SİBER GÜVENLİĞİN SAĞLANMASINDA ULUSLARARASI HUKUKUN VE TÜRK HUKUKUNUN ROLÜ

The Role of Internatıonal Law and Turkish Law in Providıng Cyber Security

Merve ERDEM[*], Gürkan ÖZOCAK[**]

ÖZ

Teknolojinin gelişmesiyle birlikte, enerji, haberleşme, su kaynakları, tarım, sağlık, ulaşım, eğitim ve finansal hizmetler gibi kritik altyapı sektörlerinde faaliyet gösteren kamu kurumları ile özel kurum ve kuruluşlar bilgi ve iletişim teknolojilerini kullanmaya başlamışlardır. Ancak siber ortamın, önemli kamu hizmetlerinde ve özel kişilerin sağladığı hizmetlerde kullanılması, beraberinde yeni bir güvenlik sorunu; aynı şekilde özel şahısların pek çok faaliyetine sirayet eden bilgisayar kullanımı, beraberinde yeni bir suç tipi doğurmuştur. İşbu noktada siber güvenlik, siber faaliyetlerin aksamasının yaratacağı sonuçlar göz önüne alındığında hem ulusal hem de uluslararası bir mesele olarak karşımıza çıkmaktadır. Dolayısıyla, siber güvenliğin sağlanması ve muhafazasında hem ulusal hukuk düzeninin hem de uluslararası hukuk düzeninin rolü yadsınamaz.

Anahtar Kelimeler: Siber güvenlik, siber uzay, kuvvet kullanma yasağı, meşru müdafaa hakkı, siber suçlar, Türk Ceza Kanunu bilişim suçları.

ABSTRACT

Along with the development of the technology, public facilities and private facilities which operates at the critical infrastructures like energy,

Makalenin geliş tarihi: 04.06.2018 **Makalenin kabul tarihi:** 01.04.2019

[*] Dr., Ankara Üniversitesi Hukuk Fakültesi, Milletlerarası Hukuk ABD., Ankara, erdemm@ankara.edu.tr.

[**] Avukat, İstanbul Barosu, Ankara Üniversitesi Sosyal Bilimler Enstitüsü Kamu Hukuku (Ceza ve Ceza Usul Hukuku) Doktora Programı Öğrencisi, gurkanozocak@gmail.com.

communication, water resources, agriculture, transportation, education and financial services have started use information and communication technologies. However, the utilization of cyber platform for the public services and the services provided by the private persons has raised a brand new security problem, in the same way the computer usage which spread into private person's a lot of activities has caused to create a brand new crime type. At this point cyber security constitutes a national and international issue, considering the consequences which are caused by the hitch of the cyber activities. Therefore, the role of national and international law cannot be ignored to provide and to maintain the cybersecurity.

Key Words: Cybersecurity, cyber space, prohibition of the use of force, the right of self-defence, cyber crimes, cybercrimes in Turkish Criminal Code.

I. GİRİŞ

Siber uzay, internet, telekomünikasyon, bilgisayar sistemleri, intranet, hücresel teknolojiler, kablo ve uydu iletişim servisleri gibi teknik bileşenlerden oluşan ve sınırları olmayan küresel bir platformdur.[1] Siber uzay, kendisini oluşturan bileşenler itibariyle, tüm insanlığın ortak hafızası olarak nitelendirilmekte, siber faaliyetlerin işlemesini sağlayan lojistik unsurlar da ortak mal olarak kabul edilmektedir. İşbu nitelik, siber uzayda devlet egemenliği veya mülkiyet hakkı tesis edilmesini imkânsız kılmaktadır.[2]

---

[1] "Defense Department Cyber Efforts: Definitions, Focal Point and Methodology Needed for DOD to Develop Full-Spectrum Cyberspace Budget Estimates, US Department of Defense, Memo CM-0477-08" 2011, bkz. http://www.gao.gov/ assets/100/97674.pdf (e.t. 01.04.2018); KITTICHAISAREE, Kriangsak, Public International Law of Cyberspace, Springer, Switzerland, 2017; NYE, Joseph S., *"The Regime Complex for Managing Global Cyber Activities",* The Centre for International Governance; Global Commission on Internet Governance: Paper Series No. 1, 2014, s. 2; WEBER, Rolf H., *"Elements of a Legal Framework for Cyber Space",* Swiss Review of International and European Law, Vol. 26, No. 2, 2016, s. 196; ZIOLKOWSKI, Katharina, *"General Principles of International Law as Applicable in Cyberspace",* in Peacetime Regime for State Activities in Cyberspace International Law, International Relations and Diplomacy NATO CCD COE Publication, Tallinn, 2013, s. 155.

