AJIT-e Academic Journal of Information Technology
10.5824/ajite.2022.04.004.x

2022 . Fall - Güz . Volume – Cilt: 13 . Issue – Sayı: 51

Siber Savaşta Mütekabiliyet

Mustafa Veysel GÜLDOĞAN, *Marmara Üniversitesi, Sosyal Bilimler Enstitüsü, Dr., mvguldogan@hotmail.com, 0000-0002-1381-5319*

Şevki IŞIKLI, *Marmara Üniversitesi, İletişim Fakültesi, Doç. Dr., sevki.isikli@marmara.edu.tr, 0000-0002-8075-9177*

ÖZ

Yirminci yüzyılda hızla gelişen yarı iletken teknolojilerin gündelik hayatımıza hızlı bir şekilde entegre olması, bilginin işlenmesi ve yönetiminde kullanılan altyapı değişikliklerini de beraberinde getirmiştir. Bilişim dünyasında gözlemlenen hızlı dönüşümler ve bu dönüşümlerin dünyaya sunduğu yenilikler, bilişim olarak isimlendirilen yeni bir kavramın ortaya çıkmasına neden olmuştur. Bilişim dünyasında yaşanan gelişmelerin sonucunda toplumun bilgi ve iletişim teknolojilerini kullanım amaçları çeşitlenmiştir. İnternet ve teknolojik gelişmenin sunduğu bu imkânlar doğrultusunda oluşan, zaman ve mekân sınırlaması olmayan bu sanal dünyaya siber uzay denilmektedir. Küreselleşme ve hızlı teknolojinin beraberinde getirdiği zaman ve mekân kısıtlamasının olmadığı siber uzayda iletişim kolaylığı güvenlik açısından önemli açıkların oluşmasına neden olmakta, siber tehditler ve saldırılara neden olmaktadır. Siber tehditler ve saldırılar, fiziksel altyapı veya internet ağları üzerinden kontrol sistemlerine yapılabilmektedir. Siber saldırılar ülkelerin birbiri arasında olabileceği gibi; bireyler, terör örgütleri veya aktivist örgütlenmelerin terör saldırıları şeklinde de gerçekleşebilmektedir. Ancak her siber saldırı faaliyeti karşısında mütekabiliyet esasına uygun şekilde yanıt vermek mümkün olmayabilir. Bu noktada uluslararası diplomatik arenada maruz kalınan davranışa yönelik benzer yönde karşılık verme esası olarak tanımlanan mütekabiliyet kavramının siber uzayda nasıl karşılık bulacağına dair soru işaretleri ortaya çıkmaktadır. Bu çalışmada ise siber uzay, siber saldırı ve siber savaş kavramları bağlamında siber saldırıların tespit edilmesi ve sorumlulukların isnat edilmesi üzerine genel bir değerlendirme yapılmakta, daha sonra ise siber tehdit ve siber savaş sırasında uygulanması gereken mütekabiliyet esası temel alınarak siber saldırılara nasıl mukabele edileceği ile ilgili tartışmalara yer verilmektedir.

Anahtar Kelimeler **:** Siber Savaş, Mütekabiliyet, Uluslararası Siber İlişkiler, Siber Suçlar, Dijital Hukuk

Araştırma Makalesi / Research Article
Date Received: 1.11.2022
Publishing Date: 30.11.2022

Reciprocity in Cyber War

ABSTRACT *The rapid integration of semiconductor technologies, which developed rapidly in the twentieth century, into our daily lives has brought about infrastructure changes used in the processing and management of information. The rapid developments in information and communication technologies and the innovations these developments offer to the world have led to the emergence of a new concept called informatics. As a result of the developments in the world of informatics, the society's use of information and communication technologies has diversified. This virtual world, which is formed in line with these opportunities offered by the internet and technological development, and has no time and space limitations, is called cyberspace. Ease of communication in cyberspace, where there is no time and space restriction brought about by globalization and fast technology, causes important security gaps and cyber threats and attacks. Cyber threats and attacks can be made against physical infrastructure or control systems over internet networks. Cyber attacks can occur between countries, as well as in the form of terrorist attacks by individuals, terrorist organizations or activist organizations. However, it may not be possible to respond in accordance with the principle of reciprocity in the face of every cyber attack activity. At this point, questions arise about how the concept of reciprocity, which is defined as the principle of responding in a similar way towards the behavior exposed in the international diplomatic arena, will find a response in cyberspace. In this study, a general evaluation is made on the detection of cyber attacks and attribution of responsibilities in the context of the concepts of cyber space, cyber attack and cyber warfare, and then there is a discussion on how to respond to cyber attacks based on the principle of reciprocity that should be applied during cyber threat and cyber warfare.*

Keywords **:** *Cyber War, Reciprocity, International Cyber Relations, Cybercrime, Digital Law*

GİRİŞ

Yirminci yüzyılda hızla gelişen yarı iletken teknolojilerin günlük hayat pratiklerine olabildiğince çabuk entegre olması, bilgisayar sistemleri ve internet ağlarının birbiri ile bütünleşik şekilde çalışarak bilginin hızlı bir şekilde yayılımını sağlayan bilişim teknolojileri kavramının ortaya çıkmasını sağlamıştır. Bilginin hızlı iletimi için elektromanyetik spektrum ve internet temelli ağ sistemlerinin kullanıldığı bu bilişim alanına siber uzay da denilmektedir. Bilişim teknolojileri, çağdaş toplumun iletişim şekillerinin belirlenmesinde etkin rol almaktadır ve bireyler günlük yaşamlarında bu teknolojilerin sağladığı olanaklar ile siber ortam adı verilen yeni bir iletişim dünyasını kullanmaya başlamıştır.

Ulusal bilgi güvenliğinden bahsedilirken, sadece devletin ulusal çıkarları doğrultusunda oluşturulan bilgiler değil; daha geniş anlamda her türlü ticari bilginin korunması da anlaşılmaktadır. Siber ortamda oluşabilecek tehditler, ülke güvenliğinin temelini oluşturan askerî, siyasi ve ekonomik boyutlara yönelik olarak gerçekleştirilmektedir. Asimetrik savaş çeşidi olarak değerlendirilen siber savaşlar,

10.5824/ajite.2022.04.004.x

günümüzde hem klasik savaşlara takviye olarak hem de tek başına bir savaş yöntemi olarak uygulanabilmektedir.

Siber savaşların askerî hedefi genelde ülkelerin kritik bilgi işlem tesisleridir. Siber teröristler; ülkelerin bilişim sistemlerinin baraj kapaklarını açabilir, hava trafik kontrol sistemlerini ele geçirerek uçakların kaza yapmasını sağlayabilir, gıda fabrikalarının otomasyon sistemlerine sızarak gıda formüllerini değiştirip kitlesel ölümlere yol açabilirler. Siber saldırılar; kamu düzenini doğrudan etkiledikleri, klasik bir terör eylemine benzer şekilde korku ve dehşet ortamı oluşturabildikleri, toplumsal yaşamı bir anda felç edebildikleri için ciddi bir ulusal güvenlik sorunu hâline gelmiştir.

Siber risk ve tehditlerin bu tarz asimetrik karakterleri, siber tehditlerle mücadeleyi zorlaştırmaktadır. Hem siber saldırıların yol açtığı ekonomik kayıplar hem de siber saldırıları önlemek için yapılan yatırımların maliyetleri artmaktadır. Yine de siber güvenliğin mutlak olarak sağlanmış olduğundan bahsedilememektedir. Siber güvenlik risklerinin ancak üstesinden gelinebilir ve kabul edilebilir düzeyde tutmanın imkânı ve saldırı durumunda mütekabiliyet ilkesinin nasıl uygulanabileceği tartışılmaktadır. Ancak her siber saldırı faaliyeti karşısında mütekabiliyet esasına uygun şekilde yanıt vermek mümkün olmaz. Uluslararası diplomaside *tarafların maruz kaldıkları davranışa benzer veya denk bir karşılık verme hakkı* olarak tanımlanan mütekabiliyet ilkesinin siber saldırılarda nasıl uygulanabileceği, tartışmaya açık bir sorudur.

Bu çalışmada, ülkeler arasında gerçekleşebilecek siber tehdit veya siber savaş esnasında uygulanması gereken güvenlik stratejileri, mütekabiliyet esasları temel alınarak analitik bir yaklaşımla değerlendirilmiştir.

1. SİBER ORTAMDAKİ TEHDİT VE KAVRAMLAR BAĞLAMINDA SİBER GÜVENLİK

1.1. Siber Uzay (Siber Ortam) ve Siber Saldırı Kavramları

Teknolojide yaşanan hızlı gelişmeler, bilginin fiziksel dünyadan internet tabanlı sanal dünyaya doğru hızlı bir şekilde taşınmasına neden olmuştur. İnternet tabanlı bu sanal dünyaya siber uzay veya siber ortam da denilmektedir. Sibernetik kelimesinin ön eki olan Siber, bu kelimenin kısaltılmış hâli olarak da kullanılmaktadır (Ada, 2018).

En temel şekliyle ifade edilmek istenildiğinde siber kelimesi bilgisayar ve bilgisayarla çalışabilen sistemlerin olduğu alan; bilişim de bu alandan aktif bir şekilde faydalanarak bilgi üretilmesi, değerlendirilmesi ve aktarılması anlamına gelmektedir. Siber uzay (cyberspace) kavramının literatürde ilk olarak William Gibson'ın *Neuromancer* adlı eserinde kullanıldığı ifade edilebilir (Akyeşilmen, 2016).

ABD Savunma Bakanlığı siber uzay kavramını, web tabanlı ağlar, çevre birimleri ve gömülü işlemcileri içeren teknolojileri altyapılı sistemlerin kullanılması ile enformasyonun küresel anlamda paylaşıldığı alan olarak tanımlamaktadır.*

Siber ortamda zaman ve mekân kavramının olmayışı, coğrafi sınırlar boyutunda uluslararası ilişkiler içinde potansiyel tehditler oluşturmaktadır. Bununla birlikte bilişim sistemleri konusunda uzman bir kişi, dünyanın herhangi bir yerinden ve herhangi bir zaman aralığında mevcut ağ sistemlerine bağlanarak siber saldırı gerçekleştirebilme potansiyeline sahiptir (Auerswald 2004: 631-662). Bu nedenle ülkeler kritik derecede önemli iletişim sistemlerini dışardan ulaşıma kesmeye çalışsalar da zaman zaman zorluklar yaşamaktadırlar. Bu durum, siber saldırıların oluşması için uygun bir ortam hazırlamaktadır.

Bilgisayar tabanlı bilgi-işlem ve iletişim sistemlerine maddi ve manevi amaçlı zarar vermek amacı ile yapılan bu saldırı türüne *siber saldırı* adı verilmektedir. Siber saldırılar, **hacker** adı verilen bireyler veya birden fazla kişiyi içeren gruplar tarafından yapılabileceği gibi, terör örgütleri ve devletlerin kendileri tarafından da yapılabilmektedir. Kim tarafından yapılırsa yapılsın siber saldırılar; virüslü elektronik posta ekleri, kamu hizmetlerinin kontrolünde kullanılan bilgisayar sistemlerinin aşırı yüklenmesini sağlayarak hizmet engellenmesi, ülke veya ticari kuruluşlara ait web sayfalarının çalışmaz hâle getirilmesi veya bilgisayar sistemlerine yetki dışı giriş yapılarak kişisel verilerin elde edilmesi şeklinde yapılabilmektedir (Başaranoğlu, 2016).

Siber saldırılar, verilere doğrudan erişim veya kontrol sistemlerinin engellenmesi yolu gibi farklı şekillerde gerçekleştirilebilmektedir. Bilginin yetkisiz olarak elde edilmesi ya da çalınması, verilere doğrudan erişime yönelik olarak yapılan siber saldırı faaliyetleri olarak gösterilmektedir (Bayraktar 2015). Bir alt yapının bilinçli olarak bozulması ve kullanılamaz hâle gelmesi ise kontrol sistemlerine yönelik siber saldırı yöntemi olarak bilinmektedir. Siber saldırılar, faaliyet nitelikleri ve motivasyon farklılıklarına göre **siber suç, siber terörizm ve siber savaş** gibi farklı isimlerle ifade edilebilmektedir (Berner, 2003). Öte yandan Buna göre siber ortamda kişisel ve kurumsal bilgilere illegal yollar kullanılarak ulaşmak sureti ile tahrip niteliği taşıyan **siber saldırı** veya saldırı girişimine **siber tehdit** adı verilmektedir (Bıçakçı, 2012).

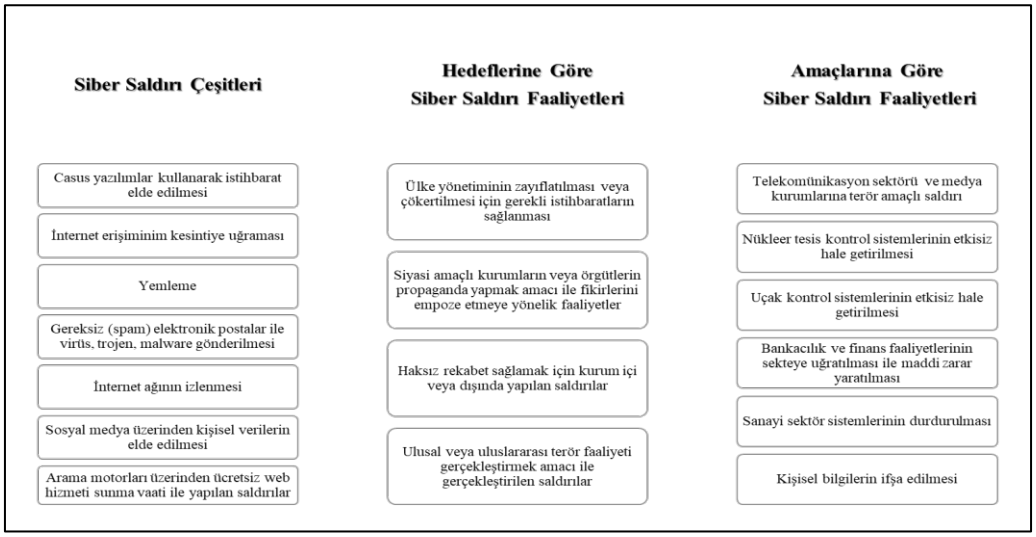
Sonuç olarak bilişim teknolojilerinin hızlı gelişimi devlet ve devlet dışı aktörler için yeni güvenlik sorunlarının doğmasına neden olmuştur. Siber tehditlerin sanal ortam üzerinden gerçekleştirilmesi, eylemi gerçekleştirenin tespit edilebilmesi için öngörülmez bir durum oluşturmaktadır (Bıçakçı 2014, ss. 100-130). Ayrıca siber tehditlerin belirli bir merkezden gerçekleştirilmemesi de siber güvenlik endişelerini arttırmaktadır.

