerde de bilgi savaşının yani "information war" 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[38].

Konunun yeni ortaya çıkmaya başladığı 1990'lı yıllarda siber savaş, bilgi savaşı ile birlikte değerlendirilmiş ve askeri doktrinde siber savaş, bilgi savaşı içinde icra edilen harekatlardan sayılmıştır [39]. Bilgi savaşı, siber savaşı da kapsayacak bir üst terim olmasına rağmen, günümüzde siber savaş ve bilgi savaşı terimleri birbirinin eş anlamlısı terimler olarak kabul edilmemektedir[40].

---

35 2001 yılındaki ABD Kongre Araştırma Servisi (The Congressional Research Service) raporunda resmi bir tanımlama yapılmasına rağmen bu tanımlama siber savaşa özgü bir tanımlama değildir. Bu raporda siber savaş, "siber ortamda gerçekleşen bir savaştır. Bu savaş bilgi ve network ağının savunulmasının yanında, saldırılara karşı caydırıcı önlemler alınmasını da içerir. Aynı zamanda düşmana karşı saldırı amaçlı bilgi operasyonları yapmayı ve savaş alanında bilgiye hâkim olmayı da kapsar" şeklinde tanımlanmıştır. HILDRETH, Steven A., **Cyberwarfare,** Congressional Research Service Report for Congress, 19.6.2001, s.CRS-16, http://www.fas.org/irp/crs/RL30735.pdf (erişim tarihi 13.1.2012); 2011 tarihli "Siber Uzay Operasyon Stratejisi"nde siber ortamdaki tehditleri tanımlamak için "siber saldırılar" yerine "siber tehditler" terimi kullanılmıştır. (Department of Defence Strategy For Operating in Cyberspace, **2011**, s.2).

36 **Information Operations (Joint Publications 3-13),** 27.11.2012, s.GL-3, http://www.dtic.mil/doctrine/new_pubs/jp3_13.pdf (erişim tarihi 13.1.2013).

37 **United Nations Terms**, http://unterm.un.org/dgaacs/unterm.nsf/WebView/ E996B25EA7D3B36E85256B090056D806?OpenDocument (erişim tarihi 31.10.2012).

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

39 WINGFIELD, Thomas C., **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. KAŞIKÇIOĞLU, Nafi, "Elektronik Harp". **Siber Savunma Sempozyumu**, Askeri Müze ve Kültür Sitesi Komutanlığı, Harbiye, İstanbul, 24-25.5.2011; LIBICKI, Martin C., **What is Information Warfare?,** National Defence University, Washington, 1995, s.7, 75 vd.; "Bilgi savaşı", NATO Bilgi Harekatı 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.

40 **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).

ABD Ulusal Araştırma Konseyi tarafından siber saldırı, "bilgisayar sistemlerini, ya da bilgisayar sistemlerinde bulunan bilgileri veya programları değiştirmek, bozmak, aldatmak, azaltmak, yok etmek veya bu programlara veya sistemlere geçiş yapmak" olarak tanımlanmıştır[41]. ABD tarafından siber saldırı için "amaç bazlı" bir tanım yapılması yaklaşımı tercih edilmiştir.

Şangay İşbirliği Örgütü, siber saldırı için daha geniş anlamlı ve "araç bazlı" bir bakış açısı geliştirmiş ve "bilgi ve iletişim teknolojilerinin uluslararası tehdit oluşturduğunu, bu tehditlerin sivil ve askeri alandaki mevcut barış ve düzenin bozulmasına sebebiyet vereceğini ve bununla mücadele edilmesi gerektiğini" ifade etmiştir. Örgüt "bilgi savaşı"nı, "toplum ve devlet düzenini bozmak için toplu psikolojik beyin yıkama faaliyetlerinin yanında devleti, düşman devlet isteklerine göre karar almaya zorlamak" olarak tanımlamaktadır [42]. Bu tanımdan anlaşılacağı üzere, Örgüt "siber saldırı" terimine, siber teknolojiler kullanılarak barışı ve siyasi düzeni bozmak anlamını yüklemektedir.