[2] NYE, s. 3; OSTROM, Elinor vd., Revisiting the Commons: Local Lessons, Global Challenges*,* Science, 1999, s. 278; RAYMOND Mark, *"Puncturing the Myth of the Internet as a Commons",* Georgetown Journal of Internet Affairs, Special Issue, 2013, s. 5- 15, 58. Nitekim internet Kaliforniya Üniversitesi'nde gerçekleştirilen devlet destekli bir araştırma sonucu ortaya çıkmış ve zaman içerisinde gelişerek bugünkü şeklini almıştır. Özellikle 1990'larla birlikte toplum hayatına dahil olmaya başladığında, *Elektronic Frontier Foundation* tarafından, internetin insanlara ait ve serbest bir alan olduğu, devlet

Ancak devletlerin kendi ülkesinde bulunan siber altyapı ve siber faaliyetleri kontrol altına alması, siber güvenliğe ilişkin gerekli hukuki düzenlemeleri oluşturup yaptırım mekanizmaları oluşturması, siber uzayda bir nevi egemenlik hakkı kullandıklarını da göstermektedir.[3]

Devlet kontrollü ancak aynı zamanda tüm insanların ortak hafızası olan siber uzay, yaşamımızı kolaylaştırarak hayatımızın merkezine girmiştir. Ancak yıllar içinde giderek insanlığı olumsuz yönde etkileyen faaliyetlerin işlendiği bir alan haline gelmiştir. Siber suçlar bunun bir boyunu oluştursa da insanoğlunu aslında daha büyük bir tehlike beklemektedir. Çünkü klasik çatışma mekanlarına ek olarak, siber uzayın da artık yeni bir çatışma alanına dönüştüğü ifade edilmektir.[4] Devletler, devlet faaliyetlerini yürüten sistemlerini dijital dünyaya entegre ettikçe, siber saldırılara karşı bir o kadar savunmasız hale gelmektedirler. Siber saldırı neticesinde, devletler bünyesinde oluşturulan belli altyapıların gizliliği, birliği bozulabilmekte, bilgi, kaynak ve herhangi bir işleme ulaşım etkilenebilmekte, kamu hizmetleri kilitlenebilmektedir.[5] Siber dünyada meydana gelen düzensizlik, uluslararası barış ve güvenliği, artık dünyayı terörizm tehlikesi, sınır aşan organize suçlar, açlık, salgın, çevre sorunları kadar etkileyecek derecededir.[6]

Siber saldırıların farklı nitelikleri bulunmaktadır. Bilgisayar sistemlerine, verilere saldırıda bulunan, bu sistemlerde kalan, verileri çalan, elinde tutan, bu faaliyetler yoluyla dolandırıcılık, sahtecilik yapan kişi ve guruplar işbu saldırılarla siber suç işlemiş olmaktadır. Dünyayı yaygın olarak etkiyen bu adi suç, 378 milyon dan fazla kişiyi etkilemiş, mağdurları 113 bilyon dolar maddi

---

egemenliğinde olamayacağına ilişkin bir bildirge yayınlanmıştır. BARLOW, John Perry, A Declaration of the Independence of Cyberspace, ELECTRONIC FRONTIER FOUND., 8 February 1996), bkz. https://www.eff.org/ cyberspace-independence (e.t. 15.04.2018).

3 LOTRIONTE, Catherine, *"State Sovereignity and Self Defence in Cyberspace: A Normative Framework for Balancing Legal Rights",* Emory International Law Review, Vol. 26, 2012, s. 829.

4 GERVAIS, Michael, *"Cyber Attacks and the Laws of War",* Berkeley J. Int'l L., Vol. 30, 2012, s. 526.
Aksi görüş için bkz. RID, Thomas, "*Cyber War Will Not Take Place",* Journal of Strategic Studies, Vol. 35, Iss. 1, 2012, ss. 5- 32.

5 "US National Security Strategy" (May 2010), s. 27, http://www.whitehouse.gov/sites/ default/files/rss_viewer/ national_security_strategy.pdf, (e.t.30.03.2018).

6 LOTRIONTE s. 828. Ayrıca 21. yüzyılda bit ve byteların, silahlar kadar tehlikeli olduğun yorumu için bkz. Remarks on the Department of Defense Cyber Strategy, As Delivered by Deputy Secretary of Defense William J. Lynn, III, 14 July 2011, http://archive.defense.gov/speeches/speech.aspx?speechid=1593 (e.t. 15.04.2018)

kayba uğratmıştır. 1,966,324 bilgisayar, kişilerin banka hesaplarına sızmak için geliştirilen zararlı yazılımlardan etkilenmiştir. Hatta işbu nitelikteki suçlara devletler de maruz kalmıştır. 2016 yılında Bangladeş Merkez Bankası'ndan 101 milyon dolar sadece siber saldırı yoluyla çalınabilmiştir.[7]

Diğer saldırı türü de dağıtık hizmet aksatma saldırılarıdır. Söz konusu saldırılardan özellikle 2007 yılında Estonya etkilenmiş, hatta bu saldırı insan hayatını tehlikeye atacak boyuta gelmiştir. Çünkü acil durum aramaları servisi bir saat kadar devre dışı kalmıştır. Yine 2008 Ağustos ayında, Rusya ile Gürcistan arasındaki askeri gerilimde, Rusya'nın Güney Osetya'yı işgali esnasında, Gürcistan'ın internet üzerinden dünyayla bağlantısı kesilmiştir. İkinci saldırı türü de kusurlu veri yerleştirme saldırısıdır. İşbu saldırı, dağıtık hizmet aksatma saldırısından daha karmaşık olup bilgisayarların düzgün çalışıyormuş gibi görünmesini sağlar. Örneğin, İsrail 2007 yılında Suriye'deki nükleer tesisleri bombaladığında, Suriye hava radar sistemine yapılan siber saldırı sonucu, radar sistemi İsrail savaş uçaklarını tespit edememiştir. Siber saldırının başka bir türü de Güvenli Bilgisayar Ağına sızmaktır. Örneğin İran'ın nükleer tesislerinin bilgisayar sistemine sızan Stuxnet virüsü, nükleer tesislerin çalışmasını sekteye uğratmak için tasarlanmıştır.[8]