*Bkz: https://csrc.nist.gov/CSRC/media/Projects/ISPAB/documents/DOD-Strategy-for-Operating-in-Cyberspace.pdf

10.5824/ajite.2022.04.004.x

1.2. Siber Saldırı Türleri

Siber tehditler ve saldırılar, fiziksel altyapıya yönelik olarak internet ağları üzerinden kontrol sistemlerine yapılabilmektedir. Siber tehdit amaçlı aktivasyon göstermek isteyen kişi ya da gruplar faaliyetleri ve saldırı nedenlerine göre farklı hedefleri isabet alabilmektedir. Bu bağlamda saldırı çeşidine, hedefe ve amaçlarına göre siber saldırı türlerini farklı şekillerde sınıflandırmak mümkündür.



Şekil 1: Siber Saldırı Çeşitleri, Hedeflerine ve Amaçlarına Göre Siber Saldırı Faaliyetleri

Belirtilen siber saldırılar dünyanın herhangi bir bölgesinde web tabanlı sistemler aracılığı ile gerçekleştirilebilmektedir (Chen, Walsh 2009). Bu sebeple bireylerin, ülkelerin ve ülkeler arası ilişkilerin siber zararlardan korunabilmesi için hem ulusal hem de uluslararası güvenlik stratejileri geliştirmeleri gerekmektedir (Choucri 2012).

Burada önem arz eden bazı kavramların açıklanması gerekmektedir. Üzerinde durulması gereken ilk husus **hacker** kavramıdır. Hacker, siber ortamda bilgisayar ağlarına yönelik saldırı gerçekleştiren birey olabileceği gibi birtakım organizasyonlar da olabilmektedir. Bununla birlikte, literatürde siber saldırıları yapanların genellikle hacker olarak adlandırıldığı da söylenebilir. Hackerlar kendi aralarında özelliklerine göre siyah, gri ve beyaz şapkalı hackerler hatta kimi zaman mavi ve kırmızı şapkalı hackerler olarak nitelendirilmektedir. *Siyah şapkalı hackerlar*, kötü niyetle ağ altyapılarına ve bilgisayarlara sızarak, kişisel ve kurumsal bilgileri ele geçirerek bu bilgilere zarar verme ya da yok etme niyeti taşıyabilirler. *Gri şapkalı hackerlar*, daha ziyade merak ve ego tatmini nedeni ile sistemlere sızarlar. Bunların amacı siyah şapkalılar kadar kötü olmamakla birlikte etik açıdan beyaz şapkalılar kadar güçlü değillerdir. İyi niyet taşıyarak buldukları sistem açıklarını ağ sahibine bildiren ya da tamir etmeye yardımcı olanlar ise *beyaz şapkalı hackerlar* olarak adlandırılmaktadır. Siber uzayın muhafızları olarak da nitelendirilebilecek olan bu

gruptaki hackerler, tıpkı siyah şapkalı hackerların sistemlere giriş yöntemlerini kullandıkları gibi hareket ederler. Ancak bunların amacı sistemlere zarar vermek değildir. Kötü niyetli hackerların kullandıkları yol, yöntem ve teknikleri iyi bilen beyaz şapkalı hackerler daha çok sistemdeki açıkları belirlemek ve korumak peşindedirler.

Bir nevi biyolojik virüs tarzında çalışan siber kaynaklı **virüsler**, üzerinde durulması gereken bir diğer konudur. Virüsler belli bir program dâhilinde ve içlerine sızdıkları yapıda kendilerini kopyalayarak çoğalan zararlı yazılımlar olarak tanımlanabilir. Virüsler, en tehlikeli ve ilk zararlı yazılımlar olarak da bilinmektedir. Virüsler yayılma eğilimi gösterirler ve yayılmak için bir taşıyıcıya ihtiyaç duyarlar. Virüsler bilgisayarı takip etme, şifre çalma veya reklam gösterme faaliyetleri ile sistemi tamamen kullanılamaz hâle getirebilmektedir. Örneğin 1999 yılında dünya çapında bilgisayarlara sızan *Melissa virüsü*, önemli siber saldırı faaliyetlerden birisidir. Davis Smith tarafından kötücül yazılımlar aracılığı ile yayılan virüs, o dönemde 80 milyon dolarlık zarara neden olmuştur (Garber, 1999, s. 17).

Üzerinde durulması gereken bir başka konu **Hizmeti Engelleme Saldırısı (DDoS Saldırıları)** konusudur. Bilgisayar sistemlerinin, ağlarının ve dağıtıcı servislerin bant genişlikleri, belli bir kapasitede isteğe yanıt verecek şekilde oluşturulmuştur. DDoS saldırısı; hedef kullanıcı kitlesinin web kaynağına, adına köle bilgisayarlar da denilen zombi ve botnetler kullanılarak birden çok istek gönderme yoluyla web sitesinin işleme kapasitesinin üstündeki isteği göndererek stabil çalışmasını engellemeyi amaçlamaktadır. Bu saldırı tipine de örnek olarak 2007 yılındaki Estonya'ya yönelik siber saldırı verilebilir. Bunların dışında Truva atı (kendisi zararı olmayan fakat genellikle bilgi çalma amaçlı yazılımlar), klavye takipçisi, fidye yazılımlar, reklam yazılımlar, casus yazılımlar gibi yaygın saldırılardan bahsetmek de mümkündür.

1.3. Siber Saldırı Örnekleri

Bu çalışmada temel olarak ülkeler arasında mütekabiliyet usulü yeni güvenlik anlayışı ele alındığı için örnek olarak ülkeler arasında gerçekleşen siber saldırı ve siber savaş örneklerinden bahsedilmiştir.

Uluslararası ilişkilerde etkin olan ilk siber saldırılardan birisi **Estonya'ya yönelik DDoS saldırısıdır**. Bu alandaki en bilindik olay olma özelliğini taşıyan 2007 yılında siyasi amaçlar ile gerçekleştirilen Estonya saldırısıdır [M.1][MVG2](Kozłowski, 2020). Rus gizli servisinin ve siber operasyon elemanlarının siyasi amaçlarla yaptıkları düşünülen saldırıda devlet başkanlığı ve parlamentonun web siteleri, birçok kamu bankası, haberleşme ve iletişim kuruluşları etkilenmiştir. Yapılan bu siber saldırılarda [M.3][MVG4]bilgisayarlar ve bilgisayar sistemlerini hedef kullanıcı kitlesinin kullanmasını engellemek için DDOS yöntemi kullanılmıştır. Böylelikle söz konusu kurumların siteleri çalışamaz hâle getirilmiş ve ülke içinde birçok sosyal hizmet durma noktasına gelmiştir. Estonya siber saldırısı, siber güvenlik literatüründe önemli bir yer edinmiştir. Bugün siber saldırılara ve çatışmalara yönelik politik

veya akademik çerçevede siber güvenlik çalışmalarında bu saldırının önemli bir yer kaplaması, bunun bir göstergesi olarak ifade edilebilir. Bu saldırının aynı zamanda uluslararası arenada da büyük bir etkisi olmuştur. Öyle ki saldırı sonrasında NATO, 2008 yılında Bükreş'te bir zirve gerçekleştirmiş, bu zirvede alınan kararlara göre, NATO Siber Savunma Yönetimi Otoritesi'nin ve Estonya Tallinn merkezli bir NATO Siber Savunma İş Birliği Mükemmeliyet Merkezi kurulması kararlaştırılmıştır. Bu siber saldırı, uluslararası ilişkilerde siber güvenliğin ilk alarm zilini çaldırarak uzun ve derin etki yaratan önemli saldırılar arasında yerini almıştır.

Siber saldırıların ne denli ciddi sonuçlar yaratabileceğinin önemli bir örneği de **Sibirya Doğalgaz patlamasıdır.** Siber teknolojiler kullanarak gerçekleştirilen ilk saldırı, 1982 yılında Sibirya Doğalgaz Boru Hatları hedef alınarak gerçekleştirilmiştir (Çakmak ve Demir 2009). ABD'nin Sovyet Rusya yönetimine ambargo uyguladığı dönemde, Sovyetler Birliği yönetimi ambargoyu aşmak için Kanada'da bulunan bir şirketin doğalgaz boru hattını kontrol eden programı ele geçirmeye çalışmış ancak bunu fark eden CIA (ABD'nin Merkezi Haber Alma Örgütü) bahsi geçen yazılımın içine akıllı bomba adı verilen kötü huylu bir yazılım entegre etmiştir. Amerikalılar, yazılımın Ruslar tarafından çalındığını anlamalarına rağmen operasyonun devam etmesine izin vererek yazılıma virüs entegre etmiş ve söz konusu yazılım bir süre sonra bozularak borunun patlamasına sebep olmuştur (Sertçelik, 2015, s. 31). Bu olay, savaşların artık beşinci boyut olarak siber alanda gerçekleşeceğine ve teknolojide üstün olan ülkelerin üstünlük kuracağına önemli bir örnek teşkil etmektedir (Çavuş 2008).

Yine **Ay Işığı Labirenti** olarak adlandırılan siber saldırı ABD'nin askerî (Pentagon), altyapı (enerji) ve uzay (NASA) gibi ülke güvenliğinin sağlanmasında kritik önem taşıyan sistemlerine yönelik olarak gerçekleştirilmiştir. Saldırı; askerî haritalar, askerî tesisler ve Ar-Ge projeleri gibi devlet sırlarını içeren verilerin çalınması ile sonuçlanmıştır (Çelik 2018: 110-119). Araştırmalar sonucunda saldırıyı Rusya'nın gerçekleştirdiği tespit edilmiştir. Saldırının tespit edilmesi iki yılı aşkın bir süre almıştır (Çeliktaş 2016). Saldırı 1996 yılında başlamış fakat ABD bu saldırıyı ancak 1998 yılında tespit edebilmiştir. Bu siber saldırı, ABD gibi teknolojide ileri devletlerin dahi ağır siber saldırılara uğrayabileceğini göstermektedir (Çiftçi, 2013).

Bir başka örnek ise **Kosova Krizi'dir.** 1990'lı yıllarda Yugoslavya'da yaşanan iç savaş ve özellikle sivillere karşı yapılan katliamlar dünya kamuoyunun tepkisine neden olmuş, bu tepkilerin artmasıyla ve yapılan katliamların soykırım boyutuna ulaşmasını engellemek amacıyla NATO üyesi ülkeler bölgeye müdahale etmek zorunda kalmıştır. Yapılan askerî müdahalelere karşılık olarak hackerler NATO'nun veri aktarım sistemlerine sızmıştır. Bu zafiyet, NATO'nun siber alandaki egemenliğinin ve güvenilirliğinin sorgulanmasına sebep olmuştur (Çubukçu ve Bayzan, 2013). Siber saldırı boyunca NATO yönetim birimleri

arasında koordinasyon kurulamamış ve diğer üye ülkeler ile çevrim içi iletişim sağlanamamıştır. Bu saldırının bir başka özelliği de NATO'nun hedef alındığı ilk siber saldırı olmasıdır (Daban, 2016). NATO, yaşanılan siber saldırı deneyimi ile birlikte konvansiyonel güvenlik anlayışının değişmesi gerektiğini ve yeni siber güvenlik kurullarına ihtiyaç duyulduğunu beyan ederek 2002 Prag Zirvesi sırasında siber saldırılara hızlı ve etkin bir şekilde karşılık verecek bir merkez kurulacağını bildirmiştir (Darıcılı, 2016: 412).

Gürcistan siber saldırısı, Rusya Federasyonu tarafından gerçekleştirildiği öne sürülen ve arkasında tarihî sorunların yattığı bilenen bir diğer örnektir. Bu olayların devamı olarak 2008 yılında Gürcistan'a karşı gerçekleştirilen siber saldırılar, Estonya saldırısına benzer niteliktedir. Saldırılar sonucunda Gürcistan'ın hükümet altyapı bilişim sistemleri ağır zararlar görmüştür. Saldırıların sadece Rusya'dan değil, farklı bölgelerden de gerçekleştirildiği tespit edilmiştir (Martellini, 2013). Gürcistan'ın NATO'ya üye ülkelerden biri olmaması nedeni ile NATO saldırılara doğrudan müdahil olamamış, ancak sistemlerin düzelebilmesi için ülkeye uzman ekipleri göndermiştir (Geers, 2008). Saldırılar boyunca Gürcistan, konvansiyonel savaşlardan daha büyük zarar görmüştür. Ülkenin diğer ülkeler ile bağlantı sistemleri kopmuş, ayrıca ödeme ve haberleşme sistemleri kullanılamaz duruma gelmiştir (Goodman, 2010, ss. 102-135).

Yine İran'a yönelik Stuxnet saldırısı, Batı dışı dünyada da siber güvenliğin ulusal ve uluslararası güvenlik için önemli bir unsur olduğunu gösteren bir saldırıdır. Bu saldırıdan sonra birçok ülke, siber güvenlik strateji belgelerini geliştirme çabası içine girmiştir. Yine uluslararası örgütler, ulusal siber güvenlik belgelerini ve rehberlerini bu saldırıdan sonra yayınlamaya başlamıştır. Söz konusu saldırı; 2010 yılında gerçekleştirilen, karmaşık kodlardan oluşan bir kurtçuk saldırı ile İran'ın nükleer çalışmalarına zarar veren bir saldırıdır. Etkileri bakımından en önemli siber saldırıların başında gelen Stuxnet, bilgisayar programlarına hasar vermekle kalmamış; aynı zamanda makinelere de zarar vermiştir. Saldırı, endüstriyel kontrol sistemlerini, bir başka isimlendirme ile SCADA'nın (Supervisory Control And Data Acquisition) Uranyum zenginleştirmede önemli bir role sahip laboratuvar cihazlarını hedef almıştır. Hedef sistemdeki açıklar kullanılarak bir USB sürücüsüyle sızan bu zararlı yazılım, SCADA sistemlerine yönelik üretim kumanda merkezî sisteminin işlevselliğini ve çalışma şeklini değiştirerek yarattığı fiziksel tahribatın yanı sıra, sistemi maddi olarak da zarara uğratmıştır. Bu saldırı; bilgisayarla beraber endüstriyel kontrol sistemlerinin ve dış dünyadan izole edilmiş sistemlerin hedef alınmasında, bunun yanında bu hedefin nihayete ermesinde önemli bir yere sahiptir.