Yukarıda verilen iki örnek terimler konusunda ortak bir tanımın yapılamadığını göstermektedir. Devletler ya da devlet toplulukları ile uluslararası örgütler kendilerine göre tanımlamalar yapmakta, ancak bu tanımlamalar birbiri ile örtüşmemektedir. Bu durum, hukuki tanımlamalar ve açıklamalar konusunda, bilim adamlarının karşılaştığı en büyük güçlüklerden birisi olarak ortaya çıkmaktadır. Ancak bu güçlüğe rağmen en azından siber ortamda silah ve saldırı kavramlarının neyi ifade edeceği aşağıda anlatılmaya çalışılacaktır.

2. SİBER SAVAŞIN SİBER ORTAMDAKİ DİĞER KÖTÜ NİYETLİ HAREKETLERDEN FARKI

2.1. Siber Savaş-Siber Saldırı-Siber Suç

Siber suç kavramının tanımı konusunda uluslararası kamuoyunda ortak bir görüş bulunmamaktadır. Siber suç üzerine en kapsamlı uzlaşma belgesi olan Avrupa Konseyi Sibersuç Sözleşmesi'nde de siber suç tanımı yapılmış değildir. Sözleşme'de siber suçlar; yetkisiz erişim, sisteme ve veriye müdahale, bilişim sistemi aracılığıyla sahtekârlık ya da dolandırıcılık suçları ile sınırlı tutulmamaktadır. Siber suçların, sadece bilgisayar ve veriye yönelik fiilleri esas almadığı bilişim sistemlerinin kullanılmasıyla ve özellikle internetin yaygınlaşması ile birlikte niceliksel olarak ortaya çıkan sorunları da kapsadığı görülmektedir[43]. Bu açıdan çocuk pornografisi, telif haklarına ilişkin ihlaller ve son olarak Sözleşme'ye yapılan ek protokolle kapsama alınan, yabancı düşmanlığının ve ırkçılığın

---

41 OWENS, William A./DAM, Kenneth W./LIN, Herbert S. (Editörler), **Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities,** National Research Council, Committee on Offensive Information Warfare Computer Science and Telecommunications Board Division on Engineering and Physical Sciences, 2009, s.1, http://www.carlisle.army.mil/DIME/documents/2Cyberattack%20 Brochure_FINAL.pdf (erişim tarihi 11.12.2013).

42 **Agreement between the Governments of the Member States of the Shanghai Cooperation Organization on Cooperation in the Field of International Information Security**, 61st Plenary Meeting (2.12.2008).

43 KETİZMEN, Muammer, **Türk Ceza Hukukunda Bilişim Suçları**, Ankara Üniversitesi Sosyal Bilimler Enstitüsü Kamu Hukuku Anabilim Dalı Doktora Tezi, Ankara, 2006, s.61.

önlenmesine ilişkin hükümler de siber suç kapsamına alınmıştır[44]. Sözleşme'de bu suçların minimum bir uzlaşmayı temsil ettiği ve taraf devletlerin kendi mevzuatlarında başka suçları da düzenleyebilecekleri belirtilmiştir.

Siber suçların çoğu çeşidi, siber saldırı veya siber savaş kapsamında değildir, politik amaçlar gütmez veya ulusal güvenlik açısından sorun teşkil etmemektedir. Siber saldırıların aksine siber suçlar, diğer suçlar gibi kişi, kişiler veya organize suç örgütleri tarafından işlenirler ve hukuka aykırı bir fiil olarak suç olarak tanımlanmaktadırlar. Örneğin, ulusal güvenlik tehdit etmeden ekonomik çıkar sağlamak amacıyla işlenen banka sistemine girilmesi eylemi, ya da internet üzerinden çocuk pornografisi yayma eylemleri siber suça bir örnek olarak verilebilir. Ancak bu suçlar, siber saldırı veya siber savaş kapsamında sayılmazlar.