Yukarıda da görüldüğü üzere siber uzayda güvenlik giderek önemli bir mesele haline gelmekte ve uluslararası toplumu yakından ilgilendirir hale gelmektedir.[9] Bu noktada siber güvenliği sağlamaya ilişkin klasik hukuk araçlarının nasıl kullanılabileceği sorusu akla gelmektedir. Siber güvenliği tehdit eden siber saldırılarla mücadele etmek adına gerek uluslararası gerek ulusal hukuk araçlarında, adi bir suç olarak siber suçların düzenlendiğini ve devletler arasında siber suçlarla mücadele etmek adına işbirliği adımları atıldığı görülmektedir.[10] Adi bir suç olarak, siber suçlar da siber güvenliği

---

7 Veriler için ve ayrıntılı bilgi için bkz. KITTICHAISAREE, ss. 263- 270.

8 Ayrıntılı bilgi için bkz. HATHAWAY, Oana vd., *"The Law of Cyber-Attack,"* CALIF. L. REV., Vol. 100, 2012, ss. 837 – 839; SCHMIT, Michael, "*Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework*", COLUM. J. TRANSNAT'L L. Vol. 37, 1999, ss. 914-15.

9 NYE, s. 11.
Siber güvenlik olarak karşımıza çıkan bu husus, siber uzayda gizliliği, birliği, bilgi, kaynak ve işlemlere ulaşılabilirliği koruma çabasını ifade etmektedir. GUIORA, Amos, Cybersecurity, Geopolitics, Law and Policy, Routhledge, NewYork, 2017, s. 4.

10 Bkz. ERDEM Merve/ ÖZOCAK Gürkan, *"Sınıraşan Bir Suç Olarak Siber Suçlarla Mücadelede Uluslararası İşbirliği*", 19. Akademik Bilişim Konferansı, 8-10 Şubat 2017, Aksaray Üniversitesi, Aksaray.

tehdit eden suçlardan olmakla birlikte, siber güvenlik açısından özellikle toplumları geniş çaplı etkileyen siber saldırılar ve siber terörizmin boyutu ve olası etkileri karşısında klasik uluslararası hukuk ve iç hukuk mekanizmalarında yer alan önlemlerin neler olduğunu tespit etmek de önem arz etmektedir.[11] İşbu çalışmamızın odak noktasını, uluslararası hukuk ve iç hukuk sistemlerinin, özellikle Türk hukuk sisteminin, siber güvenliği nasıl tesis edileceği oluşturmaktadır.

II. SİBER GÜVENLİK VE ULUSLARARASI HUKUK

A. Genel Olarak

Siber saldırı, bilgisayar ve benzeri ağ veya sistemlerine karşı saldırgan faaliyetler ile kritik siber sistemi, varlık ve fonksiyonlarını bozma veya tamamen yok etme faaliyetlerini içermektedir.[12] Siber saldırının verdiği zararlar üç derecelidir. Öncelikle siber saldırı, bilgisayar sistemlerini veya ağlarını, verileri, yazılımları ya da sistemleri hedef almaktadır. Dolayısıyla siber saldırı, doğrudan siber dünyaya zarar vermektedir. Ancak siber ortamda gerçekleştirilen saldırı doğrudan bilgisayar sitemlerini etkilese de sistemde meydana gelen zarar, bilgisayar sitemlerinin kullanıldığı hizmetleri, son olarak da bu hizmetten yararlanan bireyleri etkilemektedir. Sonuç olarak siber saldırı domino etkisi yaratarak bilgisayar sistemleri yanında, bilgisayar sistemine bağlı olarak sağlanan hizmetlere ve ilgili hizmetlerden faydalanan bireylere de zarar vermektedir.[13]

---

[11] GUIORA, s. 25.

[12] Memorandum for Chefs of the Military Services Commanders of the Combatant Commands Directors of the Joınt Staff Directorates, Joint Terminology for Cyberspace Operations, Joint Terminology for Cyberspace Operations, s. 5. Bkz. http://www.nsci-va.org/CyberReferenceLib/2010-11-joint%20Terminology%20for%20 Cyberspace%20Operations.pdf (e.t. 01.04.2018)
Siber saldırının daha ayrıntılı tanımı için bkz. HATHAWAY vd., s. 826- 832.

[13] ROSCINI, Marco, Cyber Operations and the Use of Force in International Law, Oxford University Press, the UK, 2014, ss. 52 – 53; OWENS William A./ DAM, Kenneth W./ LIN, Herbert S., Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities, The National Academies Press, Washington, 2009, s. 80.
See also PALOJARVI, Pia, *"A Battle in Bits and Bytes: Computer Network Attacks and the Law of Armed Conflict",* Erik Castrén Institute of International Law, Helsinki, 2009, s. 32; BOOTHBY, William H., *"Methods and Means of Cyber Warfare"*, International Law Studies, Vol. 89, 2013, s. 390.