İsrail'in Orchard Siber Saldırısı; Eylül 2007'de Suriye'nin doğusunda inşa edilen bir tesisin, nükleer silah geliştirdiği iddiasıyla İsrail tarafından Suriye'nin hava savunma sistemleri ve radarlarına yakalanmadan bombalanması olayıdır. Bu olayın siber güvenlikle ilişkisi, İsrail'in Suriye'nin hava savunma sistemlerine ve radarlarına yakalanmadan bu operasyonunu gerçekleştirmiş olmasıdır. Suriye hava savunma sistemlerinin İsrail savaş

uçaklarını görmesi gerekirken bu siber saldırı yöntemleri kullanılarak uçakların görülmesi engellenmiştir. İsrail, saldırıdan önce Suriye hava savunma sistemlerine ışık ve pals darbelerini kullanarak I ve O şifrelerini iletmek amacıyla sistemi kontrol altına almıştır. Böylelikle İsrail, Suriye'nin radar ekranlarına istediği görüntüyü yerleştirebilmiştir. Nitekim bombalama sırasında Suriye radar ekranlarında İsrail'in uçakları gözükmemiştir. Bu saldırı, savunma sistemlerinin nitelikli ve güvenlikli olsa dahi siber saldırılar karşısında işlevini yitirebileceğini göstermiştir. Bu saldırının diğer önemli bir yönü ise ne tür radar sistemleri kullanıldığıyla ilgili olmasıdır. Görece eski ya da güvenlik açığı olan sistemlerin kullanılması bu tür saldırıları kolaylaştırmaktadır. Yine bu saldırı, uluslararası ilişkilerde teknolojiyi iyi kullanmanın bir devlete avantaj sağladığını da göstermektedir. Bu nedenle siber teknolojide ileri ülkeler, siber uzayda hem savunma hem de saldırıda üstünlüklere ve kabiliyetlere sahip olacaktır.

Bir başka siber saldırı örneği: ABD Dış İşleri Bakanlığına ait, 1996'dan 2010 yılına kadar yapılan ve devlet sırrı olma niteliği taşıyan yazışmaları, ordusu mensubu Bradley Manning'in Wikileaks isimli web sayfası üzerinden tüm dünyaya yayması **"Wikileaks Skandalı"** olarak isimlendirilmektedir (Gözükeleş, 2014). İlgili web sayfasının kurucusu olan Julian Assange; Kenya'da yapılan infazlar, Fildişi sahiline bırakılan kimyasal atıklar, Guantanamo Kampı'nda kullanılan insanlık dışı yöntemlere kadar çok sayıda bilgiyi kamuoyu ile paylaşmıştır. Wikileaks Skandalı'nı önemli hâle getiren, saldırının bir kişi tarafından devletler arası gizli platformları hedef almış olmasıdır. Bu gelişme, ABD'nin siber güvenlik stratejilerini yeniden gözden geçirmesine neden olmuştur (Gürsoy, 2013).

ABD Seçimlerine Rusya'nın Siber Saldırıları, Amerika Birleşik Devletleri'nde 2016 yılında yapılan başkanlık seçiminde gündemde yer alan hususlardan birisi de Rusya'nın seçimlere yönelik siber saldırılar gerçekleştirdiği iddiaları olmuştur. Bu iddiaya göre Rusya, Hillary Clinton'ın seçim kampanyasından mesul olan John Podesta ile Clinton'un seçim sırasındaki çalışmalarına aktif olarak destek veren Colin Powell'in e-postalarını ele geçirmiş, bu e-postalardan bir kısmını kamuoyuna sızdırmış, böylelikle seçimi Rusya çıkarlarına uygun olacak şekilde manipüle etmiştir. Düşünce kuruluşu Atlantic Council'in yayımladığı raporda Rusya'nın amacının Hillary Clinton'ın seçilmesini engellemek, ABD'deki fikirsel ve yöntemsel olarak bölünmüş online grupları daha da bölmek ve ABD kurumlarına güveni zedelemek olduğu iddia edilmektedir. ABD Başkanlık seçimlerindeki siber saldırılara ilişkin tartışmalar devam etmişse de Rusya'nın müdahalesi kesin delillerle kanıtlanamamıştır. Tartışmalar her ne kadar ABD seçimlerine odaklanılarak yapılmış olsa da Atlantik'in öbür kıyısındaki diğer seçimlerde de Rusya'nın siber müdahalesinden korkulmaktadır. Bazı raporlara göre Rusya sadece Amerika kıtasındaki değil, Avrupa'daki seçimlere de siber müdahalelerde bulunma potansiyeli taşımaktadır. 2016 yılından beri dünyada, yapılan tüm ulusal seçimlerle ilgili şüphe ve güvenlik korkuları oluşmuştur. Ağustos 2017'de Kenya'da

yapılan Başkanlık seçimlerine siber saldırı olduğu ihtimali ile seçim sonuçları geçersiz sayılmıştır. Bu tür korkular küresel düzeyde devam etmekte ve bu da demokratik sistemin ve demokratik süreçlerin güvenilirliğini sarsmaktadır.

1.4. Siber Suç ve Siber Savaş Kavramları

Bu noktada siber suç ve siber savaş kavramlarının açıklanması gerekmektedir. Siber suçlar kredi kartları, bilgisayarlar, cep telefonları, hatta bazen akıllı ev aletleri gibi günlük hayatımızda hayati önem taşıyan araçlarla işlenmektedir. Kavramın bu kadar geniş bir kapsamının olması, birçok farklı tanımın yapılmasına neden olmuştur. Basitçe söylemek gerekirse dijital suç, internet suçu, elektronik suç, yüksek teknoloji suçu gibi terimler, bilgisayar suçu olarak adlandırılan siber suçları tanımlamak için kullanılmaktadır. Siber suçlar ile ilgili en kapsamlı düzenleme, Avrupa Konseyi bünyesinde gerçekleştirilen "Avrupa Konseyi Siber Suç Sözleşmesi"dir. Adı geçen sözleşme Avrupa Konseyi Bakanlar Komitesi'nde kabul edilmiş ve müteakiben 2001 yılında Budapeşte'de toplanan Siber Suçlar Uluslararası Konferansı'nda imzaya sunulmuştur. Bu sözleşmenin ikinci bölümünde, siber suçlar aşağıdaki sınıflandırmaya tabi tutulmuştur:

i. Bilgisayar verilerine ve bilgisayar sistemlerinin gizliliğine, bütünlüğüne ve erişilebilirliğine yönelik suçlar: Yasa dışı erişim, yasa dışı müdahale, verilere müdahale, bilişim sistemine müdahale, cihazların kötüye kullanımı,
ii. Bilgisayarlarla ilgili suçlar: Bilgisayarla ilgili sahtecilik ve dolandırıcılık eylemleri,
iii. İçerikle ilgili suçlar: Çocuk pornografisi ile ilgili suçlar,
iv. Telif haklarıyla ilgili suçlar.

Çizilen bu geniş çerçeveye rağmen konuyla ilgili çalışmaların siber suçların kavramsallaştırılmasında ortak bir tanım ve içerik konusunda uzlaştıkları söylenemez. Brenner; siber suç sözleşmesine paralel olarak siber suçu, "suç işlemek ya da toplumsal düzeni tehdit eden faaliyetlerde bulunmak için bilgisayar teknolojisinin kullanılması" olarak tanımlar.

Çoğunluğu oluşturan bazı araştırmacılar ise bilgisayarların eskiden tanımlanan bir suçun işlenmesinde kullanılmasının veya fiziksel olarak bilgisayarların hedeflenmesinin siber suçların kapsamına alınmaması gerektiği görüşündedirler. Bu uzmanlara göre **geleneksel suçların bilgisayar vasıtasıyla yeni ve daha etkin yöntemler ile işlenmesi**, teknolojinin gelişiminin ortaya koyduğu saldırı hedefi olarak tamamen bir bilgisayar sistemini esas alan siber suçlardan farklıdır. Uzmanlar, bilgisayarların suç işlerinde bir araç olarak kullanılması ile bilgisayar olmadan da bu suçların işlenebilir olması ayrımına odaklanırlar.

Özetle siber suç, sistem sahibinin rızası olmadan sisteme girilmesi, sisteme girmek için yetkinin aşılması, bilgisayar verisine yetkisiz erişim, verilerin değiştirilmesi veya

10.5824/ajite.2022.04.004.x

silinmesi, bilgisayar işlem zamanının ve kaynaklarının yetkisiz olarak kullanılmasından oluşmaktadır.

Bilgisayarlara fiziksel olarak zarar veren saldırıların siber suç olarak nitelendirilmesi daha özel bir incelemeyi gerekli kılar. Eğer bir saldırı, bilgisayarların taşıdığı elektronik verileri imha etmek, ele geçirmek veya bozmak maksadıyla yapılıyorsa, bu eylem **siber suç** olarak nitelendirilebilir.

Siber terörizm, siyasi nedenlerle önceden planlanmış ve nihayetinde toplumda korku ve huzursuzluk yaratmayı amaçlayan; bilgisayarlara, bilgisayar sistemlerine, internet teknolojilerine ve tesislerine karşı gerçekleştirilen eylemlerdir. Diğer bir deyişle, siber terörizm bilgisayar korsanlığı tehdidi, izinsiz giriş veya bilgisayar ihlali gibi siyasi bir amaçla yapılan eylemin neden olduğu engelleme sonucunda toplumun bir kesiminin davranışlarını etkileyen ya da etkilemeye çalışan eylemler olarak kendini gösterebilir. Siber suçlarda olduğu gibi bilgisayarların ve bilgisayar sistemlerinin bir araç veya hedef olarak kullanılması siber terörizm kapsamına alınabilir. Bununla birlikte siber suç ile siber terörizm arasındaki temel ayırt edici faktör, eylemin siyasi amaçlı olup olmadığıdır.

Siber terörizm ve siber suçlar genellikle aynı eylemleri içerdiğinden, aralarındaki farklılığı anlamak için eylemin ortaya çıkış sebebine, yani motivasyonuna bakma gerekliliği doğmaktadır. Bu da kavramların ayrımında karışıklığa sebep olmaktadır. Bundan sonra incelenecek siber savaş kavramı ise siber suç ve siber terörizmle aynı ortamı ve eylemleri paylaşsa da nedensellik ve failler açısından ikisinden de ayrılmaktadır.

1.5. Siber Uzayın Güvenlik Açısından İncelenmesi

Küreselleşme sürecinin ve teknolojik gelişmelerin de güvenlik çalışmalarına göz ardı edilemeyecek boyutta katkısı olmuştur. Özellikle küreselleşme sürecinin güvenlik algısında dönüştürücü ve değiştirici etkisi olmuştur. Bir diğer ifadeyle, 1990'larla beraber küreselleşmenin doruk noktasına ulaşması çerçevesinde, güvenlik yaklaşımları kabuk değiştirerek çeşitlilik kazanmıştır. Öte yandan, küreselleşmenin ileri boyutlara ulaşmasında etkisi olan internet ve teknoloji de bu çalışmalara doğrudan katkı sunmuştur. Belirtilenler içerisinde mihenk taşı olarak kabul edebileceğimiz, "siber uzay" adı verilen yeni bir alan ve kavramsal olarak soyut bir durum olan internet ortaya çıkmıştır. Güvenlik boyutunun genişlemesine yol açan bu alan, siber güvenlik kavramının ortaya çıkmasına zemin hazırlamıştır.

Siber güvenlik genel olarak birçok eylem planında ve çalışmada, “siber uzayda bilgilerin gizliliğinin, bütünlüğünün ve kullanılabilirliğinin korunması” şeklinde tanımlanmaktadır. Ancak, siber uzay olarak ifade edilen alanın mevcut sınırlarının net olmaması güvenlik durumumun sağlanması konusunda sorunlar oluşturmaktadır. Fiziksel

olarak net olmayan veya net olarak çizilemeyen bu alanda, devletlerin sahip oldukları somut sınırlar da muğlaklaşmaya başlamıştır. Bundan dolayı da herhangi bir siber saldırı ve tehdit karşısında devletlerin refleksleri de buna bağlı olarak net şekilde belirginleşememiştir. Bu durumun da güvenlik kaygısını ve artan güvenlik ikilemini etkilediği görülmektedir. Sınırların muğlaklığını daha zor bir hâle getiren başka bir durum ise siber uzayda coğrafya kavramının önemini yitirmiş olmasıdır. Coğrafyadan bağımsız olarak dünyanın herhangi bir yerinden bir saldırı ve tehdit unsuru gelebilmektedir. Bu durum ise sınırların çizilmesinde oldukça engelleyici bir faktör durumundadır. Öte yandan, siber uzayın yapısından dolayı, uluslararası ölçekte uygulanacak net bir hukuk sistemi bulunmamaktadır. Birçok devlet veya örgütün üzerinde konsensüs sağlamış olduğu uluslararası siber hukuk ve buna bağlı olarak yaptırım sistemi düzenlenmemiş olması, yapılan saldırılara karşı yaptırımları ve bu konudaki mütekabiliyet esaslarını muğlak hâle getirmektedir.

1.6. Ulusal Güvenlik Çerçevesinde Siber Güvenliğin Sağlanması

Ulusal güvenlik yaklaşımı, II. Dünya Savaşı sonrası yaygın şekilde kullanılmaya başlayan Soğuk Savaş'ın bir ürünüdür. **Ulusal güvenlik yaklaşımı**, gücün ulusların davranışlarında ve uluslararası sistemin işleyişinde anahtar rol oynadığını kabul eder. Bu yaklaşıma göre, bir ülkenin sahip olduğu gücünün siyasi istikrarına, sosyal bütünlüğüne ve ekonomik verimliliğinin yanı sıra askerî anlamda sahip olduğu birliklerine, tanklarına, uçaklarına, gemilerine, füzelerine ve nükleer savaş başlıklarına bağlı olduğu ifade edilmiştir.