Siber saldırı ise basit tanımıyla, siber ortamdaki imkânlar kullanılarak, bilgisayar sitemleri, yazılım ya da iletişim sistemlerine yapılan kötü niyetli eylemler olarak tanımlanabilir. Bazı siber saldırı vardır ki, devlete bağlı kişi veya organizasyonlar aracılığıyla işlenen ancak siber savaş veya siber suç kapsamına girmeyecek cinstendir. Buna, Çin'in 2011 yılında Falun Gong adında bir ruhani grubun internet sitesine düzenlediği siber saldırı gösterilebilir. Çin, bu grubu, "milli onuru tamamen ayaklar altına almakla, kendilerini Çin'e karşı olan güçlerin ellerine bırakmakla ve uluslararası düşman kuvvetlerinin Çin'in iç işlerine karışmaları için bir araç olarak kullandırmaya istekli olmakla" suçlayarak politik ve ulusal güvenlik amaçlı olarak siber saldırı düzenlemiştir[45]. Bu saldırı devlet eliyle gerçekleştirildiğinden siber suç kapsamına girmez, mağdur devlet olmadığı gibi silahlı çatışma kapsamında da değerlendirilemeyeceğinden siber savaş da değildir.

Bazı siber saldırılar ise, devlet dışı aktörler tarafından işlenen ancak siber suç olarak tanımlanmayan, bunun yanında silahlı çatışma kapsamında da sayılamayacak cinsten saldırılardır. Buna, kişi veya gruplar tarafından işlenen ancak suç teşkil etmeyen siber saldırılar örnek olarak verilebilir.

Bir kısım siber saldırılar, siber savaş kapsamında değerlendirilemeyecek olsa da siber suç kapsamına girmektedirler. Devlet dışı kişi ya da grupların suç teşkil eden hukuk dışı hareketleri veya bunların, ulusal güvenliği tehdit edecek politik amaçlı saldırıları hem siber saldırı hem de siber suç kesişiminde olabilir. Devlet dışı aktörlerin politik veya ulusal güvenliği tehdit amaçlı olarak, bir devletin resmi kayıtlarının tutulduğu sistemi kapatması veya zarar vermesi buna örnek olarak verilebilir.

Diğerlerine kıyasla çok az sayıdaki siber saldırı çeşidinin, hem siber saldırı hem de siber savaş kesişiminde olması muhtemeldir. Buna iki örnek verilebilir. Suçu işleyen aktörün, devlet dışı veya devlete bağlı olup olmadığına bakılmaksızın, uluslararası hukukta "silahlı çatışma" olarak kabul edilebilecek ancak, konvansiyonel bir savaşın sonuçlarına

---

44 **Additional Protocol to the Convention on Cybercrime, Concerning the Criminalisation of Acts of a Racist and Xenophobic Nature Committed Through Computer Systems**, 28.1.2003, Strasbourg, http://conventions.coe.int/Treaty/en/Treaties/Html/189.htm (erişim tarihi 16.11.2012).

45 MCMILLAN, Robert/KAN, Michael, **China Hacking Video Shows Glimpse of Falun Gong Attack Tool,** 23.8.2011, http://www.pcworld.com/article/238655/china_hacking_video_shows_glimpse_of_falun_gong_attack_tool.html (erişim tarihi 14.1.2013).

eşit olmayacak bir siber saldırıyı, bilgisayar veya iletişim sistemi üzerinde gerçekleştirmesi ilk örnek olarak verilebilir. Diğeri ise, bir devlet veya devlete bağlı aktör tarafından bilgisayar veya iletişim sistemi kullanarak, sonuçları konvansiyonel bir savaşın sonuçlarına eşit olacak bir saldırı gerçekleştirilmesidir. Bu, saldırıların hukuka aykırı olarak siber suç olarak tanımlanmamış veya hareketin suç unsurları taşımıyor olması durumunda geçerlidir.

Siber savaş olan bir hareketin, hem siber suç hem de siber saldırı olarak kabul edilmesi de mümkündür. Bu kesişim şu iki halde olabilir. İlki, devlet dışı bir aktörün, bir devletin bilgisayar veya iletişim sistemi üzerinde, bilgisayar veya iletişim sistemi kullanmak suretiyle politik veya devlet güvenliğini tehdit amaçlı bir saldırı gerçekleştirmesi ve bu saldırının silahlı çatışma eşiğine ulaşmasının yanında ulusal veya uluslararası ortamda suç olarak da düzenlenmiş olması durumudur. İkincisi ise, bir devlet veya devlete bağlı aktör tarafından bilgisayar veya iletişim sistemi kullanılarak, sonuçları konvansiyonel bir savaşın sonuçlarına eşit olacak bir siber saldırı gerçekleştirilmesi, bu saldırının ulusal veya uluslararası ortamda suç olarak da düzenlenmiş olmasıdır.