Siber saldırılar hedef aldıkları grup ve kullanılan yöntemler itibariyle, maddi saldırılarda olduğu gibi terör faaliyetlerine de konu olabilir. Nitekim, bazı terörist örgütlerin ya da organize suç örgütlerinin, devletin belli birimlerine siber saldırı düzenlediği olaylar olmakta, siber saldırı giderek klasik terör faaliyetlerinin yerini almaktadır. Klasik terör faaliyetlerinden farklı olarak, siber saldırıda bulunan kişi ve grupların siber uzayda kimliğinin gizli ve tespitinin zor olmasıdır. [14]

Siber saldırının başladığı ve tesir ettiği mekân, saldırıyı gerçekleştiren ve saldırıdan etkilenen kişiler ile saldırı neticesinde oluşan zararlar sebebiyle hem siber suçlar hem de siber suçun ötesinde daha ağır nitelikte olan siber saldırılar uluslararası toplumu yakından ilgilendirmektedir. Bu nedenle siber güvenliğin küresel çapta tesisi için gerekli önlemler uluslararası hukukun kapsamına girmektedir.[15] Başta Amerika Birleşik Devletleri olmak üzere Avustralya, Çin, Küba, Macaristan, İran, İtalya, Mali, Hollanda, Katar Rusya Federasyonu, Birleşik Krallık gibi devletler ve Avrupa Birliği gibi uluslararası örgütler, mevcut kuvvet kullanma yasağına ilişkin uluslararası hukuk kurallarının siber faaliyetler bakımından da uygulanılırlığını kabul etmişlerdir.[16]

---

[14] GUIORA, ss. 20, 23.

[15] BROWN, Gray, "International Law Applies to Cyber Warfare! Now What?, Southwestern Law Review, Vol. 46, 2017, s. 375.

[16] ROSCINI, s. 44.
Burada özellikle Çin ve Rusya'nın tutumu biraz karmaşıktır. 2011 yılında ABD, Siber Uzay İçin Uluslararası Strateji belgesi metninde, mevcut uluslararası hukuk kurallarının (konumuz açısından kuvvet kullanmaya ilişkin kuralların) siber uzaya da uygulanabileceği yaklaşımını dünyaya duyurmuştur. İşbu metnin kamuoyuyla paylaşılmasından sonra, Çin, Rusya, Tacikistan ve Özbekistan, BM'ye Bilgi Güvenliği İçin Uluslararası Davranış Kuralları başlıklı bir taslak sunmuştur. İşbu taslakta, açıkça uluslararası hukukun siber uzayda uygulanabilirliğine atıf yapılmamasının ve yeni bir düzen öngörülmesinin önerilmesinin, devletlerin uluslararası hukukun siber uzaya uygulanması hususunda hem fikir olmadıkları şeklinde yorumlanmıştır. Ancak devam eden yıllarda BM Hükümetlerarası Uzmanlar Grubu'nda yer alan Çin ve Rusya, mevcut uluslararası hukuk kurallarının siber uzaya da uygulanacağını deklare eden raporu hazırlayan devletler arasında yer almıştır. 2015 yılında içinde Çin, Rusya, Kazakistan, Tacikistan ve Özbekistan 2011 yılında hazırlanan taslağı yenileyerek tekrar BM'ye sunmuşlardır ve yine özel olarak uluslararası hukuka uygulanırlığının altının çizilmemesi, devletlerin uluslararası hukukun siber uzaya uygulanmasına ilişkin yaklaşımlarının aynı olmadığı ve özellikli Çin ve Rusya'nın pozisyonunun net olmadığı yorumlarına sebep olmuştur. EICHENSEHR, Kristen E., *"Cyberwar & International Step-Zero",* Texas Law Journal Vol. 50, Iss. 2, 2015, ss. 366- 367.

Ayrıca Birleşmiş Milletler (BM), Kuzey Atlantik Antlaşması Örgütü (NATO), Afrika Birliği, Güneydoğu Asya Milletleri Kuruluşu, Avrupa Konseyi, Batı Afrika Devletleri Ekonomik Topluluğu, Avrupa Güvenlik ve İşbirliği Örgütü, Şangay İşbirliği Örgütü gibi uluslararası örgütler de uluslararası toplumun karşı karşıya olduğu işbu fenomenle yakından ilgilenmektedir.[17]

Örneğin BM 1998 yılından beri BM Genel Kurulu'nun bilgi teknolojisine ilişkin aldığı kararlarda, meselenin bütün uluslararası toplumu ilgilendirdiği ve uluslararası hukukun, başta BM Şartı olmak üzere, siber faaliyetler bakımından da uygulanabilir olduğu ifade edilmektedir.[18] Aynı şekilde BM nezdinde kurulan Uzmanlar Heyeti tarafından 2013 ve 2015 yılında kaleme alınan raporlarda da uluslararası hukukun, başta BM Şartı olmak üzere, siber uzaya uygulanabileceğinin altı çizilmiştir.[19]