Son yıllarda birçok ülke ve uluslararası kuruluşun gündeminde yer alan siber güvenlik yeni bir olgu olmasına rağmen, güvenlik açısından uluslararası ilişkiler disiplinine entegre edilmiş bir kavramdır. Ülkeler arasındaki siber savaşın ölçeği, geleneksel rekabete dayalı çatışma olgusuyla örtüşmeye başlamıştır. Aynı zamanda ülkeler saldırı ve savunma unsurları geliştirmek için tüm çabalarında daha temkinli hâle gelmiş lakin siber uzaydaki tüm faaliyetler, güvenlik tartışmaları ve her unsurun geliştirdiği farklı yaklaşımların savaşa ve çatışmaya yol açabileceği ihtimalini öngören tezleri daha da güçlendirmiştir. Bu nedenle, ortak bir siber savaş hukuku ve tüm tarafları bağlayıcı mütekabiliyet esaslarının düzenlenmesi kaçınılmaz bir ihtiyaç hâlini almıştır.

Ulusal güvenliğin önemli kavramlarından biri de caydırıcılıktır. Soğuk Savaş döneminde ABD ve Sovyetler Birliği'nin karşılıklı olarak güçlü olmaları ve birbirleriyle nükleer bir yarış içinde olmaları, bu durumun somut bir örneğidir. Siber uzay ve yaratmış olduğu sistem ise bu durumla benzerlik göstermektedir. Ancak, siber alanda mevcut olabilecek bir yıkım ayrıştırılabilir ve zamanla küçük dozlar şeklinde görülebilirken, nükleer yıkım ise çok daha dramatik bir olgu olarak görülmektedir. Bu bağlamda kısmen siber güvenlik, nükleer caydırıcılık kadar bir ikilem yaratmamaktadır. Buna ek olarak, siber uzayda sivil kesim ve normal bireyler bir tehdit unsuru oluşturmaktayken, nükleer alanda

10.5824/ajite.2022.04.004.x

ise sadece askerî güce sahip devletler bir tehdit unsuru olmuştur. Ana aktör olan devlet uluslararası sistemde eskiden olduğu gibi tek ve güçlü aktör konumunu artık kaybetmiştir. Ancak siber güce ulaşım ve erişim konusunda siber uzayın yaratmış olduğu yapı ve maliyetlerin çok daha ucuz olması, nükleere erişime kıyasla daha avantajlı görüldüğü için tam bir ikilem durumu yaratmaktadır. Burada durumun farklı boyutlarda farklı sonuçlar doğurduğu ifade edilebilir.

Pek çok devlet ulusal güvenliğine katkı sağlamak amacıyla ulusal siber güvenlik strateji belgeleri yayımlamıştır. Bu, birçok devlet için ulusal güvenlik açısından siber güvenliğin öncelikli alan olmaya başladığını göstermektedir. Bu eylem planları doğrudan ulusal olarak siber güvenliği geliştirmeye yöneliktir. Eylem planları içinde kırılma noktası Estonya'ya karşı yapılan 2007 yılındaki saldırı olmuştur, çünkü bu saldırı sonrasında ülkelerde bir farkındalık oluşmaya başlamış ve bu farkındalığın ardından birçok ülke siber güvenlik ajansları ve eylem planlarını geliştirme eğilimine yönelmiştir. Keza bazı ülkeler siber alanla alâkalı elçi atamıştır. Buna örnek olarak Avustralya'nın 2016 yılında atadığı Siber İşler Elçisi örnek verilebilir.

1.7. Uluslararası Güvenlik Bağlamında Siber Güvenlik

Uluslararası sistemde meydana gelen birçok güvenlik durumunun, özellikle Soğuk Savaş sonrası dönemde meydana gelen güvenliğin değişimi ve dönüşümü ile alakalı olduğu görülmektedir. Yaşanan dönüşümde güvenlik salt askerî unsurlardan ve devletlerin genişleme politikalarından ayrılmaya başlayarak daha geniş anlamda ve kapsayıcı çalışmaları içerisine dâhil ederek genişlemiştir. Bu çalışmalardan en önemlisi, son zamanlarda önemi giderek artmaya başlayan siber güvenlik çalışmalarıdır. Özellikle Soğuk Savaş'ın sona erdiği döneme paralel şekilde ortaya çıkan internetin küresel ölçekte kullanılmaya başlanması, birçok avantajla birlikte birçok tehdit unsurunu da beraberinde getirmiştir. İnternetin küresel bir fenomen hâline gelmesiyle birlikte, birçok ülke ve insan bu yapıya katılmaya başlamıştır. İnternet birçok alanda çığır açarak yaratıcı yeniliklerle platformunun çok daha ileri boyutlara genişlemesine vesile olmuştur.

Uluslararası güvenlik bağlamında siber güvenlik, daha çok devletlerin hissettiği birtakım kaygılardan ve güvenlik ikileminden oluşmaktadır. Güvenlik kaygısının mevcudiyeti uluslararası sistemin anarşik yapısı ile alakalıdır. Bunu ortadan kaldıracak herhangi bir yasa veya yasal çalışma olmadığı için uluslararası arenada herhangi bir uzlaşı sağlanamamıştır. Buna göre birçok ülke kendi güvenliğini sağlamayı seçmiştir ve sorunların kökenine yönelik olarak diğer ülkelerle birlikte çalışmaktadır. Her ülkenin kendi başına birtakım alternatifler geliştirme girişimleri ve silahlanma gibi temel önlemleri önceliklendirerek hareket etmesi, güvenlik ikilemi açısından diğer ülkelerin güvenliğini

azaltma eğilimindedir. Güvenlik ikilemi bu aşamada uluslararası ilişkilerin en önemli paradokslarının başında gelmektedir.

Uluslararası anlamda siber güvenliğin sağlanamaması konusundaki en temel nedenlerden birisi devletlerin temel aldığı kurumların olmaması ve yaptırımların bulunmamasıdır. Siber güvenliğin uluslararası alandaki etkisi esasında ulusal güvenlikten geçmektedir. Çünkü bir ülkenin güvenliğindeki olası bir gelişme, uluslararası çevreyi de etkilemektedir. Bu sebeple her ulusal problem, siber alanda uluslararası bir boyuta dönüşerek uluslararası güvenliği de etkilemektedir. Bu bağlamda öncelikli olarak ulusal siber güvenliğin sağlanması ve uluslararası iş birliğinin yapılması gerekmektedir. Bunun sebebi, klasik nükleer gibi güvenlik mekanizmaları sadece devletlere belirli bir güç verirken siber teknolojinin devlet dışı aktörlere de güç vermesidir. Bu durum herhangi bir tehdidin sadece devletlerden gelmeyeceğini göstermekte ve ayrıca, bireylere kadar uzanan bir tehdit listesinin oluşmasına yol açmaktadır.

2. GÜÇ, CAYDIRICILIK VE HUKUK BAĞLAMINDA SİBER UZAY

2.1. Siber Uzaydaki Güç Unsurları ve Siber Güç Kullanma Kapasitesi

Siber ortamda bulunan diğer elemanları güç unsurlarını kullanarak etkileyebilme kabiliyeti "siber güç" olarak tanımlanmaktadır. Siber ağ üzerinden gerçekleştirilen faaliyetlerin giderek artması, ülkelerin kritik öneme sahip altyapı işlemlerini bu ağlar aracılığı ile sağlayarak küresel alanda gücün siber güce odaklanmasına neden olmuştur (Şentürk vd., 2012, ss. 112-125). Realist uzmanlara göre, ülkeler arasında yaşanan güç üstünlüğü mücadelesi konvansiyonel savaşların temelinde yer alan ana unsur olarak kabul edilmekte olup militer güç devletin gücünün en önemli simgesi olarak vurgulanmaktadır (Tarhan, 2017, ss. 105-124).

Web servis sunucuları ile web sayfaları gibi dijital araçlar birbiri ile yakın ilişkide olmakla beraber fiziksel olarak farklı birimlerde bulunmaktadır. Siber uzay kullanıcı, medya içeriği, internet protokolleri, yazılım ve siber uzayın yönetildiği fiziksel alan olmak üzere beş farklı unsurdan oluşmaktadır. Bu unsurlardan her biri farklı altyapılar içermektedir. Fiber kablolardan oluşan ilk altyapı sisteminin kötü niyetli güçler tarafından yönetilmesi, siber sistemlerin bulunduğu ikincil sistemin de ele geçirilerek yönetilebileceği düşüncesini ortaya çıkarmıştır. Bu durumda, üçüncü sistem olan bilgilerin erişimi ile ilgili veri yönetim sistemleri de kontrol edilebilir hâle gelecektir. Son sistemde ise kişinin hedefine bağlı olarak hâkimiyetin söz konusu olacağı düşünülmektedir. Tüm bu sistemler bir bütün olarak düşünüldüğünde, siber alanda bulunan verilerin doğru değerlendirilmesi gerektiği ve her stratejik bilginin de siber güce sahip olmak için önemli olduğu düşünülmektedir. Ülkeler, devlet dışı faktörlerin siber güç hâkimiyeti için anarşik tehditleri kullandığı siber ortamda, ulusal güvenliklerinin korunması için farklı güç unsurları kullanmaya ihtiyaç duymaktadır.

10.5824/ajite.2022.04.004.x

Ülkeler, siber hâkimiyeti elde edebilmek için maksimum güç kullanmaya ve nitelikli stratejiler geliştirmeye çalışarak yeni ve etkili siber ordular kurmaya başlamıştır. Dünyanın teknolojik gücünü ellerinde tutabilen ülkeler arasından ABD, Çin, Rusya, İsrail, Kuzey Kore ve İran'ın legal ve illegal faaliyet haklarına sahip olan siber ordularının olduğu bilinmektedir. Bu sınıflandırmanın dışında bulunan ülkeler ise merkezini güvenlik stratejilerinin oluşturduğu yeni siber savunma teknikleri geliştirmektedir. Bunun yanı sıra, ülkelerin siber ortamda gerçekleştirdiği diğer bir faaliyet ise siber dünya kullanımı konusunda hâkimiyet sahibi olan uzman hacker sayısını artırmaktır. Siber kavramının stratejik bir silah olarak bilgisayar tabanlı yazılımlar kullanılarak yapılabilmesi, programlama bilgisine sahip olmayan kişilerin bile siber saldırı yapabileceği gerçeğini ortaya koymaktadır. Ancak bilgisayar kullanım uzmanlığı siber uzayda önemli bir etki yaratabilmek için stratejik bir yöntem değildir.

Siber alan, NATO tarafından konvansiyonel anlamda kara, deniz, hava ve uzaydan sonra yeni bir savaş alanı olarak tanınmıştır (NATO, 2016). Siber savunma yeteneklerinin güçlendirilmesi ihtiyacı ilk olarak 2002 yılında Prag Zirvesi'nde tartışılmış ve o zamandan beri siber güvenlik konusu giderek NATO zirvesi gündeminde yer almaya başlamıştır (Brent, 2019). İlk siber savunma politikası 2008 yılında kabul edilmiş ve 2014'te Müttefik Siber Savunması toplu savunmanın ayrılmaz bir parçası olarak nitelendirilerek her siber saldırı, Sözleşme'nin temelini oluşturan toplu savunmaya ilişkin NATO'nun 5. maddesi kapsamında değerlendirilmiştir (Brent, 2019). Bu bağlamda, dünyada ülkelerin siber hâkimiyeti ele geçirebilmek için siber araçlarını güçlendirdiği, siber saldırı yetenekleri geliştirdiği ve kendi güvenliklerini sağlayabilmek için siber güvenlik kanunları üzerinde çalıştığı görülmektedir. İçinde bulunduğumuz bilgi çağında ülkeler arası arenada hâkimiyeti kazanabilmek için, bilginin iktidar kaynağı olarak kullanıldığı düşünülmektedir.

Ülkelerin son yıllarda siber saldırı araçlarını güçlendirmek ve aynı zamanda da siber güvenliği sağlamak amacı ile ciddi bir bütçe ayırdıkları izlenmektedir. Günümüzde, yüksek düzeyde siber savaş kapasitesine sahip olduğu bilinen ülkeler arasında ABD, İngiltere, Çin, Rusya ve İsrail bulunmaktadır. NATO da yaşanılan gelişmelere paralel olarak "Mükemmeliyet Merkezi" adını verdiği kendi siber savunma merkezinin kuruluşunu gerçekleştirmiştir. Ayrıca, Avrupa Konseyi, Siber Suç Sözleşmesi'ni hayata geçirerek uluslararası arenada önemli bir girişime imza atmıştır. Amerika Birleşik Devletleri ise siber suçlara karşı caydırıcılık unsuru olarak yaptırımları artırma yöntemlerine başvurmaktadır.

Caydırıcılık kavramı ABD'nin siber suçlara karşı geliştirdiği stratejik devlet politikasında merkezî konumda bulunmaktadır. ABD hükümeti ayrıca uluslararası kurallara uygun olarak siber saldırılara karşı cevap verme hakkı konusunda da kararlığını korumaktadır. Bunun yanında, ABD alınan tüm önlemler ve ceza artırımı politikasına rağmen, kendilerine karşı yürütülecek olası bir siber operasyonda askerî gücü de devreye

sokabileceğinin sinyalini vermiştir (Federal News, 2015). 2011 yılında ABD ve Rusya'nın bilgi transferi ve siber güvenlik konularında yayınladıkları ortak rapor, siber gücü elinde bulunduran ülkelerin siber saldırılara karşı hükümet düzeyinde iş birliği yapabileceğinin de göstergesi olmuştur (Lin, 2017). ABD'nin siber suçlara karşı yüksek düzeyde önlem almasının nedeni, siber güç hâkimiyeti için yeni teknolojiler geliştirirken siber saldırıya uğrama riskini de artırmış olmasıdır. Çin, Rusya ve İran gibi ülkeler ise kritik askerî altyapılarının büyük bir kısmını siber uzaya yönlendirmiştir.

Siber uzayda güç üstünlüğünün sağlanabilmesi için ülkelerin sadece teknik kapasiteleri ve ellerinde bulundurdukları teknolojik donanım yeterli değildir. Bunun nedeni siber saldırıyı gerçekleştiren aktörlerin fiziki anlamda silahsızlandırılamaması, yok edilememesi veya karşı müdafaa yöntemlerinin kısıtlı olmasıdır. Siber uzayda siber güvenlik stratejilerinin uygulanması ile caydırıcılık sağlansa da saldırıyı yapan ya da yaptıran gücün belirlenememesi siber güce karşı yaptırım uygulamanın önüne geçmektedir. Siber alanda caydırıcılığı kısıtlayan başlıca üç engel şunlardır: Asimetrik güç kullanımı, siber saldırganın belirlenememesi, devlet dışı aktörlerin aşırı güçlenmesi. Bahsedilen faktörlerin 2007 yılında Rusya'nın Estonya'yı hedef alarak gerçekleştirdiği siber saldırı üzerinden incelenmesi, bu faktörlerin etkisini anlamak açısından daha anlamlı olacaktır (Guzman, 2017).

