SİBER DÜNYA RİSKLERİ VE ALINABİLECEK ÖNLEMLER

Ayşegül Güler[♣]

Özet

Dünyayı örümcek ağı gibi saran sanal ağların oluşturduğu siber alan insanlara büyük kolaylıklar sağlamasının yanında ciddi riskleri de bünyesinde barındırmaktadır. İnsanların teknolojiden yararlanması onların hayatlarını kolaylaştırmanın yanında, belli merkezlerce kontrollerine imkân da tanımaktadır. İnternet üzerinden yapılan her işlem, kullanıcılar hakkında yapılan analizlere veri tabanı oluşturmaktadır. Teknolojiyi elinde bulunduran devletler uluslararası hukuki boşluktan yararlanarak devlet dışı aktörler üzerinden hasımlarına zarar verebilmektedir. Kötü niyetli hackerler ahlaki sorumluluk duymadan insanların bilgilerini kendi amaçları doğrultusunda kullanabilmektedir. Sanal dünyada yapılan bilgi devşirme ve manipüle davranışlarına karşı ise insanların savunma mekanizmaları yetersiz kalmaktadır.

Devletlerarası rekabet de sanal alana kaymış ve rakip görülen tarafın ekonomisinden sağlığa, siyasete ve askeri alanlara kadar bilgileri kısa sürede toplanabilirken zorlayıcı önlemler hayata geçirilebilmektedir. Sanal tehlikelerden korunmanın en garanti yolu, onu kullanmamaktır. Ancak kişiler interneti kullanmasa bile devletler kamu hizmetlerinin büyük bir bölümünü bilişim sistemleri üzerinden yapmakta ve vatandaşlarının bilgilerini bazen koruyamamaktadır. Uluslararası yasaların yetersiz olması ise etkin güçlerce sanal saldırıların baskı unsuru olarak kullanılmasına zemin hazırlamaktadır. Saldırıya uğrayan tarafın meşru müdafaa hakkının bulunup bulunmadığı ise tartışmalıdır. Klasik Birleşmiş Milletler (BM) sisteminin sanal mağdurlara yönelik alacağı önlemlerin yetersiz olacağı düşünüldüğünde, siber suçlarla ilgili uluslararası toplumun ortak bir kavram oluşturması, insanların mahremiyetlerinin korunması ve suçluların cezasız kalmaması için ortak aklın hayata geçirilmesi gerekmektedir. Bu çalışmada kişilerin, kurumların ve devletlerin karşı karşıya kaldığı sanal tehditlerin neler olduğu üzerinde durulacaktır. Sanal alanı kötü niyetle kullananlara karşı, ulusal ve uluslararası alanda alınabilecek önlemler ve devletleri hedef alan saldırılarda meşru müdafaa hakkının kullanılıp kullanılamayacağı incelenecektir.

Anahtar Kelimeler: Siber Alan, Güvenlik, Riskler, BM, Müdahale.

[♣] Dr., Kazım Karabekir Meslek Yüksek Oklu, Karamanoğlu Mehmetbey Üniversitesi. aseguler@gmail.com

*Ayşegül Güler, Öğr. Gör. Dr. Karamanoğlu Mehmetbey Üniversitesi.

Cyber World Risks, Precautions To Be Taken Of People And States

Abstract

The cyber space created by virtual nets that surround the world like a spider web provides great convenience to people and also contains serious risks. Also making their lives easier, people benefit from technology, and they also have the opportunity to control certain centers. Every transaction made on the internet creates a database for the analyzes made about the users. States that have the technology can take advantage of the international legal gaps and damage their opponents over non-state actors. Malicious hackers can use people's knowledge for their own purposes without moral responsibility. The defense mechanisms of people are inadequate against the manipulation and manipulation of information made in the virtual world. The interstate competition has also shifted to the virtual space. The competing side of the economy, health, politics and military information can be gathered in a short time, the compulsory measures can be passed on to the imagination.