2.2. Siber Savaş-Siber Casusluk

Devlet güvenliğine karşı işlenen suçların en önemli, en tehlikeli ve en eskilerinden biri casusluk suçudur. 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.[46] Nitekim batı dillerinde[47] casusluk, gözetlemek anlamına gelen "spigare", "epier" fiilinden alınmış bir kelimedir[48].

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, 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[49]. Bu

---

46 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. DEVELLİOĞLU, Ferit, **Osmanlıca-Türkçe Ansiklopedik Lûgat**, 24. Baskı, Aydın Kitabevi, Ankara, 2007, s.20.

47 Casusluk: Fransızca Espionnage; İngilizce Espionage; Almanca Spionage; İtalyanca Spionaggio; İspanya Espionaje; Rusça Špionstvo; bunların kökü İtalyanca spia (casus) kelimesinin abartılı sekli olan "spione" kelimesinden gelmektedir. "spiare" (Eski Fransızca "ıpier", 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.

48 GÖZÜBÜYÜK, Abdullah P., Alman, **Fransız, İsviçre ve İtalyan Ceza Kanunlarıyla Mukayeseli, Türk Ceza Kanunu Açıklaması**, Cilt 1, 3. Baskı, Kazancı Yayınevi, Ankara, 1982, s.509.

49 AKGÜÇ, Atıf, "Casusluk Suçu", **Siyasi İlimler Mecmuası**, 1948, Yıl 10. Sayı 118, s.478.

tarifler, daha çok savaş zamanında yapılan askerî casusluğa ait olup, konunun muhtelif şekillerini kapsayacak bir kapsam taşımamakta, mesela barış 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.

Teknolojinin büyük bir hızla geliştiği günümüzde casusluk faaliyetlerinin geçmişte sadece askeri ve siyasi alanlara yöneldiği, bugünün dünyasında ise telekomünikasyondan bilgisayar teknolojisine, genetikten havacılık endüstrisine, lazer teknolojisinden optik alanındaki araştırmalara kadar her alanda etkisini hissettirdiği ortadadır.

Günlük yaşamın internet ile iç içe geçtiği günümüzde, internet üzerinden şahısların ve küçük ölçekli şirketlerin kimlik bilgilerinin, kullanıcı hesaplarının ele geçirilmesi artık çok sık yaşanan vakalar haline gelmiştir.

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.

Siber savaş nedeni olarak değerlendirilebilecek siber casusluk faaliyetlerinin hedefi günümüzde devlete ilişkin sırların yanında endüstriyel sırlar da olmaktadır. Büyük emek, mesai ve kaynak harcanarak yapılan buluşların gizlenmesi ve yanlış kişilerin eline geçmemesi veya kullanılmaması devlet güvenliği için büyük 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.[50]

2.3. Siber Savaş-Siber Terörizm

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 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

50 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.

hususunda mutabakat yoktur. Ülkelerin yaklaşımındaki farklılıklar tanımı zorlaştıran en önemli etkenlerin başında gelmektedir[51].

Her devlet, terörizmin tanımını, kendi siyasi bakış açısına göre değerlendirmektedir[52]. 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[53]. 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[54]. 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[55].

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 değiştirtmek maksatlı olarak silah veya hedef olarak kullanılması şeklinde tanımlanabilir[56]. Siber terörizmi icra 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.

---

51 **Terörizmle Mücadelede Uluslararası İşbirliği ve Tanım Sorunu,** Dışişleri Bakanlığı Resmi İnternet sitesi, http://www.mfa.gov.tr/terorizmle-mucadelede-uluslararasi-isbirligi_-ve-tanim-sorunu-.tr.mfa (erişim tarihi 12.11.2012).