2.2. Siber Saldırılar Karşısında Devletlerin Hukuki Hakları

2.2.1. Siber Saldırılara Karşı Meşru Müdafaa

Konvansiyonel savaş kavramı ile sıkça anılan güç kullanımı ve meşru müdafaa kavramlarının siber saldırılar ile nasıl bağdaştırılacağı konusu, siber savaş hukuku ile ilgili çözülmesi gereken sorunların üst sıralarında gelmektedir. Birleşmiş Milletler Sözleşmesi'nin ikinci maddesi, günümüz koşullarında güç kullanma yasağını düzenleyen en temel maddedir. Söz konusu madde şöyledir:

"Tüm üyeler, uluslararası ilişkilerinde gerek başka bir devletin toprak bütünlüğüne ya da siyasal bağımsızlığa karşı, gerekse Birleşmiş Milletler'in amaçları ile bağdaşmayacak biçimde kuvvet kullanma tehdidine ya da kuvvet kullanılmasına başvurmaktan kaçınırlar".

Bahsedilen maddede kullanılan güç kavramı yalnızca silahlı güç kullanımını içermekte olup siyasi ve ekonomik anlamda düzenlenen tedbirler bu kapsamda değerlendirilmemektedir. Bu nedenle, bazı görüşler bu maddeyi siber savaşta bir tür uluslararası teamül olarak görmemekte ise de siber saldırıların birçok fiziki saldırıdan daha büyük hasara sebep olduğu dikkate alındığında, bu görüşlere katılma imkânı bulunmamaktadır. Güç kullanma yasağının iki önemli istisnası bulunmaktadır: **Birinci istisna**, Birleşmiş Milletler Güvenlik Konseyi'nin (BMGK) uluslararası alanda barışın tehdit altına girmesine yönelik bir saldırı olduğunun belirlenmesi hâlinde, ilgili sözleşmenin yedinci bölümü kapsamında üye ülkelerin diğer bir ülkeye karşı güç kullanımına başvurabilmesidir. Bahsedilen istisna, Birleşmiş Milletler Güvenlik Konseyi'nin yirmi

10.5824/ajite.2022.04.004.x

dördüncü maddesi uyarınca uluslararası alanda barış ve güvenliğin korunması konusunda yetkili organ olarak kabul edilmesinin getirdiği bir durumdur. **İkinci istisna** ise Meşru Müdafaa Hakkı olarak kabul edilmektedir. Meşru Müdafaa Hakkı, ilgili sözleşmenin elli birinci maddesinde açık olarak tanımlanmış olup uluslararası teamül hukukunda da yerini almıştır.

Bu maddeye göre ilgili anlaşmada, üye ülkenin silahlı saldırıya uğraması durumunda barış ve güvenliğini koruması amacıyla gerekli önlemler alınıncaya kadar bireysel ya da kolektif meşru savunma hakkını zedeleyen hiçbir hüküm bulunmamaktadır. Üye ülkeler meşru savunma hakkını kullanırken başvurduğu tedbirleri güvenlik konseyine bildirmekte ve güvenliğin yeniden tesis edilmesi amacıyla Güvenlik Konseyi'nin yetki ve görevleri devam etmektedir. Siber savaşta mütekabiliyet esasları da bu kapsamda değerlendirilmelidir.

2009'da Estonya'nın Tallinn şehrinde kurulan NATO Müşterek Siber Savunma Mükemmeliyet Merkezi'nde konu ile ilgili uzmanlardan oluşan bir kurul, siber saldırı durumunda uygulanabilecek hukuksal konuları derleyerek **Tallinn Kılavuzu'**nu oluşturmuştur. Bu kılavuzun 11. kuralına göre, siber saldırılar **güç kullanımı** olarak değerlendirilmektedir. İlgili madde, bir siber eylem ölçü ve etki bakımından konvansiyonel eylemle aynı seviyede etkide bulunuyorsa, bu siber saldırıyı **güç kullanımı olarak** değerlendirmektedir. Ayrıca, ilgili kılavuza göre, ülkelerin toprak bütünlüklerine yönelik tehdit içeren siber saldırılar da yasa dışı güç kullanımı olarak kabul edilmektedir. Aynı kılavuzun 13. maddesi, siber saldırıya maruz kalan bir ülkenin Meşru Müdafaa Hakkı'na sahip olduğunu belirtmektedir. Tüm bu maddeler uyarınca siber güç kullanımı, fiziksel alanda zarara sebep olan ve bilgisayar sistemlerini geçici veya kalıcı şekilde devre dışı bırakan **terörist faaliyetler** kapsamına girmektedir.

2.3. Siber Saldırı Karşısında Devletlerin Yargı Yetkisi

2.3.1. Uluslararası Hukuk Açısından Yargılama Yetkisi

Siber saldırılar karşısında yargılama usullerine ilişkin tüm devletleri kapsayacak uluslararası bir sözleşme bulunmamakla beraber, bu konudaki kapsamı en geniş olan düzenleme Avrupa Konseyi Siber Suç Sözleşmesi'dir. Sözleşmeye taraf devletler, iç hukuk yollarında sözleşme uyarınca düzenlemeler yapıp hem yargılama hem de iş birliğine ilişkin normları sözleşme kapsamında belirlemektedirler. Bu konuda Birleşmiş Milletler'in de uluslararası bir anlaşma için taslak hazırlama girişimleri de bulunmasına karşın henüz somut bir ilerleme sağlanamamıştır. Bu nedenle, uluslararası hukuk açısından savaş suçları mahkemesi benzeri bir yargılama organı ya da yetkisinden bahsedilememektedir. Ülkeler arasındaki genel kabul gören uygulamalar dikkate alınarak BM bünyesinde benzer bir anlaşma düzenlenmesi ve taraf devletlerin bunu kabulü ile bu konudaki eksiklikler

giderilebilecek, aksi takdirde yerel ya da bölgesel uygulamaları aşan bir yetkiden bahsedilemeyecektir.

Genel kabul gören uygulamada yasa dışı erişim devletlerin ve toplumların bilişim sistemlerine yönelik işlenen en temel suçlar arasında kabul edilmektedir. Siber Suç Sözleşmesi'nde yasa dışı erişim "bilişim sistemlerinin ve bu sistemlerde depolanan verilerin gizliliğine yönelik işlenen yasa dışı eylem" olarak nitelendirilmiştir. Bilişim suçlarının icrası, saldırılmak istenen hedef sisteme erişim sağlanması ile başlamaktadır. Saldırıyı gerçekleştiren kişi veya gruplar, amaçlarına göre farklı türde siber saldırı suçları işleyebilmektedir. Sisteme yasa dışı olarak erişen bir fail, yalnızca kişisel verilere ulaşmak amacıyla hareket edebildiği gibi, sistemi değiştirmeyi ya da tamamen silmeyi de hedefleyebilir.

Uluslararası hukukta, yasa dışı erişim denilen olgu, suçun oluşmasında etkili olan maddi ve manevi unsurların tespiti açısından çok önemlidir. Avrupa Konseyi'nin düzenlemiş olduğu Siber Suç Sözleşmesi'nde ve Birleşmiş Milletler'in hazırlamış olduğu tasarılarda "illegal access" terimi kullanılmış, bahsedilen terim Türkçeye "yasa dışı erişim" olarak çevrilmiştir. Literatürde yasa dışı erişim teriminin "yetkisiz erişim" olarak da kullanılabildiği görülmektedir. Erişim eylemi, bu çerçevede, hedef sisteme ulaşmak veya gizli bilgilere erişmek şeklinde tezahür edilebilmektedir. Yetkisiz erişim kavramı yasal çerçeve ve siber suç tanımı açısından değerlendirildiğinde doğru bir yaklaşımdır, çünkü sisteme erişime yönelik eylemlerin çoğu yetkisiz erişim kullanılarak gerçekleştirilmektedir.

Bilgi sistemlerine erişim, kullanım haklarının derecesine bağlı olarak kısıtlanabilir. Böylece, bilgi sistemi sahipleri, başkalarının haklarına tecavüz etmemek kaydıyla, bilgi sisteminin kullanımını kısıtlayarak kendi mahremiyetlerini oluşturabileceklerdir. Ancak, sistem erişim eylemleri de yetkisiz erişimin bir parçası olarak düşünülmelidir. Bu, yetkilendirilmiş kısıtlı kullanıcının yetkisiz erişim suçu işleyip işlemediği ve kullanıcıların arasında yetki farkı olup olmadığı belirlenerek değerlendirilebilir. Erişim kısıtlama koşullarında farklılık yoksa suç oluşmayacağı savunulmaktadır. Sistem hesabında daha yetkin bir kullanıcı açısından, içeriğin hizmet dâhilinde kalması durumunda yasa dışı giriş ve kalış ihlali oluşmayacağı ifade edilmektedir.

Avrupa Konseyi Siber Suç Sözleşmesi (AKSSS) Açıklayıcı Raporu'nda belirtildiği üzere, sistem sahibinin veya sistemin tamamı ya da bir kısmı üzerinde hak sahibi olan kişilerin sistem içindeki eylemleri suç olmayacaktır. Kamu kullanımı için ücretsiz sistemlere erişim de cezalandırılmayacaktır. Ancak raporda, bu tür sistemlere erişimin yasalar dâhilinde olması gerektiği belirtilmiştir. Bu nedenle, erişim eyleminin bir hakka dayalı olarak gerçekleştirilmiş olması dikkate alınması gereken bir husustur. Bu hak, hukuka uygunluğun temeli olan rıza şeklinde kendini gösterebilir. AKSSS'ye göre yasa dışı erişim, bir bilgisayar sisteminin tamamına veya bir kısmına erişmek ve içeriği kullanmak sureti ile

10.5824/ajite.2022.04.004.x

oluşan suçların hepsini kapsamaktadır. Yargılama yetkisi ise mağdurun bağlı olduğu hukuk sisteminin yetkisi dâhilinde kalmaktadır.

Ancak BM'nin güncel anlaşma taslağına göre suiistimal, sisteme girmek veya sistemde kalmak gibi iki alternatif eylemden oluşan bir suç olarak düzenlenmiştir. Bu düzenleme ile sisteme yasa dışı girişleri engellemek bunu ihlal edenlere yaptırım uygulanmasının önü açmak hedeflenmiştir. Lakin bu konudaki yetkiye ilişkin uluslararası bir düzenleme henüz bulunmamakta olup her ülke kendi hukuki düzenlemeleri kapsamında yetki sahibidir.

2.3.2. İç Hukuk Açısından Yargılama Yetkisi

Türk Ceza Muhakemeleri Kanunu'na göre, işlenen suçlarda davaya bakma yetkisi, suçun işlendiği yerin mahkemesine aittir. Fakat bilişim suçlarının kendine özgü yapısından dolayı 2021 yılında yapılan değişiklikle, bilişim sistemlerinin araç olarak kullanıldığı suçlarda, mağdurun yerleşim yeri mahkemeleri de yetkili hâle getirilmiştir. Vatandaşlık bağı olsun ya da olmasın Türkiye'de bulunan bir mağdura karşı yapılan bilişim temelli saldırılarda yargılama yetkisi Türk makamlarına verilmiştir. Özellikle yurt dışı kaynaklı siber saldırılarda oluşan yetki sorunu bu şekilde aşılmıştır. Diğer devletlerin de kanun koyucular aracılığı ile benzer düzenlemeler getirerek siber suçlara karşı kendi yargı sistemlerini yetkili hâle getirmek için gerekli adımları attığı bilinmektedir. Uluslararası saldırılara karşı henüz tüm taraf devletleri bağlayıcı bir uluslararası düzenleme yapılmamış olması, bu konuda yerel makamlara daha büyük sorumluluk yükler hâle gelmiştir. AKSSS, bu konuda yapılan en kapsamlı çalışma olup taraf devletlerin iç hukuklarını da bu sözleşme kapsamında düzenlemeleriyle, ortak bir siber suç hukuku oluşturma amacına yönelik önemli bir adım atılmıştır. Yapılan düzenlemeler hem suçların tanımlanmasını hem de soruşturma ve kovuşturma aşamalarında iş birliği altyapısının oluşturulmasını sağlamıştır. Böylece, yerel hukuklar ve uluslararası sözleşmeler arasındaki çelişkiler giderilerek ortak bir anlayışın yerleştirilmesi sağlanabilecektir. Yine mütekabiliyet açısından bu durum önemli bir gelişme olup yapılan düzenlemenin genel kabul görmesi, mütekabiliyet esaslarında da genel kabul görmesinin önünü açacaktır.

Bu düzenlemeler ile Türk Ceza Kanunu'nun 243. Maddesinde değişiklik yapılmış ve yasa dışı erişim suç hâline gelmiştir. Daha önceki metinde sadece erişim suç olarak kabul edilmez iken AKSSS kapsamında yapılan değişiklik ile yasal dayanak olmadan bilgi sistemine girmek suçun oluşması için yeterli kabul edilmiştir. Yine yapılan düzenlemeler ile "kişisel verilerin kaydedilmesi" suçu (TCK 135. Madde) veya "verilerin hukuka aykırı olarak aktarılması veya müsadere edilmesi" (TCK 136. Madde) yasa koyucu tarafından düzenlenmiştir. Daha önceki düzenlemelerin aksine, yasa dışı erişim fiilinin suç olarak düzenlenmesi önemli bir gelişme olarak kabul edilmektedir.

5237 sayılı TCK'nın üçüncü kısım onuncu bölüm başlığı "Bilişim Alanında Suçlar" olarak değiştirilmiş, 243. Maddenin birinci fıkrasında bilişim sistemine yasa dışı olarak girme veya orada kalmaya devam etme fiilinin cezalandırılacağı düzenlenmiştir. AKSSS ve Türk Ceza Kanunu, bir suçun kasten işlenebileceğini belirtmektedir. Böylece, bir kişinin ihmal yoluyla bilgi sistemine girmesi suç teşkil etmeyecek olup ceza verilmesi için kasıt unsurunun bulunup bulunmadığı dikkate alınacaktır.