The safest way to protect yourself from virtual threats is not to use it. However, even if people do not use the internet, the state sometimes does not protect the information of their citizens when they make a large part of the public services through the information systems. The inadequacy of international laws paves the way for the effective use of virtual attacks as pressure elements. Whether the attacking party has the right to self-defense is controversial. When the classical United Nations system was deemed inadequate for virtual victims, the international community on cybercrime to form a common concept, protection of people's privacy and common mistakes must be made to prevent the criminals from going unpunished. This study will focus on the virtual threats facing people, institutions and governments. Measures that could be taken in the national and international arena against malicious users of the virtual space, and whether the right to self-defense can be used in attacks targeting states will be examined.

Keywords: Cyber Field, Security, Risks, UN, Intervention.

Giriş

Gerçek hayatın gölgesi olmaya başlayan siber uzay gelişmeye açık, hayatımızın her noktasına giren kaçamadığımız bir dünyadır. Dünyada milyonlarca insan bilgisayarın sağladığı kolaylıklardan yararlanmaktadır. Sanal ağ dünyayı örümcek ağı gibi sarmıştır. İnsan eliyle

oluşturulan sistemler insanı dışlama boyutuna gelmiş ve avantajları yanında ciddi riskleri bünyesinde barındıran siber dünya iki yüzü keskin bir kılıca benzetilmektedir.

İletişim teknolojisi ile bilgisayar teknolojisini birbirinden ayırmak imkânsızlaşmıştır. 1957 yılında uzaya yerleştirilen ilk uydu o tarihlerde büyük heyecan uyandırmış insanlık tarihinde önemli bir gelişme olarak değerlendirilmiştir. Günümüzde bu teknoloji sıradanlaşmış uzay, değişik amaçlarla gönderilen sayısız uydularla dolmuştur. Uydular aracılığıyla yapılan işlemler sabit telefonları dinlemekten daha kolay hale gelmiştir. Uydular, bilgisayar komutlarına göre iş görmekte, bilgisayar sistemleri üzerinden her konuda istenilen bilgileri toplayabilmektedir. Bilgisayarlar yapay zeka olarak insanlara büyük hizmetlerde bulunmasına rağmen kendisine hizmet edecek programları yeğlemektedir. Herhangi bir merkezdeki bir bilgisayar ülkenin en ücra köşesindeki bir evin elektrik harcamasını görebilmektedir. Toplumun büyük bir bölümünün yanında taşıdığı cep telefonları, uydu teknolojisi ile çalışmakla birlikte analiz ve taramayı yapan bilgisayarlardır. Ses özellikleri kaydedilen bir şahsın cep telefonu ile yaptığı görüşme neticesinde yeri tespit edilebilmektedir. Konuşulmayan hatta kapalı durumdaki cep telefonlarını izleme imkânı olması elektronik perdeleme sistemlerini de zaman zaman yetersiz kılmaktadır. Telefon firmaları ise insanların para vererek izlenmek istemeyeceklerinden bu gerçeği reddetmektedir.

Tüm bilişim sistemlerini içine alan kişilerin, kurumların ve devletlerin bilgi işlemlerinin hedeflerine güvenilir bir şekilde ulaşmasını sağlayan kaynakları ifade eden siber güvenlik kavramı günümüz dünyasında sıklıkla kullanılan bir kavram olmuştur. Teknik bir konu olan bilgi güvenliği konunun detayını ifade ederken, sosyal bir tanım olan siber güvenlik ise yazılım güvenliği, web güvenliği donanım ve ağ güvenliği gibi farklı alanları içine alan geniş kapsamlı bir kavramdır. Toplumda internet kullanımının yaygınlaşması ile sanal dünyadaki tehlikelere karşı insanlar daha duyarlı olmaya başlamıştır. Kullanıcıların kaydedilen verileri artıkça bilgi güvenliği daha da önemli hale gelmektedir.