Ancak işbu yorum bir hukuk sisteminin kendi problem çözme araçlarını yok sayan ve uluslararası hukuku sadece devletlerle bağdaştıran bir yaklaşımdır. Halbuki hukukun kural koyucudan bağımsız ve uygulayıcıya yol gösteren problem çözme methodları vardır. Lex spatialis bunlardan biridir. Bir konuya ilişkin özel bir düzenleme bulunması halinde, genel düzenleme yerine özel düzenleme uygulanır. İşbu ilkeyi tersiyle yorumlayacak olursak, özel düzenlemenin yokluğu karşısında genel düzenleme uygulanacaktır. Siber uzayın güvenliğiyle ilgili durumda da özel bir antlaşmanın yokluğu karşısında, genel kurallar koyan antlaşmalar uygulanabilecektir. Sonuç olarak kanımızca, devletlerin ilgili konuya ilişkin iradelerinden bağımsız olarak, siber güvenliğe ilişkin özel bir antlaşmamanın olmaması sebebiyle uluslararası hukukun siber uzaya uygulanması mümkün olmanın ötesinde, zorunludur.

Çalışmamızda, devletlerin ve uluslararası örgütlerin uluslararası hukukun siber uzaya uygulanabilir olduğuna dair görüşlerine yer vermemizin sebebi, vardığımız sonucu pekiştirmektir.

[17] Group of Govermental Experts on Developments in the Field of Information and Telecommunicatipns in the Context of International Security, A/68/98, 24 June 2013, s. 7, para. 14.

[18] UN Doc. A/RES/53/70, 4 December1998; UN Doc. A/RES/54/49, 1 December1999; UN Doc. A/RES/55/28, 20 November 2000; UN Doc. A/RES/56/19, 29 November 2001; UN Doc. A/RES/57/53, 22 November 2002; UN Doc. A/RES/58/32, 8 December 2003, UN Doc. A/RES/59/61, 3 December 2004; UN Doc. A/RES/60/45, 8 December 2005; UN Doc. A/RES/61/54, 6 December 2006; UN Doc. A/RES/62/17 5 December 2007; UN Doc. A/RES/63/37, 2 December 2008; UN Doc. A/RES/64/25, 2 December 2009; UN Doc. A/RES/65/41, 8 December 2010; UN Doc. A/RES/66/24, 2 December 2011; UN Doc. A/RES/67/27, 3 December 2012; UN Doc. A/RES/68/243, 27 December 2013, UN Doc. A/RES/69/28, 2 December 2014; UN Doc. A/RES/70/237, 23 December 2015, UN Doc. A/RES/ 71/28, 9 December 2016.

[19] Group of Govermental Experts on Developments in the Field of Information and Telecommunicatipns in the Context of International Security, A/68/98, 24 June 2013; Group

Siber güvenlikle ilgilenen bir diğer uluslararası örgüt de NATO'dur. Özellikle Estonya'nın maruz kaldığı siber saldırının ardından, NATO bünyesinde 2010 yılı Kasım ayında Yeni Strateji Konsepti kabul edilmiştir. Söz konusu belgede, NATO üyesi devletlere karşı klasik saldırıların gerçekleşme olasılığının günümüzde artık düşük olduğu, ancak siber saldırıların daha organize ve verdiği zarar itibariyle NATO üyesi devletleri tehdit ettiği belirtilmiştir.[20]

B. Siber Saldırının Hukuki Niteliği

1. Siber Saldırı ve Kuvvet Kullanma Yasağı

Siber suçların, siber saldırı boyutuna ulaştığı hallerde, siber güvenliği sağlamak adına siber saldırıyı önleme ve siber terörizmle mücadele etmek amacıyla, uluslararası hukukun, uluslararası barış ve güvenliği sağlamak için getirdiği kural ve mekanizmaları yürütmek mümkündür.[21] Başka bir ifadeyle, hem hukuken hem de pratikte kuvvet kullanma yasağına ilişkin mevcut uluslararası hukuk kurallarının, siber uzaya uygulanmaması için bir gerekçe ya da sebep yoktur.[22] Çünkü devletlerin fiziksel olarak saldırıya maruz kalmaları ile siber uzayda saldırıya maruz kalmaları arasında, özellikle saldırının sonucu bakımından derin bir fark olmayabilir. Dolayısıyla da maddi dünyada yer alan Birleşmiş Milletler (BM) Şartı 2/IV'te düzenlenen kuvvet kullanma yasağı; BM Şartı 51. maddede düzenlenen meşru müdafaa hakkı ve saldırıya/silahlı saldırıya karşı alınabilecek diğer tedbirler, siber uzayda da geçerli olacaktır.[23]

---

of Govermental Experts on Developments in the Field of Information and Telecommunicatipns in the Context of International Security, A/70/174, 22 July 2015.

[20] Strategic Concept fort he Defence and Security of the Members of the North Atlantic Treaty Organization, Adopted by Heads of State and Governments at the NATO Summit in Lisbon, 19- 20 November 2010, s. 11, para. 12.

[21] Teknolojinin gelişmesiyle birlikte, konuya ilişkin temel tartışmalardan biri, siber güvenliğin mevcut anlaşmaların kapsamına girip girimediği ve mevcut uluslararası hukuk sisteminde siber saldırıların yasak olup olmadığı tartışmaları baş göstermiştir. Yukarda yer verdiğimiz görüşün aksine, konuya ilişkin hukuki bir boşluk olduğunu savunan görüşler de mevcuttur. EICHENSEHR, ss. 328- 335; HATHAWAY, ss. 880- 882; JENSEN, Eric Talbot, *"The Future of the Law of Armed Conflict: Ostriches, Butterflies, and Nanobots",* MICH. J. INT'L L., Vol. 35, 2014, ss. 263- 264.