Türk hukuk normlarının AKSSS ile uyumlu hâle getirilmesi, bilişim suçlarına karşı yargılama esaslarında önemli bir rol oynamaktadır. AKSSS ile paralel düzenlemeler yoluyla uluslararası iş birliği sağlanabilmektedir. AKSSS'nin 2. Bölümündeki yasa dışı yaklaşımla ilgili olarak, "taraflardan her biri, bir bilgisayar sisteminin tamamına veya bir kısmına yetkisiz erişimin kasıtlı olarak yapılması hâlinde, kendi ulusal kanunlarına göre suç sayılması için gerekli yasal ve diğer önlemleri alacak" ifadesi ile tüm taraf ülkelerde bu yönde düzenlemelerin yapılmasını ve ortak bir hukuk oluşturulmasını sağlamıştır.

Literatürde, bilişim teknolojisinin doğası gereği, suç işleme fiilinin ve suçun sonuçlarının farklı yerlerde ortaya çıkabileceği belirtilmektedir; bu hususta suçun "mesafeli suç" olarak nitelendirildiği de ifade edilmiştir. Tartışmasızdır ki bilgi sistemine karşı işlenen suçların en önemli özelliklerinden biri, bilgi sistemine erişim fiilinin uzaktan gerçekleştirilebilmesidir. AKSSS, sisteme kablosuz ağlar üzerinden yakın mesafeden veya uzak mesafelerden erişilmesinin önemli olmadığını ifade ederek bu suçların farklı şekillerde işlenebileceğini düzenlemiştir. Katzman'a göre sistemdeki zafiyetlerden istifade ederek veya sistemde zafiyetler oluşturarak sistemin tamamına veya bir kısmına sızmak ya da kodları yakalayıp girmek arasında fark yoktur.

Siber suçların işleniş şekli ve teknolojik gelişmelerin failin bulunmasında her zaman yeterli olamadığı da dikkate alındığında, mücadele edilmesi zor bir suç türü olduğu ve bir devletin egemenliği dışında işlenen suçlara karşı uluslararası iş birliği yapılması gerektiği tartışmasızdır. Siber uzayda coğrafi ülke sınırlarının bulunmadığı göz önüne alınarak tüm devletlerin taraf olduğu ortak bir düzenleme yapılması, olası mağduriyetlerin önüne geçeceği gibi faillerin yakalanması ve olası saldırıların da engellenmesi için kritik bir önem arz edecektir. Mevcut düzenlemelerde ülkelerin iç hukuklarında benzer suç tanımları yaptığı görülmekte, fakat henüz faillerin tespiti için yeterli iş birliği gerçekleştirilememektedir.

- İtalya Ceza Kanunu 615. Maddesinde, güvenlik önlemleriyle korunan bilişim veya telematik sistemlerine yasa dışı bir şekilde girme veya yetkili kişinin rızası olmaksızın kalma fiili suç olarak düzenlenmiştir.

- Fransa Ceza Kanunu 323-1 maddesiyle bilgileri otomatik işleme tabi tutmuş bir sistemin tamamına veya bir kısmına aldatıcı hareketlerle erişmek veya kalmaya devam etmek cezalandırılmaktadır.

10.5824/ajite.2022.04.004.x

- Almanya Ceza Kanunu 202-a maddesine göre, herhangi bir kişi yetkisiz şekilde kendisi veya başkası için özel olarak korunan sistemden veri elde ederse üç yıla kadar hapis veya para cezasıyla cezalandırılmaktadır.

Somut örneklerin AB üyesi ve AKSSS'ye taraf ülkeler olması, beraber hareket etmelerini kolaylaştırmaktadır. Lakin gerekli düzenlemelerin çok daha kapsamlı bir şekilde yapılması ve BM nezdinde siber suçlara ilişkin özel bir birim kurulması ile birlikte, yapılan bu düzenlemeler, siber suçlarla mücadelede somut olarak daha etkili sonuçlar doğurabilecektir.

3. MÜTEKABİLİYET ESASI VE ULUSLARARASI SİBER GÜVENLİK POLİTİKALARI

3.1. Mütekabiliyet Esasları

3.1.1. Mütekabiliyet Kavramı

Mütekabiliyet ilkesi temel olarak ülkeler arası hukuk alanında öncelik kazanmıştır. Mütekabiliyet, özellikle diplomasi alanında ön plana çıkmış ve zaman içerisinde devletler arasında hukuk normlarının uygulanmasında yaygın olarak kullanılmaya başlanmıştır. Bu ilke, iki veya daha fazla taraf içeren ve devletler arasında imzalanan sözleşmelerle beraber teamül hukuku olarak yer edinmiştir. Bu bağlamda mütekabiliyet ilkesi, uluslararası hukukun ana kaynaklarında kendine yer bulan ve genellikle uluslararası hukuk tüzel kişilikleri tarafından uygulanan önemli bir ilke olarak karşımıza çıkmaktadır. Mütekabiliyet ilkesinin uluslararası sözleşmelere biçimsel anlamda dâhil edilmesi ile bu ilke uluslararası hukukta kullanılmaktadır. Mütekabiliyet ilkesi, uluslararası hukukta ve özellikle silahlı çatışma hukukunda en çok tartışılan ilkelerden biri olmuştur. Bu ilkenin fayda ve önleme olmak üzere iki işlevi olduğu söylenebilir.

Yararlanıcının rolü bağlamında, bireyler, ülkeler veya vatandaşlar, karşılıklılık koşullarına saygı gösteren uluslararası bir anlaşmada belirtilen hak ve menfaatlerden yararlanabilecektir. Engelleme işlevi bağlamında karşılıklılık koşulunun bulunmadığı durumlarda, bireyler, devletler veya vatandaşlar anlaşmada belirtilen hak veya menfaatlerden yararlanamayacaklardır.

Bu rollerin her ikisi de karşılıklılık ilkesinin izlenebildiği uluslararası anlaşmalarda belirtilmiştir, ancak zamanla, uluslararası sözleşmelerin bazı hükümlerinin mütekabiliyet ilkesiyle ilişkilendirilemeyeceği fikri gelişmiştir. Bu bağlamda örnek vermek gerekirse, 1951 tarihli Mültecilerin Hukuki Statüsüne İlişkin Cenevre Sözleşmesi içeriğinde hangi durumlarda sözleşme kapsamında mütekabiliyet ilkesinin engelleyici işlevinin uygulanamayacağı düzenlenmiştir. Bu ve benzer durumlarda, devletlerin anlaşmada öngörülen sınırlı hâllerde mütekabiliyet ilkesinin uygulanmasına istisna getirebilmeleri

mümkün olacağı gibi, hafifletme yoluyla uygulanmasını da kararlaştırabildikleri görülmektedir.

3.1.2. Uluslararası Diplomaside Mütekabiliyet

Mütekabiliyet kavramı temel olarak "karşılıklılık, karşılık verme veya yapılan olumlu ya da olumsuz eyleme karşılık gösterme" anlayışını ifade etmektedir. Mütekabiliyet kavramı, hukukun farklı dallarında farklı tanımlarla ifade edilebilmektedir. Uluslararası özel hukuk alanında, "başka bir devletin vatandaşlarına karşı tutumuna, yargı kararlarına veya herhangi bir davranış biçimine karşılık olarak başka bir devletin aynı tepkisi" anlamına gelmektedir. Bu bağlamda, "bir ülke, başka bir ülke vatandaşlarının kendi ülkesine girişinde vize talep etmiyor ise, o ülkenin de diğer ülkeden vize talep etmemesi" en basit anlamda mütekabiliyete örnek olarak gösterilebilir. Dolayısıyla karşılıklılık, ilgili uygulamaya aynı minvalde tepki gösterilmesi ya da karşılık verilmesi olarak ifade edilebilir.

Uluslararası özel hukuk alanında geniş bir kapsamı olan mütekabiliyet, en az iki devlet arasında geçerli olan ve bir devlette, başka bir devletin vatandaşları için aynı nitelikteki hakların tanınmasını ifade eden bir ilkedir. Başka bir tanıma göre, "bir yabancının devlette, devletinin yabancılara tanıdığından daha fazla hakkı yoktur." Devletlerin kendi ülkelerinde yabancılara haklar tanırken benimsedikleri ilke olan mütekabiliyet, aslında devletler arası eşitlik üzerine kuruludur. Diğer bir deyişle, en az iki ülke arasında var olabilen mütekabiliyet, bir ülke vatandaşının yabancı bir ülkede belirli haklardan yararlanabilmesi için, o yabancı ülke vatandaşlarının, ikamet ettikleri ülkede, fiilen aynı haklardan yararlanabilmesi anlamına gelir.

3.1.3. Mütekabiliyet Çeşitleri

Mütekabiliyet kavramı içerik açısından "belirli mütekabiliyet" ve "yaygın mütekabiliyet" olarak iki farklı şekilde incelenebilir. Özellikle ikili sözleşmelerde belirli mütekabiliyetten bahsedilirken, daha genel uygulamalarda yaygın mütekabiliyet kavramından bahsedilmektedir. Mütekabiliyet çeşitlerini kısasa kısas ya da karşılıklı bağımlı mütekabiliyet olarak ayırmak da mümkündür (Dost, 2015: 8).

Yapılan tanımlamalar doğrultusunda, mütekabiliyet esasının eş değer uygulama esaslarına dayalı olduğu görülmektedir. Mütekabiliyet kavramı, tarihsel süreç boyunca temel olarak uluslararası hukuk alanında kullanılmış olup zaman içerisinde hukukun farklı alanları içinde de uygulanmıştır. Uluslararası hukuk bazında mütekabiliyet kavramı, iki yahut daha çok taraf içeren uluslararası anlaşmalarda **teamül esaslı hukuk** olarak da yer almaktadır. Bu açıdan bakıldığında, mütekabiliyet olgusu uluslararası hukukun temel kaynaklarında bulunabilen ve uluslararası hukukun işlemesi gereken süreçlerde başvurulan esas olarak ortaya çıkmaktadır.

10.5824/ajite.2022.04.004.x

Mütekabiliyet terimi, uluslararası hukukun silahlı çatışmalar ile ilgili altyapısında en çok tartışılan ana ilkelerden biri olarak karşımıza çıkmaktadır. Temel olarak mütekabiliyet ilkesinde, **faydalanma** ve **blokaj koyma** olmak üzere iki zıt fonksiyon gösterilmektedir (Dost, 2015: 15). Faydalanma kapsamına giren bireyler, ülkeler veya vatandaşlar mütekabiliyet esasının bulunduğu uluslararası sözleşmelerde öngörülen haklar kapsamından yararlanabilmektedir. Blokajlama fonksiyonu ise mütekabiliyet esasının gerçekleştirilmediği durumlarda, ilgili ülkeler veya vatandaşların, anlaşma kapsamında bahsedilen haklardan yararlanamamasını ifade eder. Bununla birlikte, zaman geçtikçe bazı uluslararası sözleşme hükümlerinin mütekabiliyet esasına bağlanamayacağı ile ilgili tartışmalar da gündeme gelmiştir. Örneğin, insan hakları ya da mülteciler hukukuna ilişkin alanlarda, mütekabiliyet esasının blokajlama özelliğine istisna konulabilmektedir. Bu sayede ülkeler, sözleşme kapsamında belirtilen bazı durumlarda mütekabiliyet kavramının uygulanma esaslarına istisna getirebilmekte ya da yumuşatma yoluyla uygulamaya koyabilmektedir. Özellikle insan hakları hukuku kapsamında mütekabiliyet esası, taraflardan birinin esası ihlal etmesi hâlinde, bu uygulamamanın sadece ihlal eden ülkeyi değil, bütün sistemi etkileyebileceği gerekçesi ile kullanılmamaktadır. Böyle durumlarda, özellikle yaşama hakkı, dokunulmazlık ve adil yargılanma hakkı gibi temel haklarda mütekabiliyet esasının uygulanması, bu hakların doğasına aykırı olması nedeni ile kapsam dışında bırakılmaktadır.

3.2. AB ve NATO Tarafından Benimsenen Siber Güvenlik Politikaları

3.2.1. Avrupa Birliği Siber Güvenlik Kuralları

Avrupa Birliği (AB), üye devletlere veya adaylara çeşitli alanlarda gelişmeleri için rehberlik eden bir kuruluştur. Bu alanlardan biri de küresel dünyada güvenlik açısından son yıllarda giderek önem kazanan siber saldırılara karşı mücadele yöntemleri ve uluslararası arenada siber güvenliği sağlamaya yönelik tedbirler olmuştur.

AB, siber saldırılara karşı birçok yasal düzenleme ile tedbir alma yoluna gitmiştir. Bunun nedeni, AB'nin saldırılara aracısız müdahale edecek operasyonel kapasiteye de ilgili yasal kurumlara da sahip olmamasıdır. AB'de yürürlüğe giren yasal düzenlemelerle, üye devletlerin siber güvenliklerini artırmaları ve siber saldırılara karşı hazırlıklı olmaları beklenmektedir.

AB; üye devletleri, siber güvenlik alanındaki yatırımlarını artırmaya ve uzman yetiştirmeye teşvik etmektedir. Dolayısıyla, birliğin operasyonel yetenekleri veya yasal kurumları bulunmazken, üye ülkelerde belirlenen hedefler doğrultusunda yapılacak düzenlemeler ile ortak bir siber güvenlik anlayışı inşa edilmeye çalışılmaktadır.

Siber saldırıların ne zaman ve ne şekilde gerçekleşeceğinin öngörülemez olması, Avrupa Birliği'ne üye devletlerin siber güvenlik kurumları ve politikalarının sürekli olarak güncellemesine öncülük etmesini sağlamaktadır.

Bu kapsamda uygulanan yasal düzenlemeler ve kurallar arasında, 2004 yılında Avrupa Konseyi Siber Suç Sözleşmesi'nin kabul edilmesi, 2004 yılında AB Ağ ve Bilgi Güvenliği Ajansı'nın (ENISA) kurulması, 2005'te Bilgi Sistemleri Koruma Yönetmeliği'nin oluşturulması, 2013'te Europol Siber Suç Merkezi'nin kurulması, 2016 yılında Avrupa Siber Güvenlik Enstitüsü'nün (ECSO) kurulması gösterilebilir.