Bilişim teknolojisinin tehlikeli olmasının nedeni, onun kötü amaçlar için kullanılmasıdır. Temel görevi bilgiyi işlemek olan bilgisayarlar ne yapmaları gerektiğini söyleyen yazılımlara bağlı olarak işlem yapmakta ancak üreteni kadar performans gösterdiğinden mutlaka bir açığını bulmak mümkün olabilmektedir. İnternete bağlanabilen veya sinyal gönderebilen her cihaz, potansiyel bir tehdit kaynağı olabilmektedir. Virüsler, Truva atları içine gizlenen kurtlar, tuzak kapıları, elektronik sıkışıklık siber saldırılar için alt yapı oluşturmaktadır. Siber

saldırı denildiğinde akla ilk gelen hack kavramı yazılım açıklarını bularak kendisine yarayacak şekilde kullanma davranışıdır. Dijital sistemde bir kapı varsa her iki tarafa da açılma imkânı vardır. Bu da siber alanda ahlaki sorumluluk duymayan saldırganlara, teröristlere ve kötü niyetli kişilere yeni ufuklar açarak yok etme imkânı sunmaktadır. Belli bir konu hakkında dikkat çekmek ve kamuoyu oluşturmak amacıyla faaliyet yürüten hacktivistlik kavramı ise bilişimin iyi amaçlarla kullanılıp kısa sürede geniş kitlelere ulaşma imkânı vermesi, olumlu bir yararlanma şeklidir. Burada üzerinde duracağımız konu ise iletişimi kötü niyetli kullanan sanal dünyanın korsanları, hackerlerdir. Hackerler, siber sistemlere şifre kırma işlemi ile izinsiz sızma işlemlerini gerçekleştirebilen kişi veya kişilerdir ve özel hayatın gizliliğine büyük tehdit oluşturmaktadır. Diğer bir ifadeyle yazılımlara açık bulma mantığı ile yaklaşan kişilerce sistem gerektiğinde içeri girmek için kapı kırılmakta "hack" lenmektedir. Güvenlik önlemleri ise karşılaşılan olgular dikkate alınarak oluşturulmaktadır. Ancak gelişmiş tehditlerin standart güvenlik duvarlarını aşma, kendini gizleme, değerli bilgileri alma konusunda sınır tanımadıkları görülmüştür. Güvenlik altyapısının güçlü olması saldırganlarla mücadele imkânlarını artıracak olmakla birlikte siber suçlarla mücadelenin maliyeti de giderek artmaktadır.

İnternetin sivil alanda kullanılması sanal bir hayatın oluşmasını gündeme getirmiştir. Sosyal medya, vahşi kapitalizm mantığı içinde çok hızlı gelişmekte, etkisinden kaçılamayacak bir ağ oluşmakta ve şahıslar siber dünyadan yararlanırken zararları çoğu kez göz ardı edilebilmektedir. Elektronik haberleşmenin hızı ve ucuzluğu onun yaygınlaşmasını sağlarken, haberleşmeye, güvenliği tehdit eden virüslerin gölgesi düşmektedir. İnternette tıklanan şeyler her bir saniyede 1500-2000 merkezle paylaşılmakta, profilinize yeni sayfalar eklenmektedir. Bu belirsizlik de insanlarda özellerinin ifşa edileceği endişesini artırmakta ve depresyona neden olabilmektedir. Hayatımız hakkında birçok bilgi dijital ortamda saklanmakta, bilgiler sürekli bilgisayarlar arasında gidip gelmektedir. İnterneti kullanan e-posta, haber ve web sayfaları ve sohbet odalarının her biri ardında iz bırakmaktadır. Yapılan aramaların bazı çevreler tarafından takip edildiği düşünülmekte ve insanlar bu veriler kullanılarak yönlendirilebilmektedir. Örneğin Facebook gibi sosyal medya platformlarında kişilerin aramaları yönünde reklamlar çıkmaktadır.

Alınan ve gönderilen bilgilerin şifresinin çözülüp çözülmediğini bilmek her zaman mümkün değildir. Bilgisayar sistemine sızma paranoyası giderek büyümektedir. 2005 yılında ortaya çıkan Facebook kısa sürede neredeyse dünyanın tüm kişisel bilgilerini kendinde toplamayı