[22] GILL, Terry D. – DUCHEINE, Paul A.L., "Anticipatory Self Defence in the Cyber Context", "*Int'l L. Stud.",* Vol. 89, 2013, s. 439.

[23] DeWEESE, Geoffrey S., "*Anticipatory and Preemtive Self-Defence in Cyberspace: The Challange of Imminence",* in the 7th International Conference on Cyber Conflict:

BM Şartı'nın 2/IV maddesinde düzenlenen kuvvet kullanma yasağıyla; devletlerin uluslararası ilişkilerinde herhangi bir devletin toprak bütünlüğüne veya siyasal bağımsızlığa karşı, BM'nin amaçlarıyla bağdaşmayacak biçimde kuvvet kullanma tehdidine ya da kuvvet kullanılmasına başvurulması yasaklanmıştır.[24] Devletlerin faaliyetlerinin kuvvet kullanma yasağına aykırılığının tespiti için iki farklı yaklaşımdan bahsedilmektedir. Bunlardan biri vasıta temelli yaklaşım diğeri de etki yaklaşımıdır. Vasıta temelli yaklaşım, kuvvet kullanma ve kuvvet kullanma tehdidi yasağının ihlali için, başta silah olmak üzere belli araçların kullanılması gerektiği ileri sürülmektedir. Diğer yaklaşımda ise, kullanılan aracın yıkıcı ve zarar verici etkisi göz önüne alınarak yasağın ihlal edildiği tespit edilebilir.[25]

Ancak siber saldırıların gerçekleşmesiyle birlikte, vasıta temelli yaklaşımının, vasıtanın silah olmaması nedeniyle, kuvvet kullanma yasağı ihlalinin tespiti için bir kriter olarak kullanılamayacağı aşikardır.[26] Bu durumda kuvvet kullanma yasağının siber uzayda kullanılabilecek vasıtalar aracılığıyla ihlali kabul edilebilecektir. Nitekim Uluslararası Adalet Divanı, Nükleer Silah Kullanma veya Tehdidinin Hukukiliği 'ne ilişkin danışma görüşünde de BM şartı 2/IV, 51 ve 42. maddelerinde spesifik bir silaha atıf yapılmadığı gerekçesiyle, kuvvet kullanma için spesifik bir silah kullanılıp kullanılmadığının bir önemi bulunmamaktadır. [27] İşbu durumda siber saldırının ağırlığı ve yol açtığı hasarın anında etki göstermesi sebebiyle, kuvvet kullanma yasağı kapsamında değerlendirilebilecektir. [28]

Architectures in Cyberspace, (MAYBAUM, M., Osula, A. A.- LINSTRÖM, M. L. ed.), 2015, s. 92; LOTRIONTE, s. 829; O'CONNEL, Mary, *"Cyber Security and International Law"*, Clatham Hause International Law: Meeting Summary, 29 May 2012, ss. 6- 7.
Siber saldırının kuvvet kullanma yasağının kapsamında kabul edilmesi ve hatta meşru müdafaa hakkının da uygulanmasının uluslararası toplumda karmaşa yaratacağı görüşleri de mevcuttur. İlgi karşı görüş için bkz. WAXMAN, Matthew C., *"Cyber-Attacks and Use of Force: Back to the Future of Article 2(4)",* Yale Journal of International Law, Vol. 2, Iss. 2, 2011, s. 443.

[24] Türkçe metin için bkz. https://www.tbmm.gov.tr/komisyon/insanhaklari/pdf01/3-30.pdf (e.t.15.04.2018).

[25] ROSCINI, s. 50.
Waxman BM Şartı'nda yer alan "kuvvet" kavramının, silahlı şiddet olayları, cebir ya da karışma şeklinde üç farklı şekilde yorumlanabileceğini, ancak genelin silahlı şiddet olayları olarak yorumlama eğiliminde olduğunu ifade etmektedir. WAXMAN, ss. 427- 431.

[26] ROSCINI, s. 50.

[27] Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion, 8 July 1996, I.C.J. Reports, para 39.

[28] GILL – DUCHEINE, s. 439; KITTICHAISAREE, s. 165; SCHMITT, ss. 914- 915; WAXMAN, s. 437.