Siber saldırıların önlenmesinde bilgi güvenliği politikasının amacını, kapsamını ve düzeyini eksiksiz açıklayan belgelerin en önemlilerinden biri "yasal düzenlemeler"dir. Bununla birlikte hukuk normları, kamu politikasının resmî düzenlemelere yansıtıldığı, üzerinde anlaşmaya varıldığı siyasi normlardır. Siber saldırılarda kullanılan yazılımlar bu tür kurallarla engellenemezken, bu kötü amaçlı yazılımların kullanımının nasıl etki edeceğini ve vereceği zararın ne kadar hafifletilebileceğini daha baştan belirlemek mümkündür. AB, üye devletler için kuralları, direktifleri, yönetmelikleri ve yönergeleri belirlerken, üye devletler de AB kurallarına ve uluslararası anlaşmalara uyarak kendi iç hukuklarını bu şekilde düzenleyebilmektedirler. Bu şekilde, siber güvenlik tedbirleri, her ülke açısından birbirleri ile eş güdümlü olarak belirli bir seviyenin üzerinde tutulmaktadır.

AB'nin siber güvenliğe yönelik yaptığı ilk çalışmalardan biri, 2001'de çevrim içi dolandırıcılığa karşı yapılan kanun hükümleridir. Bu kanunlarla AB, tüm üye devletlerin internet ortamındaki dolandırıcılık faaliyetlerini (internet üzerindeki bilgi sistemlerine saldırı, bilgi hırsızlığı, yetkisiz erişim, kişisel bilgilerin ele geçirilmesi vb.) hukuken yasa ilan etmelerini istemiştir. Söz konusu düzenleme, suç tanımına farklı kavramlar ekleyerek siber suçlar için casus yazılımların oluşturulmasını, satın alınmasını, satılmasını ve kullanılmasını yasaklamıştır. Bu suçların faillerine 5 yıla kadar hapis cezası düzenlenmiş, üye devletlerin kişisel verilere erişmek ve bilgileri çalmak maksadıyla bu suçu kasten işleyen herkese ağır cezalar uygulaması tavsiye edilmiştir. Bu ilk düzenleme siber güvenliğin temellerini atmış ayrıca siber ortamda işlenmiş olan suçları cezalandırmak, caydırıcılık düzeyini artırmak için tasarlanmıştır.

3.2.2. Avrupa Birliği Ağ ve Bilgi Güvenliği Ajansı

Avrupa Ağ ve Bilgi Güvenliği Ajansı (ENISA) 2004 yılında ilgili yönetmelik (460/2004 sayılı AB Yönetmeliği) kapsamında kurulmuştur ve merkezi Yunanistan'ın Atina kentinde bulunmaktadır.

ENISA'nın esas misyonu, AB'deki ağ ve bilgi güvenliği problemlerini önleme ve bunlara yanıt verme yeteneğini artırmak amacıyla ulusal ve sendikal kapasiteyi geliştirmektir. ENISA, ağ güvenliği ve bilgi sistemleri ile ilgili olarak 2016/1148 direktifinin (NIS Direktifi) uygulanmasını desteklemek için ek özel roller ve sorumluluklar üstlenmiştir.

10.5824/ajite.2022.04.004.x

Ajansın faaliyetleri, tavsiye ve veri analizi sunmanın yanı sıra, AB yetkilileri ile üye devletler adına farkındalık ve iş birliğini artırmayı da kapsamaktadır.

ENISA'nın, stratejik hedeflere ulaşmak için dört temel amacı bulunmaktadır:

- Bilgi güvenliği konularında Avrupa Komisyonu'na üye devletlere tavsiye ve yardım,
- Avrupa'da artan riskler ve saldırılara ilişkin toplanan verilerin analizi,
- Risk değerlendirmesi ve risk yönetiminin teşviki,
- Farkındalık ve iş birliği alanında çalışmaların yapılması.

3.2.3. Avrupa Siber Güvenlik Organizasyonu

Kendi mali kaynakları bulunan ve kâr hedefi bulunmayan Avrupa Siber Güvenlik Organizasyonu (ECSO) 2016'da kurulmuştur. Kurumun asıl maksadı, AB'deki siber faaliyetlerle ilgili güvenlik önlemlerini artırmak, bu önlemleri güçlendirmek ve bu konuda yapılacak her şeyi desteklemektir. ECSO iştirakleri büyük şirketler, KOBİ'ler, araştırma merkezleri, üniversiteler, son kullanıcılar, operatörler, kümeler ve birliklerle beraber AB üye devletlerinin yerel, millî hükümetlerinden oluşmaktadır.

ECSO'nun asıl amacı, Avrupa siber güvenliğini geliştirmeyi ve geliştirmeye teşvik etmeyi amaç edinen her türlü adım veya projeyi destekleyerek[M.1][MVG2][MVG3]:

- Avrupa dijital pazarının ilerlemesini teşvik etmek ve siber tehditlerden sakınmak,
- Avrupa'da siber güvenlik pazarını geliştirmek, bununla birlikte büyüyen bir pazardaki konumu ile siber güvenlik sektörünün ve rekabetçi bilgi ve iletişim teknolojilerinin gelişmesini sağlamak,
- Avrupa'nın öncülük ettiği endüstri uygulamalarında güvenli tedarik zincirlerinin kritik aşamaları için siber güvenlik çözümleri geliştirerek uygulanmasını sağlamaktır.

3.2.4. Avrupa Konseyi Siber Suç Sözleşmesi

Avrupa Konseyi Siber Suç Sözleşmesi, 2001 yılında üye devletler tarafından imzaya açılan ve 2004 yılında yürürlüğe giren, siber suçlara ilişkin ilk uluslararası sözleşmedir. AB'de siber güvenlik konusunda kabul edilen en önemli yasal belge olmakla beraber, dünya üzerinde de bu alandaki en gelişmiş düzenlemedir. Türkiye anlaşmayı 10 Kasım 2010'da imzalamış, 2014 yılında bu amaçla hazırlanan 6533 sayılı Sanal Ortamda İşlenen Suçlar Sözleşmesi'ne ilişkin kanun meclisten geçerek yasalaşmıştır. Bu anlaşmada siber uzayı tamamen güvence altına almak imkânsız gibi görünse de ilgili anlaşma, Avrupa Konseyi üyeleri tarafından hazırlanan, zamanının en kapsamlı düzenlemelerinden birisidir. Avrupa Konseyi üyesi

olmayan birçok devletin de sözleşmeye taraf olması, düzenlemenin önemini artırmaktadır. Sözleşmenin Türkiye tarafından da imzalanarak gerekli düzenlemelerin yapılmış olması, Türkiye'nin de bu konudaki hassasiyetinin bir göstergesidir.

3.2.5. Avrupa Birliği'nin Siber Güvenlik Stratejisi

AB'de hayata geçirilen birçok siber güvenlik ve siber savunma uygulaması, diğer ülke ve kuruluşlar tarafından da örnek alınmıştır. Özellikle siber güvenlik konusunda atılan önemli bir adım, 2013'te AB Siber Güvenlik Politikası'nın temelini oluşturacak olan ve Avrupa Ekonomik ve Sosyal Komitesi ile Bölge Komitesi tarafından hazırlanan AB Siber Güvenlik Stratejisi Raporu'dur. "Açık, emniyetli ve güvenilir bir siber ortam" sloganı altında Avrupa ve uluslararası siber güvenlik politikasına rehberlik etmek üzere hazırlanan rapor, etkin siber güvenliğin sağlanması için temel hak ve özgürlükleri kısıtlamadan siber güvenlik politikasının uygulanması gereğine dikkat çekmektedir.

AB'nin dayandığı temel siber güvenlik ilkeleri şu şekilde belirlenmiştir:

- AB'nin esas değerlerinin dijitalde de korunması,
- Temel hak ve özgürlükler ile ifade özgürlüğü ve şahsi bilgi ve mahremiyetin korunması,
- İnternete herkesin erişiminin sağlanması,
- Yönetimde etkin katılımın sağlanması,
- Sorumluluğun paylaşılarak güvenlik hedefine ulaşılması.

Bu prensipler üzerine inşa edilen 2013 stratejisi, siber dayanıklılığı temin etmek için kamu-özel sektör ortaklıklarını, siber kapasiteyi, kaynakları ve verimliliği iyileştirmeyi amaçlamaktadır.

3.3. Dijital Tek Pazar Stratejisi

Dijital ekonominin esası güven ve güvenliktir. Bu nedenle AB, 2015 Mayıs'ında kamu ve özel sektör kuruluşlarının katılımıyla, birleşik bir dijital pazar stratejisi hazırlamıştır. Bu stratejinin amacı, Avrupa'nın rekabet gücünü artırmak ve üye ülkeler arasında güven inşa ederek inovasyon yoluyla siber güvenlik pazarının bölünmesini önlemektir. Üstelik bu izlemin Avrupa'daki dijital güvenlik endüstrisinin kaynaklarının oluşturulmasında ve koordinasyonunda etkili olması beklenmektedir. İzlem, yenilikçi küçük ve orta ölçekli şirketlerden bileşen ve ekipman üreticilerine, kritik altyapı operatörlerine ve araştırma enstitülerine kadar geniş bir oyuncu yelpazesini kapsamaktadır.

Siber güvenlikte etkin unsurlardan biri de kullanılan teknolojik sistemlerin üretildiği andan itibaren kontrol edilmesi ve dışa bağımlılıktan korunmasıdır. Bu nedenle AB, yerli kaynaklara yapılan her türlü yatırımı desteklemekte ve yatırım yapmaya teşvik etmektedir.

10.5824/ajite.2022.04.004.x

3.4. NATO ve Siber Güvenlik (Tallinn Kuralları)

Estonya'nın Ruslar tarafından dikilen Kızıl Ordu anıtını kaldıracağını açıklamasının ardından yaklaşık bir ay boyunca siber saldırılara maruz kalması, birçok kamu hizmetinin sağlanmasını engellemiş ve devlet kurumlarını işlevsiz hâle getirmiş ve bu saldırılar da siber güvenlik literatüründe önemli bir yer edinmiştir. Birçok devlet bu saldırılar neticesinde siber tehditlerin önemini kavramış ve bu konuda önlemler almaya başlamıştır. Bu kapsamda NATO, 2008 yılında Bükreş'te bir zirve gerçekleştirmiş, bu zirvede alınan kararlara göre, NATO Siber Savunma Yönetimi Otoritesi'nin ve Estonya Tallinn merkezli bir NATO Siber Savunma Mükemmeliyet Merkezi'nin kurulması kararlaştırılmıştır. Bu siber saldırı, uluslararası ilişkilerde siber güvenliğin ilk alarm zilini çaldırarak uzun ve derin bir etki yaratan önemli saldırılar arasında yerini almıştır.

Siber Savunma Mükemmeliyet Merkezi, milletlerarası bağımsız uzmanlardan oluşan bir ekibi Siber Savaşa Uygulanacak Kanunlara İlişkin Tallinn Kılavuzu'nu hazırlamaya davet etmiş ve üç yılın sonunda modern uluslararası hukukun ne ölçüde uygulanacağına dair çalışma tamamlamıştır.

Bu rehber, siber savaşın hangi hâllerde haklı sebebe dayandığını, siber savaş devam ederken hangi kurallara uyulması gerektiğini ve devletlerin millî politikaları kapsamında kuvvet kullanımına ilişkin ilkelerini içermektedir.

Bu kaynak, bağımsız uzmanların görüşlerini içermekte olup bağlayıcı bir özelliği bulunmamaktadır. NATO üyesi ülkelerin resmî söylemlerini de temsil etmeyen bu kaynak, Cambridge Üniversitesi tarafından Mart 2013'te basılmıştır. Kitabın hazırlanmasına katkıda bulunan uzmanlardan hukuk alanı çalışanları; Chatham House, Kanada Askerî Başsavcılığı, Avustralya Savunma Kuvvetleri, Almanya Postdam Üniversitesi, Amsterdam Üniversitesi, Teksas Hukuk Fakültesi, İsveç Millî Savunma Koleji, Cenevre Güvenlik Çalışmaları Merkezi ve ABD Donanma Koleji gibi kurumların bünyelerinden, teknik uzmanlar ise NATO Siber Savunma Mükemmeliyet Merkezi çalışanlarından seçilmiştir. Siber Savaşta Uygulamaya Koyulacak Hukuk üzerine düzenlenen Tallinn El Kitabı "Uluslararası Siber Güvenlik Hukuku" ve "Siber Silahlı Çatışma Hukuku" başlıklı iki ana bölümden oluşmaktadır.

Uluslararası Siber Güvenlik Hukuku bölümü,

- Devletler ve Siber Uzay (Egemenlik, Yargılama Yetkisi ve Kontrol ve Devlet Sorumluluğu)
- Güç Kullanımı (Güç Kullanımının Yasaklanması / Meşru Savunma / Uluslararası Kuruluşların Faaliyetleri) alt başlıklarından ve uluslararası teamül hukukuna ilişkin (Uluslararası Ceza Mahkemesi'nce de esas alınan) 1907 Lahey Mevzuatı ve 1949

tarihli Cenevre Konvansiyonu'nda kabul edilen mevcut düzenlemeler kapsamında bağımsız uzmanlar tarafından düzenlenen kurallardan oluşmaktadır.

Siber Silahlı Çatışma Hukuku,

- Genel Olarak Siber Silahlı Çatışma Hukuku
- Düşmanca Davranışlar (Silahlı Çatışmaya Katılma / Saldırı Türleri / Savaş Hâlinin Araçları ve Metotları / Saldırıların Yönetimi / Önlemler / Uygun Olmayan Kullanım ve Casusluk / Kuşatma ve Bölgeler)
- Belirli Kişiler, Nesneler ve Faaliyetler (Tıbbi, Dinî Personel ve Tıbbi Birimler, Ulaşım ve Malzeme Birimleri / Birleşmiş Milletler Personeli, Tesisat, Malzemeler, Birimler ve Ulaşım / Tutuklu Kişiler / Çocuklar / Gazeteciler / Tehlikeli Güçleri İçeren Tesisler / Sivil Halkın Hayatta Kalması İçin Gözden
- Çıkarılabilir Nesneler / Kültürel Varlıklar / Doğal Çevre / Diplomatik Arşiv ve İletişim / Toplu
- Cezalandırma / İnsani Yardım)
- İşgal
- Tarafsızlık alt başlıklarının ve ilgili kuralların düzenlenmesiyle hazırlanmıştır.

"Devletler ve Siber Uzay (Egemenlik, Yargılama Yetkisi ve Kontrol ve Devlet Sorumluluğu)" başlığı altında on beş adet kural düzenlenmiştir.