başarmıştır. İnsanlar aslında görünür olmak için Facebook kullanmakla birlikte yapay zekâyla şahısların mahremiyeti azalmaktadır. Arka kapı kullanılarak zayıflıklardan yararlanılıp standart güvenlik tedbirlerinin algılamadığı küçük hamlelerle kötü amaçlı yazılımlar marifetiyle kimlik bilgileri çalınıp kötü amaçlarla kullanılabilmektedir. Sıradan insanların vakit geçirmek, eğlenmek, haberdar olmak için kullandığı sosyal ağlar büyük bir silaha dönüşebilmektedir. İnsanlar, verilerin nasıl bir sistem tarafından paylaşıldığının ve öneminin farkında değildir. Ücretsiz e-posta adresi veren bir siteye kaydolurken verilen bilgiler sadece o şirketin eline geçmez çünkü siteler topladıkları bilgileri başka firmalara satabilmektedir. Böylece verilerden eğilimleri belirlenmekte, ticari amaçlar dışında siyaset ve kamuoyu oluşturma faaliyetlerinde kullanılabilmektedir. İnsanlar inanmak istediklerine meyilli olduğundan sosyal medya ağlarıyla duygular manipüle edilerek insanların davranışları etkilenmekte ve yönlendirilebilmektedir. Örneğin 2016'daki Amerika Birleşik Devletleri (ABD) seçimlerine müdahale konusu gizemini korumaktadır. Facebook iddialara göre 50 milyon kullanıcısının bilgilerini satarak 2016 seçim kampanyalarında verilerin kullanılmasına aracılık etmiştir (Sabah Gazetesi, 2018). Yine bir görüşe göre de elde edilen veriler kullanılarak Rusya kontrolündeki 300 trol ordusu ABD seçimlerini etkilemeyi başarmış, Meksikalılar Trump'a yönlendirilirken, siyasiler Clinton yanlısı olarak görüldüğünden sandıktan uzak tutulmaya çalışılmıştır.

Kullandığımız e-devlet sistemi bürokrasiyi azaltıp kişilere çeşitli faydalar sağlamaktaysa da bireyleri saldırıya açık hale getirebilmektedir. Çünkü e-devlet sisteminin yaygınlaştırılması kişilerin izlenmesini kolaylaştırmaktadır. Devletin kişiler hakkında ne kadar bilgi sahibi olması kişilerin zararına olabilir? Bu soruya geniş kapsamlı bir cevap vermek gerekmektedir. Çünkü kişilerin haberi olmadan siyasi eğilimleri gibi kişisel eğilimleri belirlenmekte bu gelişme temel insan haklarından olan özel hayatın gizliliği ve kişisel verilerin korunması haklarını yerle bir edebilmektedir. Bu sebepten sitelerin her seferde bilgileri ne amaçla aldığını belirtmesi ve onaylatması gerekmektedir. Çünkü kişisel bilgilerimizin hangi alanlarda kullanıldığını bilmek hakkımız olsa gerekir.

Konuşulanları çözümleme boyutuna ulaşan bilgisayarlardan doğabilecek kâbus senaryoları ise Türkiye'de henüz görülmek istenmemektedir. 14 Aralık'tan itibaren Türkiye'de bankalara yönelik başlatılan siber saldırıların arkasında Rusya'nın olduğu şüphesi ciddi idi. Ancak böyle bir şüpheye suç isnat edilebilmesi için saldırının devletin talimatı, yönlendirmesi veya kontrolü altında yapıldığının tespiti gerekmektedir (Gümüşbaş, 2016).

Bireyler yaşadığı veya şahit olduğu olaylar nedeniyle tecrübe kazandıysa da sosyal medya insanlığın geleceğini tehdit etmektedir. Şahısların bilgisayarda sakladığı bilgiler üzerindeki kontrolleri sınırlıdır. Yanlış bilgileri düzeltmek kolay değildir. Kişiler, kendilerini güvende hissetmek ve bilgilerinin gizliliğinin korunmasını isterler. Peki, sıradan insanlar siber tehlikelerden korunabilir mi? Korunursa ne kadar korunabilir? Sorularına verebileceğimiz cevap sıradan kullanıcıların tehlikeleri engelleme imkânlarının oldukça sınırlı olduğudur. Tedbirlere rağmen geleneksel yöntemlerle bilgileri korumak mümkün gözükmemektedir. Lisanslı koruma programları bile ancak % 85 koruma sağlayabilmektedir. Dünyada Wikileaks örneği varken siber dünyanın sağladığı özgürlük zaman içinde özel hayat kavramını da yok edecektir.