52 "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 Devletinin 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.

53 *ÇİTLİOĞLU, Ercan,* **Gri Tehdit Terörizm**, 1. Baskı, Destek Yayınları, Ankara, 2008, s.17.

54 KRASAVIN, Serge, **What is Cyber Terrorism?,** http://www.crime-research.org/library/Cyber- terrorism.htm (erişim tarihi 4.11.2012).

55 DENNING, Dorothy E, **Cyberterrorism**, http://www.cs.georgetown.edu/~denning/infosec/cyberterror-GD.doc (erişim tarihi 07.11.2012).

56 ANDRESS, Jason/WINTERFELD, Steve, **Cyber Warfare,** Elsevier, 2011, s.198.

Sonuç

Devletler ulusal güvenliklerini sağlamak ve tehlikelere karşı hazırlık yapmak zorundadırlar. Günümüzde siber güvenlik, küçük büyük, gelişmiş ya da az gelişmiş her ülke için tehdit önem arz etmekte ve ulusal güvenliğin en önemli parçası haline gelmiştir. Siber alan, fiziki alan gibi sınırları olan üzerinde tek bir devletin egemenlik kurduğu bir alan olmadığından gelişen teknolojik imkânlar sayesinde siber ortamdaki kötü niyetli hareketler önü alınamaz şekilde artmaktadır.

Henüz siber savaş konusunda ittifak edememiş uluslararası toplumun; yakın gelecekte teknolojinin gelişimi ile daha karmaşık hale gelecek kötü niyetli siber hareketler konusunda ortak bir çaba içine girmesi, öncelikle kavramlar konusunda fikir birliğine vardıktan sonra hukuki anlamda gerekli hazırlıkları yapmasının kaçınılmaz olduğu değerlendirilmektedir.

KAYNAKÇA

A Strong Britain in an Age of Uncertainty: The National Security Strategy, 2010, (Başbakan tarafından Kraliçe adına Parlamento'ya Ekim 2010 tarihinde sunulan rapor), **http://www.direct.gov.uk/prod_consum_dg/groups/dg_digitalassets/@dg/@en/documents/digitalasset /dg_191639.pdf** (erişim tarihi 10.1.2013).

Additional Protocol to the Convention on Cybercrime, Concerning the Criminalisation of Acts of a Racist and Xenophobic Nature Committed Through Computer Systems, 28.1.2003, Strasbourg, **http://conventions.coe.int/Treaty/en/Treaties/Html/189.htm** (erişim tarihi 16.11.2012).

Agreement between the Governments of the Member States of the Shanghai Cooperation Organization on Cooperation in the Field of International Information Security, 61st Plenary Meeting (2.12.2008).

AKGÜÇ, Atıf, "Casusluk Suçu", **Siyasi İlimler Mecmuası,** 1948, Yıl 10. Sayı 118, s.477-484.

ANDRESS, Jason/WINTERFELD, Steve, **Cyber Warfare,** Elsevier, 2011.

ANTOLIN-JENKINS, Vida., "Defining the Parameters of Cyberwar Operations: Looking for Law in All the Wrong Places?", **Naval Law Review**, 2008, V.51, s.132-174.

ASLAN, Yasin, "Savaş Hukukunun Temel Prensipleri", **Türkiye Barolar Birliği Dergisi**, 2008, Sayı 79, s.235-274.

BAKIR, Emre, "İnternet Güvenliğinin Tarihçesi", **TUBİTAK Bilgem Dergisi**, 2011, Cilt 3, Sayı 5, s.16.

BRENNER, Susan W. / GOODMAN, Marc D., "In Defense of Cyberterrorism: An Argument for Anticipating Cyber Attacks", **University Of Illionis Journal of Law, Technology and Policy,** Bahar 2002, s.1-42.

Chicago Summit Declaration, 20.5.2012, **http://www.nato.int/cps/en/SID-D43E0787-B3987422/natolive/official_texts_87593.htm?mode=pressrelease** (erişim tarihi 3.11.2012).

Collins Dictionaries, **http://www.collinsdictionary.com/dictionary/english/cyberwar** (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).