Tallinn Kılavuzunun önemi, siber savaş hukuku üzerine günümüze dek yapılmış en kapsamlı çalışma olmasıdır. Bağımsız uzmanların uluslararası hukuk doktrinlerinden esinlenerek siber savaşa ilişkin tanımları ve olması gereken uygulamaları düzenlediği bu kılavuzun henüz bir bağlayıcılığından söz etmek mümkün olmamasına karşın bu konudaki çalışmalara önemli bir kaynak teşkil ettiği tartışmasızdır. Nisan 2013'te yayınlanan Tallinn Kılavuzu bu tarihten sonra güncellenmeye devam etmiş ve genişletilmiş yeni versiyonu Tallinn 2.0 adı ile Şubat 2017'de yayınlanmıştır. Bu tarihten sonra da yeni güncellemeler eklenerek rehberin daha kapsamlı bir doktrin kaynağı hâline getirilmeye amaçlandığı bilinmektedir. Uluslararası hukuk doktrinlerinin geçerliliğinde en önemli etken devletler tarafından kabul görmesi ve uluslararası anlaşmalarda atıf yapılarak imza altına alınmasıdır. Siber savaş hukuku henüz bu konudaki çalışmaların çok yetersiz olduğu bir alan olmasına rağmen siber saldırıların artması ve verilen zararların dünya gündemini daha çok meşgul etmesi ile yakın zamanda bu konuda bir uluslararası düzenlemeye gidilmesi kaçınılmaz görünmektedir. Özellikle tezimizin konusunu oluşturan siber savaşta mütekabiliyet esaslarını düzenleyecek bir anlaşmanın Birleşmiş Milletler nezdinde ivedilikle tasarlanması ve üye devletlerin imzasına sunulması gerekmektedir. Verdiğimiz örneklerde de görüldüğü üzere günümüzde devletler arasında yaşanan her krizin ardından siber saldırılar yapılmakta ve yeni saldırının etkisi bir öncekinden daha ağır olmaktadır. Saldırılar devletler arasında olmasına rağmen sonuçlarından siviller de etkilenmektedir. Teknolojik imkânların gelişmesi

10.5824/ajite.2022.04.004.x

ile siber saldırılar yakın gelecekte konvansiyonel silahların verdiği zararlardan daha etkili olabilecektir. Tüm bu nedenlerle siber saldırıların caydırıcı hâle getirilebilmesi için tıpkı savaş suçları yargılamalarında olduğu gibi siber savaş hukukunun uluslararası camia tarafından kabul edilmesi ve özellikle mütekabiliyet esaslarının belirlenmesi ivedi bir ihtiyaçtır.

SONUÇ

Bu çalışma siber uzay, siber saldırı ve siber savaş kavramları bağlamında siber saldırıların tespit edilmesi ve sorumlulukların isnat edilmesi üzerine genel bir değerlendirme yapılmayı daha sonra ise siber tehdit ve siber savaş sırasında uygulanması gereken mütekabiliyet esası temel alınarak siber saldırılara nasıl mukabele edileceği ile ilgili tartışmalara yer vermeyi amaçlamaktadır. Bu temel amaç doğrultusunda çalışmada genel olarak siber uzay, siber saldırı, siber savaş, güvenlik ve mütekabiliyet kavramların incelemesi yapılmıştır. Bilgi ve iletişim teknolojisinde yaşanan hızlı gelişme sonucunda bilgi hızlı bir şekilde fiziksel dünyadan zaman ve mekân kısıtlamasının olmadığı bilgisayar ve elektronik tabanlı sanal dünyaya doğru taşınmıştır. Bilgisayar ve elektronik tabanlı sistemlerin bulunduğu bu ortama siber ortam denilmektedir. Hızlı teknolojik gelişmenin zaman ve mekân kısıtlamasını ortadan kaldırmasıyla ülkeler kendileri açısından stratejik öneme sahip olan sağlık, enerji, ulaşım, haberleşme, bankacılık gibi altyapı sistemlerini bilgi otomasyon sistemlerini siber ortamda kontrol etmeye başlamıştır. Bu değişiklik sağladığı birçok faydanın yanında ülkelerin güvenlik risklerini ve uğradıkları tehditlerin kaynağını ve boyutunu da çeşitlendirerek birtakım dezavantajları da beraberinde getirmiştir. Söz konusu tehdit ve güvenlik risklerinin önceden tahmin edilmesi zorlaşmış bu da güvenlik ortamının kompleks ve belirgin olmayan bir yapıya sahip olmasına neden olmuştur. Siber ortam anılan nitelikleri bünyesinde barındırarak risk ve tehditlerin kullanılmasıyla yeni bir mücadele alanı hâline gelmiştir. Bununla birlikte bilginin gizliliği, erişilebilirliği ve bütünlüğünün sağlanması ülkeler için kritik hâle gelmiştir.

Uluslararası ilişkiler literatüründe sıkça anılan çatışma, güvenlik ve tehdit gibi hususların konvansiyonel kullanımları siber ortam ile birlikte dönüşüme uğramıştır. Değişen bu kullanım biçimleri daha etkili ve geniş ölçekte önem kazanmaya başlamıştır. Siber ortamın güvenliğe yönelik tehditlerin farklılaştırması ile yeni bir güvenlik tanımlaması gerekliliği ortaya çıkmıştır. Bunun nedeni konvansiyonel tehdit anlayışının ve mücadele yöntemlerinin yeni güvenlik risklerini önlemede yetersiz kalmasıdır. Bu durum da güvenlik kavramının yeniden ele alınarak yeni mücadele yöntemlerinin uygulanmasını zaruri kılmıştır. Güvenlik algısındaki yaşanan değişimler, Avrupa Birliği ve NATO dengesi başta olmak üzere küresel alanda için yeni bir güvenlik anlayışının doğmasına neden olmuştur. Siber ortamda yaşanan tehditler yalnızca siber ortamdaki aktörleri değil onun dışındaki

hayatı doğrudan etkileyen birçok kamu hizmetinin de güvenliğini sarstığı için söz konusu hizmet altyapılarının da güvenliği önem kazanmıştır.

Bu zaruret devletlerin ulusal güvenliklerini sağlamada yetersiz kaldığı noktalarda uluslararası iş birliğine ve NATO gibi örneklerin ortaya çıkmasına sebep olmuştur.

Bir siber saldırı sırasında o saldırının boyutunun ne olduğunu ve buna verilecek meşru tepkinin nasıl olması gerektiğini ilk anda belirlemek çoğu zaman imkânsızdır. Saldırının kapsamı saldırının gerçekleşmesinden sonra yapılacak detaylı analiz ile ortaya konulabilir. Nitekim uluslararası kamuoyu, şimdiye dek uluslararası siber saldırıların silahlı saldırıya dönüştüğüne tanık olmamıştır. Yalnızca saldırının tespitinin bir yıl gibi uzun bir süre almasından dolayı İran'ın uranyum zenginleştirme tesisine yönelik 2009 yılında gerçekleştirilen Stuxnet saldırısı ile verilen zararın silahlı saldırı eşine ulaştığına yönelik değerlendirmeler yapılmıştır. Bu durumda zarar gören ülkenin meşru müdafaa hakkı bulunduğu varsayılırsa dahi bu hak kapsamında gösterilecek mukabelenin ivedilik ve gereklilik kriterlerini karşılamaması nedeniyle saldırgana yönelik meşru müdafaa hakkını vermemektedir. Siber saldırıların birbiriyle eş zamanlı şekilde gerçekleştirilmesi saldırganların amacının veya kimliğinin tespit edilmesini zorlaştırmaktadır. Bu zorluktan dolayı uluslararası sistem ülkelerin kullanabileceği meşru müdafaa seçeneklerini sınırlandırmakta ve milletlerarası hukuku kurallarını ihlal etmeden etkin bir mukabelede bulunmayı zorlaştırmaktadır. Unutulmamalıdır ki bir ülkenin meşru müdafaa hakkından doğan karşılık verme seçeneğini kısıtlamak; ülkeleri, bireyleri ve terör örgütlerini gittikçe daha sert ve şiddetli siber saldırılar yapmaya teşvik edebilmektedir. Bütün bu nedenlerle sadece bölgesel değil küresel anlamda daha kapsayıcı bir anlaşmanın yürürlüğe girmesi, siber savaş hukukunun kurallarını ve mütekabiliyet esaslarını devletlerin bu sözleşmeye taraf olup olmaması üzerinden belirleyici olacaktır. Başta BM olmak üzere tüm uluslararası hukuk süjelerinin bu konuda ivedi ve kapsamlı bir çalışma yapılması muhtemel uluslararası krizlerin önüne geçecektir.

KAYNAKÇA

Ada, M. (2018), "NATO Üyesi Ülkelerin Siber Güvenlik Stratejileri Açısından İncelenmesi", Yüksek Lisans Tezi, Gazi Üniversitesi Bilişim Enstitüsü.

Akyeşilmen, N. (2016b), "Cybersecurity and Human Rights: Need for a Paradigm Shift?", *Cyberpolitik Journal*, *1*(1), 32-55.

Auerswald, D. P. (2004), "Explaining wars of choice: an integrated decision model of NATO policy in Kosovo", *International Studies Quarterly*, *48*(3), 631-662.

Başaranoğlu, E. (2016), Bilgi Güvenliği Unsurları. https://www.siberportal.org/blue-team/securinginformation/concepts-of-information-security

Bayraktar, G. (2015), *Siber Savaş ve Ulusal Güvenlik Stratejisi*. Yeniyüzyıl Yayınları.

Berner, S. (2003), "Cyber-terrorism: reality or paranoia?", *SA Journal of Information Management*, *5*(1), 4.

Bıçakçı, S. (2012), "Yeni savaş ve siber güvenlik arasında NATO'nun yeniden doğuşu", *Uluslararası İlişkiler Dergisi*, *9*(34), 205-226.

Bıçakçı, S. (2014), "NATO'nun gelişen tehdit algısı: 21. yüzyılda siber güvenlik", *Uluslararası İlişkiler Dergisi*, *10*(40), 100-130.

Brent, Laura (2019), NATO'nun siber uzaydaki rolü, https://www.nato.int/docu/review/tr/articles/2019/02/12/natonun-siber-uzaydakirolue/index.html

Chen, T. ve Walsh, P. J. (2009), *Guarding against network intrusions*, (Edited by: John R. Vacca), Computer and Information Security Handbook, Morgan Kaufmann Publishers.

Choucri, N. (2012), *Cyberpolitics in international relations*. MIT press.

Daban, C. (2016), "Siber Güvenlik ve Uluslararası Güvenlik İlişkisi", *Cyberpolitik Journal*, *1*(1), 78-94.

Darıcılı, A. B. (2016), *NATO'nu Siber Güvenlik Stratejisi'nin Analizi,* (Editörler: Tayyar Arı ve Barış Özdal), Uluslararası İlişkiler Konferansı- Uluslararası Sistemde Yeni Düzen Arayışları. 21-22 Ekim. Dora Basım.

Dost, S. (2015), "Milletlerarası Hukukta Mütekabiliyet İlkesi", *S.D.Ü. Hukuk Fakültesi Dergisi*, Cilt: 5, Sayı: 2, s. 1-37.

Çakmak, H., & Demir, C. K. (2009), *Siber Dünyadaki Tehdit ve Kavramlar*, (Editör: Haydar Çakmak ve Taner Altunok), Suç, Terör ve Savaş Üçgeninde Siber Dünya. Ankara: Barış Platin Kitabevi, 2355.

Çavuş, N. (2018), *NATO, Siber Saldırlar ile Nasıl Mücadele Ediyor?* https://www.webtekno.com/natosiber-saldirilar-ile-nasil-mucadele-ediyor-h47666.html

Çelik, S. (2018), Siber Uzay ve Siber Güvenliğe Multidisipliner Bir Yaklaşim. *Academic Review of Humanities and Social Sciences*, *1*(2), 110-119.

Çeliktaş, B. (2016), "Siber Güvenlik Kavramının Gelişimi ve Türkiye Özelinde Bir Değerlendirme", Yüksek Lisans Tezi, Karadeniz Teknik Üniversitesi Sosyal Bilimler Enstitüsü.

Çiftçi, H. (2013), *Her Yönüyle Siber Savaş* (Birinci Baskı), Ankara: TUBİTAK Popüler Bilim Kitapları.

Çiftlioğlu, E. (2008), *Gri Tehdit Terörizm*. Başak Matbaacılık ve Tanıtım Ltd. Şti.

Çubukçu, A., & Bayzan, Ş. (2013), "Türkiye'de dijital vatandaşlık algısı ve bu algıyı internetin bilinçli, güvenli ve etkin kullanımı ile artırma yöntemleri", *Middle Eastern & African Journal of Educational Research*, *5*, 148-174.

Garber L. (1999), Melissa Virus Creates a New Type of Threat, *Computer*, pp. (16-19), Vol. 32, No. 6. https://www.computer.org/csdl/magazine/co/1999/06/r6016/13rRUwh80Ks

Goodman, W. (2010), "Cyber deterrence: Tougher in theory than in practice?", *Strategic Studies Quarterly*, *4*(3), 102-135.

Gözükeleş, İ. (2014), Tarihten Örneklerle Siber Savaş. https://bilimvegelecek.com.tr/index.php/2014/09/01/tarihten-orneklerle-siber-savas/

Gürsoy, Y. (2013), *Türkiye'de Sivil-Asker İlişkilerinin Dönüşümü*, (1. Baskı). İstanbul Bilgi Üniversitesi Yayınları.

Kozłowski, Andrzej (2020), Comparative analysis of cyberattacks on Estonia, Georgia and Kyrgyzstan. *European Scientific Journal,* Vol.3 Special Edition, 1-14.

Martellini, M. (2013), *Cyber security: Deterrence and IT protection for critical infrastructures*. Springer International Publishing.

NATO (2016). Warsaw Summit Key Decisions. February 2017. Erişim Tarihi: 23 Temmuz 2019, https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2017_02/20170206_1702factsheet-warsaw-summit-key-en.pdf

Tarhan, Kamil (2017). "Siber Uzayda Realist Teorinin Değerlendirilmesi", Cyberpolitik Journal, 2 (3), 105124.

Sertçelik, Aşır (2015), "Siber Olaylar Ekseninde Siber Güvenliği Anlamak", *Medeniyet Araştırmaları Dergisi,* Cilt: 2 Sayı: 3, s. 25-4.

Şentürk, H., Zaim, A., & Sarıoğlu, A. (2012), "Cyber security analysis of Turkey", *International Journal of Information Security Science*, *1*(4), 112-125.