Şahıslar, bireysel güvenliklerini sağlamak amacıyla ortak ağlardan mümkün olduğunca uzak durmalı, karşılaşılan her linke okuyup incelemeden tıklamamalı, web sayfalarındaki "https" ifadesini kontrol etmelidir. Güvenli erişim kanalları (VPN) kullanılmasına gayret edilmelidir. Kolay kırılamayan şifreler kullanılmalı ve 3-5 ayda bir şifreler değiştirilmelidir. Bilgiler sık sık yedeklenmeli, aynı şifreler değişik platformlarda kullanılmamalıdır. Ortak wi-fi kullanımından kaçınılmalıdır. Toplum medya okuryazarlığı konusunda eğitilmeli ve siteler üzerinde kamuoyu baskısı oluşturulmalıdır. Çünkü verilerin korunması hakkı aslında evrensel bir insan hakkıdır. Ayrıca unutma hakkı, verilerin hangi amaçlarla toplandığını bilme hakkı ve verileri alma hakkı etkin halde hayata geçirilmelidir.

İşlevleri aktif tutması gereken kurumlar açısından konuya yaklaşıldığında, gizli bilgilerin korunması kritik bir öneme sahiptir. Elektronik ağları en çok kullanan ülkeler, siber saldırılara daha fazla maruz kalma riskini taşımaktadır. Her geçen gün virüs bulaşma riski ve güvenlik olayı artmaktadır. Virüs ve saldırılara karşı alınan önlemler aciz kalmaktadır. 21. yüzyılda bilişim teknolojisindeki hızlı değişimler sonucu devletlerarasında yaşanan rekabette savaş yöntemleri değişmiştir. Savaş ağlar üzerinden bilgi alma, zarar verme, kontrol etme gibi yöntemlere yönelmiştir. Teknolojinin gelişmesi saldırıların şahıslar tarafından da yapılmasına imkân sağlamıştır. Saldırının kaynağının tespitinin zor olması devlet destekli de olsa yaptırım uygulanmasını zorlaştırmaktadır (Kaymak, 2017:1).

Siber saldırılar henüz klasik askeri hareketlerin yerini almak için yeterli değildir. Ancak askeri faaliyetleri destekleme kabiliyeti çok yüksektir. Bilgi sistemlerine daha bağımlı olan devletler

ekonomisi daha zayıf bir devlet tarafından büyük zarara uğratılabilir. Konvansiyonel veya nükleer silahların kullanıldığı büyük bir savaş muhtemelen son savaş olacağından devletler devlet dışı aktörler üzerinden yürüttükleri saldırıları siber uzayda tutma isteğindedir (Dikbıyık, 2014:8-10). Kısacası günümüz saldırıları denizden veya havadan yapılmamakta kablolar üzerinden gerçekleşmektedir, yani savaşlar bilgisayarlaşmıştır. Post-modern savaş olgusu kitleleri etkilemek amacıyla sahaya sürülmüştür. Savaş günümüzde silahlı kuvvetlere karşı yürütülen bir eylem olmaktan çıkmış toplumun bütün kesimlerini ilgilendiren her türlü araç kullanılarak yapılan sızma girişimleri ile yürütülmektedir Körfez Savaşı'nda bilgisayarlar etkin olarak kullanılmış, savaş alanından canlı yayınlar yapılarak kuvvetler sevk ve idare edilirken hasım tarafın psikolojisinin yıpratılması amaçlanmıştır. Özetle bilgisayarlar savaş alanında komuta, kontrol, istihbarat ve iletişim amacıyla kullanılmıştır.