Siber saldırının kuvvet kullanma yasağı ihlaline vücut verebilmesi için saldırının yol açtığı etki yanında siber saldırıya vücut veren faaliyetin devlet kaynaklı olması gerektiği de ileri sürülmektedir. Dolayısıyla özel kişilerin ve hükümet-dışı grupların gerçekleştirdiği siber saldırılar, saldırının verdiği zararın boyutları ne kadar büyük olursa olsun BM 2/IV kuvvet kullanma yasağının kapsamında değerlendirilemeyecektir.[29] Karşı görüş olarak ise BM Şartı'nın devlet-dışı aktörleri de kapsayacak şekilde düzenlenme amacı taşıdığı belirtilmiştir.[30]

Son olarak da saldırının devletin uluslararası ilişkileri bağlamında gerçekleştirilmiş olması gerekmektedir.[31]

Siber saldırılar ilgili bir başka hukuki doküman da NATO bünyesinde hazırlanan Tallinn El Kitabıdır. NATO'nun kurduğu Ortak Siber Savunma Mükemmeliyet Merkezi siber güvenliğin hukuki boyutlarını tartışmak adına çalışmalara başlamış ve 2009 yılında uluslararası uzmanlar grubu oluşturulmuştur. Uzmanlar grubunun çalışmalarının ürünü olan El Kitabı'nın birinci ve ikinci versiyonunda, siber faaliyetlere uygulanacak hukuk kurallarını ayrıntılarıyla incelenmiş; siber faaliyetler için uygulanabilecek ilkeleri mevcut uluslararası kurallar ışığında, kaleme almıştır. Nitekim El Kitabı'nın uluslararası barış ve güvenlik ve siber faaliyetlerin ele alındığı kısımda yer alan ilkeler, uluslararası hukukta düzenlenen kuvvet kullanma yasağı, meşru müdafaa hakkı ve kolektif güvenlik sistemine ilişkin kuralların rehberliğinde hazırlanmıştır.[32]

---

29 ROSCINI, s. 44.

30 MÜLLERSON, Rein, *"Jus ad Bellum: Plus ça Change (Le Monde) Plus C'est L Même Chose (Le Droit)?",* J. CONFLICT & SECURITY L., Vol. 7, 2002, s. 182, LOTRIONTE, dn. 193'ten atfen.
İşbu görüş, kuvvet kullanma yasağının kapsamının genişlemesi açısından uygun gözükse de kanaatimizce BM Şartı'nın suistimale maruz bırakılması sonucuna yol açabilecektir. Aşağıda daha ayrıntılı yer verdiğimiz üzere, kuvvet kullanma yasağının muhattabı olan ve hiçbir devletle bağı olmayan devlet-dışı örgüt, işbu yorumla meşru müdafaa hakkının kapsamına girebilecektir. İlgili durumda kanımızca, herhangi bir devletle bağı olmayan devlet-dışı örgütlerin faaliyetlerine karşı meşru müdafaa hakkının kullanılabileceği gibi bir yorum çıkarılabilecektir.

31 ROSCINI, s. 44.

32 İlki 2013 yılında hazırlanan El Kitabı, 2017 yılında güncellenerek son halini almıştır. Son hali için bkz. SCHMITT, M. – VIHUL, L. (ed.), Tallinn Manual 2.0 On the International Law Applicable to Cyber Operations, Cambridge University Press, UK, 2017, ss. 301- 373. Bundan sonra Tallinn El Kitabı 2 olarak anılacaktır.

Siber saldırı ile kuvvet kullanma yasağı ilişkisi ile ilgili olarak Tallinn El Kitabı'nın ikinci versiyonunun 68. kuralında kuvvet kullanma ve kuvvet kullanma tehdidi yasağı öngörülmüş, ilgili metinde BM Şartı'yla paralel bir yaklaşım benimsenmiştir. Buna göre, bir devletin egemenliğine ya da bağımsızlığına karşı BM'nin amaçlarıyla bağdaşmayacak nitelikte kuvvet kullanma ya da kuvvet kullanma tehdidine vücut veren siber saldırılar hukuka aykırı olcaktır. Maddenin gerekçesinde, kuvvet kullanmanın silahlı kuvvetler eliyle gerçekleştirilmesinin zorunlu olmadığı, devlet adına hareket eden devlet kuruluşları, kamu görevlileri ve özel hukuk kişilerinin yaptığı faaliyetlerin de kuvvet kullanma yasağına girebilmesinin mümkün olduğu belirtilmiştir. İşbu sebeple kuvvet kullanma yasağı kapsamına giren bir faaliyetin, mutlaka bir devletle ilişkilendirilmesi gerektiği, devlet-dışı aktörlerin faaliyetlerinin, ağırlığı ne olursa olsun, kuvvet kullanma yasağı kapsamına girmesinin söz konusu olamayacağı ifade edilmiştir. [33] Devam eden 69. kuralda siber saldırının boyutunun ve etkisinin göz önüne alınarak, kuvvet kullanma yasağına aykırı olabileceği düzenlenmiştir.[34] Sonuç olarak siber saldırı, klasik anlamda saldırı olarak kabul edilebilecek ve kuvvet kullanma yasağına aykırılık teşkil edebilecektir.