***ÇİTLİOĞLU, Ercan,* Gri Tehdit Terörizm,** 1. Baskı, Destek Yayınları, Ankara, 2008.

DEIBERT, Ronald, "Tracking the Emerging Arms Race in Cyberspace", **Bulletin of the Atomic Scientists,** Ocak/Şubat 2011, s.1-8.

DENNING, Dorothy E, **Cyberterrorism**, **http://www.cs.georgetown.edu/~denning/infosec/**cyberterror-GD.doc (erişim tarihi 07.11.2012).

DINSTEIN, Yoram, "Computer Network Attack and Self-Defense", **Computer Network Attack and International Law, V.76. Naval War College International Law Studies**, Rhode Island, William S. Hein & Co.,Inc., 2002, s.100, **https://www.usnwc.edu/getattachment/95012329-e379-4341-bd1d-a4764c84dd4c/Vol—76——Computer-Network-Attack-and-Internation.aspx** (erişim tarihi 13.1.2013).

DEVELLİOĞLU, Ferit, **Osmanlıca-Türkçe Ansiklopedik Lûgat**, 24. Baskı, Aydın Kitabevi, Ankara, 2007.

Free Dictionary, **http://www.thefreedictionary.com/cyberwar** (erişim tarihi 11.11.2012).

GELLMAN, Barton, "Cyber Attacks by Al Qaeda Feared; Terrorists at Threshold of Using Internet as Tool of Bloodshed, Experts Say", **Washington Post**, 27.6.2002, s.A01, **http://ellen-bomer.com/Osama/Cyber-Attacks.html** (erişim tarihi 10.1.2013).

Government of Canada, 2010, **Canada's Cyber Security Strategy**, **http://www.publicsafety.gc.ca/prg/ns/cybr-scrty/_fl/ccss-scc-eng.pdf** (erişim tarihi 8.11.2012).

GÖZÜBÜYÜK, Abdullah P., Alman, **Fransız, İsviçre ve İtalyan Ceza Kanunlarıyla Mukayeseli, Türk Ceza Kanunu Açıklaması**, Cilt 1, 3. Baskı, Kazancı Yayınevi, Ankara, 1982.

GÜRKAYNAK, Muharrem – İREN, Adem Ali. "Reel Dünyada Sanal Açmaz: Siber Alanda Uluslararası İlişkiler", **Süleyman Demirel Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi**, Yıl 2011, Cilt 16, s.69-273, http://iibf.sdu.edu.tr/dergi/files/2011-2-13.pdf (erişim tarihi 28.02.2012).

HILDRETH, Steven A., **Cyberwarfare,** Congressional Research Service Report for Congress, 19.6.2001, s.CRS-16, **http://www.fas.org/irp/crs/RL30735.pdf** (erişim tarihi 13.1.2012).

HOLLIS, Duncan B, "Why States Need an International Law for Information Operations", **Lewis & Clark Law Review**, 2007, V.11, s.1023-1061.

Information Operations (Joint Publications 3-13), 27.11.2012, s.GL-3, **http://www.dtic.mil/doctrine/new_pubs/jp3_13.pdf** (erişim tarihi 13.1.2013).

KAŞIKÇIOĞLU, Nafi, "Elektronik Harp". **Siber Savunma Sempozyumu**, Askeri Müze ve Kültür Sitesi Komutanlığı, Harbiye, İstanbul, 24-25.5.2011.

KETİZMEN, Muammer, **Türk Ceza Hukukunda Bilişim Suçları,** Ankara Üniversitesi Sosyal Bilimler Enstitüsü Kamu Hukuku Anabilim Dalı Doktora Tezi, Ankara, 2006.

KRASAVIN, Serge, **What is Cyber Terrorism?, http://www.crime-research.org/library/Cyber-terrorism.htm** (erişim tarihi 4.11.2012).

LIBICKI, Martin C., **What is Information Warfare?,** National Defence University, Washington, 1995.

Lisbon Summit Declaration, 20.11.2010, **http://www.nato.int/nato_static/assets/ pdf/pdf_publications/20120207_strategic-concept-2010-tur.pdf** (erişim tarihi 3.1.2013).