Tek kurşun atmadan, kan akıtmadan ülkeleri zaafa uğratmak imkânına sahip olunabileceği mümkün gözükmektedir. Dünya artık bilim temelli bir savaş yaşamakta, ekonomik, siyasi, askeri gibi alanlarda ciddi bir siber mücadele yürütülmekte, korsan fonlar kullanılarak ülkelerin borsaları çökertilebilmektedir. Zaman zaman ülkemizde de karşılaştığımız gibi bir ülkenin kritik merkezlerine, örneğin elektrik santrali veya iletim hatlarına yapılacak bir müdahale ülkelerin ekonomisini bir anda felç edebilmektedir. Finans kuruluşları, hastaneler, enerji kaynakları ilk hedefler arasındadır. Hava ulaşımında kullanılan kontrol kuleleri, borsa bilgisayarları, ATM'ler ve hastaneler sıkça hedef olmaktadır. Firmaların kendilerini siber güvenlik açısından kontrol etmek amacıyla yaptırdıkları sızma testleri birçok kez yetersizlikleri ortaya koymaktadır. Kötü amaçlı kullanımları önlemenin yolu yine siber güvenlikçilerin yazışmaları izlemesinden geçmektedir. Verilere ulaşmak inanılmaz zaman ve para tasarrufu sağlamaktadır. Devletler yazılımlarda açık kapı bırakılmasında ısrarcı davranmaktadır. Bilgisayar sistemleri ABD kaynaklıdır ve tüm dünyadaki bilgileri denetleme imkânı vardır. Microsoft'un ABD çıkarlarını korumak adına yazılımlarda arka kapı bıraktığı yaygın bir kanaattir. Terör faaliyetleri siber alanda yapılırken bazı devletler siber terör gerekçesiyle dünyayı kontrol etme gayretindedir. Dünya üzerinde çıkacak muhtemel bir savaşta ilk mermiyi kimin atacağı bilinmemekle birlikte saldırıların internet üzerinden yapılacağını ifade etmek kehanet olmasa gerekir. Hükümetler, ülkelerindeki internet trafiğini güvenlik gerekçesiyle izlese de bu alan istismara açık bir alandır. Her halükarda özel hayat denetim altındadır.

Siber tehdit ortamı değiştikçe tedbirler de değişmek zorundadır. Bilgi ve iletişim teknolojisindeki gelişmeler yakından takip edilmelidir. Tecrübeler ışığında üst bir güvenlik ağı oluşturulmalı ve sürekli güncellenmelidir. Personelin siber saldırılara karşı gerekli bilgilerle donatılması gerekmektedir. Stratejik alt yapı (enerji, eğitim, ulaştırma vb.) alanlarında zaaflar belirlenip tedbirler alınmalıdır.
Siber saldırılarda bir devlet diğer devletlere karşı bilgi sistemleri üzerinde oluşturacağı etki ile üstünlük sağlamayı amaçlamaktadır (Dikbıyık, 2014:8-10).Örneğin ABD'de birçok bilgisayarın Kosova müdahalesi sırasında Çin kaynaklı saldırıya uğraması engellenememiş ve Çin'in Belgrad büyükelçiliği 9 Mayıs 1999'da ABD hava kuvvetlerince vurularak uyarılmıştır.

Devletler siber saldırılara ne kadar hazırlıklıdır? Bu soruya net bir cevap verebilmek mümkün gözükmemektedir. Çünkü tedbirler tehdidin tanınmasından sonra oluşturulduğu için siber korsanlar devletleri de aciz bırakabilmektedir. Elde edilen bilgiler illegal amaçlarla kullanılabilmektedir. Bu yüzden modern ülkelerin savunma sistemleri bilgisayar ağını zorunlu kılmaktadır. Siber mücadeleye karşı ülkeler kendi siber ordularını oluşturmakta ve kendi yazılımlarını üretmeye çalışmaktadır.

Devletleri tehdit etmeye başlayınca bilinir hale gelmeye başlayan siber saldırıların doğrudan devletleri ve insanlığı hedef alması doğacak sonuçların vahameti, konunun uluslararası hukuk açısından ciddi şekilde ele alınmasını gerektirmektedir (Kaymak, 2017:1). Siber saldırı: düşman olarak kabul edilen merkezlerin bilgisayar sistemlerini ve buradan geçen bilgileri bozmak, yanıltmak ortadan kaldırmak için yapılan hareketler olmasına rağmen uluslararası alanda bir metin üzerinde uzlaşma sağlanan bir kavram değildir. Birleşmiş Milletler (BM) 3814 sayılı kararın 1. maddesi saldırıyı "Saldırı, bir devletin diğer bir devletin egemenliğine, ülke bütünlüğüne veya siyasi bağımsızlığına karşı veya işbu tanımda belirtildiği üzere, Birleşmiş Milletler Antlaşması ile bağdaşmayan diğer herhangi bir tarzda silahlı kuvvet kullanılması" (3814 sayılı karar BM Enformasyon Merkezi) olarak tanımlanmaktadır. Bu tanım siber saldırıların silahlı saldırı kabul edilip edilemeyeceğine açıklık getirmemektedir. Silahlı saldırı, kuvvet kullanımıdır. Ancak her kuvvet kullanımı silahlı saldırı değildir. Uluslararası sistem devletleri esas aldığından siber saldırıların BM Antlaşmasının 2/4. maddesinde açıklanan saldırmazlık ilkesini ihlal edip etmediği tartışmalı hale gelmektedir. 2/4. maddesi "Tüm üyeler, uluslararası ilişkilerinde gerek herhangi bir başka devletin toprak bütünlüğüne ya da siyasal bağımsızlığa karşı, gerek Birleşmiş Miletlerin amaçları ile

bağdaşmayacak herhangi bir biçimde kuvvet kullanma tehdidine ya da kuvvet kullanılmasına başvurmaktan kaçınırlar" ifadesini taşımaktadır. Bu hükümler saldırıya uğrayan tarafa müdahale için bir meşruiyet sağlar mı? 51. maddede belirtilen meşru müdafaa veya BM Güvenlik Konseyi kararı ile kuvvet kullanma istisnası, silahlı saldırı olması durumunda meşru müdafaa hakkını vermektedir (BM Antlaşması). Siber saldırılar insan kayıpları ve büyük maddi kayıplar oluşturmuşsa meşru müdafaa hakkı doğabilmekte, can kaybı olmadığı durumda siber saldırılar kuvvet kullanımı olarak değerlendirilmemekte ve meşru müdafaa hakkı doğmamaktadır.

Siber saldırılar bu kapsamda değerlendirilebilir mi konusu tartışmalıdır. Saldırıya uğrayan tarafın konuyu Güvenlik Konseyine götürmesi halinde alınacak tedbirleri içeren 41 ve 42. maddelerin siber saldırıları engellemeyeceği de aşikârdır. Siber saldırılar konusunda en ciddi çalışma NATO'nun ortaya koyduğu Tallinn Siber Saldırı Kılavuzu'nda devletlerin iç işlerine müdahale, seçim sonuçların manipüle etme, bir hacker grubunun desteklenmesi, bu türden suçlardır (Gümüşbaş, 2016). Bir devletin siber saldırıya uğraması halinde saldırının bir devlet tarafından yapıldığının ve saldırıya uğrayanın devlet olması şartı oluşursa meşru müdafaa hakkının doğacağı Tallinn uzmanlarınca ileri sürülmektedir. Ancak siber saldırıların kaynağını bulmak ve misillemenin caydırıcılığını önceden bilmek kolay değildir (Dikbıyık, 2014:7). Günümüze kadar devletlerarasında gerçekleşen siber operasyonlar siber saldırı boyutuna ulaşmamış kabul edildiğinden meşru müdafaa hakkı da doğurmamıştır (Gümüşbaş, 2016). 11 Eylül sonrası yürürlüğe konulan Bush Doktrini olarak bilinen ABD strateji belgesi meşru müdafaaya yeni bir boyut getirdiyse de henüz siber saldırılar açısından hayata geçirilmemiştir.

Siber saldırılar kontrollü yapılma imkânı vermektedir. Hedef sistemlere küçük hamlelerle zarar verilebileceği gibi hedefin bütün kritik altyapı sistemlerini bir anda felce uğratması da mümkündür. Ancak küçük seviyede yapılan saldırılar, açıkların görülüp kapatılması konusunda yardımcı da olabilir (Dikbıyık, 2014:11-32). Devletlerin altyapıları ve desteği olmadan büyük saldırılar gerçekleştirilemeyeceği bilinmesine rağmen saldırıları kimse üstlenmemekte, bir grup kendisini ifşa ederek konu kapanmaktadır. Ayrıca İran nükleer tesislerine karşı kullanılan Stuxnet virüsü dışında devletlerin saldırı amaçlı kullandığı bir yazılım da literatüre girmemiştir (Kaymak, 2017:4). NATO uzmanları, zararın ciddi boyutta olmadığı için bunların "silahlı saldırı" sayılamayacağı görüşünü açıklamıştır. Yine de Stuxnet

adlı siber saldırı, bunun devletler seviyesinde hukuki boyutunun belirlenmesinin gerekliliğini ortaya koymaktadır (Tuğal, 2016).