Macnillan Dictionary, **http://www.macmillandictionary.com/ dictionary/american/cyberwar** (erişim tarihi 11.11.2012).

MCMILLAN, Robert/KAN, Michael, **China Hacking Video Shows Glimpse of Falun Gong Attack Tool,** 23.8.2011, **http://www.pcworld.com/article/238655/china_hacking_video_shows_glimpse_of_falun_gong_ attack_tool.html** (erişim tarihi 14.1.2013).

NATO Rapid Reaction Team to Fight Cyber Attack, 13.3.2012, http://www.nato.int/cps/en/natolive/news_85161.htm (erişim tarihi 3.1.2013).

Oxford Dictionaries, **http://oxforddictionaries.com/definition/american_english/cyberwar?region=us&q=cyber+war** (erişim tarihi 11.11.2012).

OWENS, William A./DAM, Kenneth W./LIN, Herbert S. (Editörler), **Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities,** National Research Council, Committee on Offensive Information Warfare Computer Science and Telecommunications Board Division on Engineering and Physical Sciences, 2009, **http://www.carlisle.army.mil/DIME/documents/2Cyberattack%20Brochure_FINAL.pdf** (erişim tarihi 11.12.2013).

ÖZDEMİR, Battal, **Zararlı Yazılıma Karşı Korunma Klavuzu**, Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü Doküman Kodu:BGT-1004, Kocaeli, 2007.

ÖZDEMİRCİLİ, Özgür, **Denial of Service Saldırılarının Önlenmesi**, http://www.enderunix.org/docs/dos-saldirilari.pdf (erişim tarihi 12.1.2013).

RID, Thomas, "Cyber War will not Take Place in", **Strategic Studies**, 2012, V.35, I.1, s.5-32.

Russain Federation, 2011, **Conceptual Views Regarding the Activities of the Armed Forces of the Russian Federation in Information Space**, http://pircenter.org/media/content/files/9/13480921870.pdf (erişim tarihi 10.1.2013).

SCHMITT, Michael N. / O'DONNELL, Brian T. (Editörler), **Computer Network Attack and International Law**, V.76, Naval War College International Law Studies, Rhode Island: William S. Hein & Co.,Inc, 2002, **https://www.usnwc.edu/getattachment/95012329-e379-4341-bd1d-a4764c84dd4c/Vol--76--Computer-Network-Attack-and-Internation.aspx** (erişim tarihi 10.1.2013).

SINGEL, Ryan, "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).

Terörizmle Mücadelede Uluslararası İşbirliği ve Tanım Sorunu, Dışişleri Bakanlığı Resmi İnternet sitesi, **http://www.mfa.gov.tr/terorizmle-mucadelede-uluslararasi-isbirligi_-ve-tanim-sorunu-.tr.mfa** (erişim tarihi 12.11.2012).

The White House National Security Strategy, 2010, **http://www.whitehouse.gov/sites/default/files/rss_viewer/national_security_strategy.pdf** (erişim tarihi 11.1.2013).

The UK Cyber Security Strategy: Protecting and Promoting The UK in a Digital World, 2011, **http://www.carlisle.army.mil/dime/documents/UK%20Cyber%20Security%20Strategy.pdf** (erişim tarihi 11.1.2013).

TRAYNOR, Ian, "Russia accused of unleashing cyberwar to disable Estonia", **The Guardian**, http://www.guardian.co.uk/worl d/2007/may/17/topstories3.russia, (erişim tarihi 10.1.2013).

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

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.

United Nations Terms, **http://unterm.un.org/dgaacs/unterm.nsf/WebView/ E996B25EA7D3B36E85256B090056D806?OpenDocument** (erişim tarihi 31.10.2012).

U.S. Department Of Defence, 2011, **Department of Defence Strategy For Operating in Cyberspace**, http://www.defense.gov/news/d20110714cyber.pdf (erişim tarihi 10.1.2013).

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

WINGFIELD, Thomas C., **The Law of Information Conflict: National Security Law in Cyberspace**, Aegis Research Corp., 2000.