Kısacası siber suçlarla ilgili yasal altyapılar yetersiz kalmaktadır. Bilgisayar ağları ve donanımları üzerinden işlenen suçlar siber suç olarak kabul görmekle birlikte uluslararası hukukta hangi eylemlerin siber saldırı suçu olarak kabul edileceği açıkça belirlenmemiştir. Avrupa Konseyince siber suçlarla ilgili 2001 yılında hazırlanan sözleşme 2003 yılında tarafların onayıyla yürürlüğe giren Siber Suç Sözleşmesinde "yetkisiz erişim, sisteme ve veriye müdahale, bilişim sistemi aracılığıyla sahtekârlık veya dolandırıcılık" suçlarıyla sınırlı tutulmuştur (Tuğal, 2016). Günümüz hukuk ilkeleri, devleti esas almaktadır. Yani uluslararası kişi ve kurumlar sorumlu tutulamamaktadır. Sorumlular tespit edilemediği için saldırılar cezasız kalmaktadır. Bu yüzden ulusal ve uluslararası hukukun düzenlenmesi ve güncellenmesi gerekmektedir. Siber suçlara karşı oluşturulan kişisel verilerin korunmasına yönelik düzenlemeler sık sık güncellenmediğinden yetersiz kalmaktadır. Siber suç, saldırı, casusluk gibi terminolojinin gelişmesine paralel olarak değişen eylemlere karşı ulusal ve uluslararası hukukun gerekli düzenlemeleri yapması ve sık sık güncellenmesi gerekmektedir.

Kaynakça

Birleşmiş Milletler Antlaşması, https://www.tbmm.gov.tr/komisyon/insanhaklari/pdf01/3-30.pdf, (Erişim Tarihi: 10.03.*2018*).

BM Enformasyon Merkezi UNIC-Ankara Saldırı'nın (Tecavüzün) Tanımı: Birleşmiş Milletler Genel Kurulu'nun 3814 (XXIX) Sayılı ve 1974 Tarihli Kararı, http://www.unicankara.org.tr/doc_pdf/3814.pdf, (Erişim Tarihi: 09.04.2018).

Dikbıyık, F. (2014). "Stratejik ve Operasyonel Siber Savaş" s:1-35 Siber Caydırıcılık. SG507SiberSavaşlarGüz2014, http://docplayer.biz.tr/14265180-Siber-caydiricilik-sg-507siber-savaslar-guz-2014-yrd-doc-dr-ferhat-dikbiyik.html, (Erişim Tarihi: 12.03.2018).

Gümüşbaş, A. (2016). Uluslararası Hukuk Açısından Türkiye Siber Saldırılara Karşı Ne Yapabilir? https://siberbulten.com/makale-analiz/uluslararasi-hukuk-acisindan-turkiye-siber-saldirilara-karsi-ne-yapabilir/, (Erişim Tarihi: 23.04.2018).

Kaymak, O. (2017). Siber Harekâtlar Ve Uluslararası Hukukta Meşru Müdafaa Hakkı, http://www.ilimvemedeniyet.com/siber-harekatlar-ve-uluslararasi-hukukta-mesru-mudafaa-hakki.html, (Erişim Tarihi:13.03.2018).

Sabah Gazetesi, 21.03.2018, "Yine Facebook (/haberleri/facebook) Yine Skandal!.

Tuğal T., Ş., (2016). Siber Güvenlik Savaş Casusluğun Hukuki Boyutu, http://www.itnetwork.com.tr/siber-guvenlik-savas-casuslugun-hukuki-boyutu/, (Erişim Tarihi: 23.04.2018).