2. Siber Saldırının Silahlı Saldırı Boyutuna Ulaşması

Siber saldırının, kuvvet kullanma yasağına aykırı kabul edilmesinin bir adım ötesinde, silahlı saldırıya vücut verip vermediği de tartışılan bir diğer hususdur. Silahlı saldırı bilindiği üzere BM Şartı'nda tanımlanmamıştır. Bu nedenle de hangi kuvvet kullanma faaliyetinin silahlı saldırı teşkil edeceğini tespit etmek önem arz etmektedir. Öncelikle düzenli silahlı kuvvetler tarafından başka bir devletin ülkesini işgal etmek, tartışma götürmez bir şekilde silahlı saldırı sayılmaktadır. Ancak tartışma, işgal derecesine varmadan farklı ağırlıklarda silahlı kuvvet kullanımı ve farklı nitelikteki silahların kullanımı açısından ortaya çıkmaktadır. Nitekim siber saldırı da son yıllarda ilgili tartışmaya eklenmiş durumdadır.[35]

Bu noktada BM Genel Kurulu'nun 1974 Saldırının Tanımı Kararı'na başvurmak silahlı saldırıyı tespit edebilmek açısından bir çözüm

[33] Tallinnn El Kitabı 2, Kural 68 para. 4-5.
[34] Tallinnn El Kitabı 2, Kural 71.
[35] GRAY, Christine, International Law and the Use of Force, Oxford University Press, Third Edition, the UK, 2008, ss. 128- 129.

sağlamaktadır.[36] Kararda silahlı saldırı açıkça tanımlanmamış olsa bile, kararın 3. maddesinde yer verilen bazı faaliyetlerin, silahlı saldırı olarak nitelendirilebileceği kabul edilmektedir.[37] Karar bir devletin ülkesinin işgal edilmesi yanında, bir devletin bombardımanına maruz bırakılması, liman ve kıyılarının abluka altına alınması, kara, deniz ve kuvvetleri ile hava ve deniz filolarına saldırıda bulunulması, bir antlaşma sonucu ülkede bulunan silahlı kuvvetlerin antlaşmanın amacını aşması ya da antlaşmada öngörülenden daha uzun sürede ülkede kalması, bir devletin kendi ülkesini başka bir devlete saldırı için kullandırması ve başka bir devlete silahlı saldırı yoğunluğunda güç kullanabilecek silahlı gruplar, düzensiz birlikler ya da lejyonerler gönderme faaliyetleri de silahlı saldırı kabul edilebilecektir.[38]

Karar önemli sayıda örneklere yer verse de silahlı saldırının yukarıda sayılanlarla sınırlı olmadığını da belirtmek gerekmektedir.[39] Dolayısıyla, maddenin lafzından da anlayacağımız üzere, faaliyetlerin belli bir ağırlığa ulaşması, silahlı saldırının tespiti için önem arz etmektedir. Bu noktada siber saldırının hiçbir şekilde silahlı saldırı oluşturmayacağını ifade etmek, kararın ruhuna aykırı olacaktır. Siber saldırının da birtakım kriterleri taşıması halinde, silahlı saldırı olarak nitelendirilebileceği kabul edilmelidir.[40]

Schmit siber saldırının geleneksel anlamda silahlı saldırı kabul edilebilmesi için, belli bir ağırlığa sahip olması gerektiğini; *Robertson* ise siber saldırının askeri ve sivil ağlara büyük çapta zarar vermesi, ölüm ya da fiziksel zararlara yol açması vs. gibi durumlarda silahlı saldırı kabul edilebileceğini savunmaktadır.[41] *Dinstein* verdiği sınıflandırmada; bilgisayar kontrollü yaşam destek ünitelerinin çökertilmesi sonucunda ölümlerin meydana gelmesi, ciddi derecede etki yaratan geniş çaplı elektrik kesintileri, barajların ve su dağıtım şebekelerini kumanda eden bilgisayar sistemlerinin çökmesi ve yaşam alanlarında su taşkınlarına sebep olması, uçak bilgisayar

---

[36] Nitekim, aşağıda daha ayrıntılı yer vereceğimiz üzere, Uluslararası Adalet Divanı'nın Nikaragua Kararı'nda da dolaylı saldırının tespitinde, işbu belgeye başvurması, belgenin silahlı saldırının tespiti için de önem arz ettiğini göstermektedir.

[37] KESKİN, Funda, Uluslararası Hukukta Kuvvet Kullanma: Savaş, Karışma ve Birleşmiş Milletler, Mülkiyeliler Birliği Vakfı Yayınları, Tezler Dizisi: 4, s. 48.

[38] UN Doc. A/RES/29/3314, 14 December 1974. Saldırının tanımı kararı, md. 3.

[39] KESKİN, s. 47.

[40] Aynı görüş için bkz. LOTRIONTE, s. 864.

[41] ROBERTSON, Horace B. Jr., "Self-Defense Against Computer Network Attack Under International Law", 76 INT'L L. STUD., Vol. 76, 2002, s. 121.

sistemini etkilemek suretiyle ölümcül kazalara sebep olunması, bir nükleer güç santralinde bir reaktörde çekirdek füzyonunun kontrolden çıkması sonucu radyoaktif sızıntı oluşması ve işbu sızıntının çevre ve insan hayatında sayısız zarara yol açması gibi zararları, siber saldırının silahlı saldırı kabul edilebileceği durumlar olarak göstermiştir.[42]

Tallinn El Kitabı'nın siber saldırıya karşı meşru müdafaayı düzenleyen kuralının şerhinde, her siber saldırının silahlı saldırı gibi kabul edilemeyeceği ifade edilerek, birtakım örneklere yer verilmiştir. Buna göre, bir siber saldırı, belli sayıda insanın yaralanmasına ya da ölümüne sebep olması ya da mallarında önemli derecede zarara ya da yıkıma sebep olması halinde, silahlı saldırı sayılabilecek boyut ve etkiye sahip olabilecektir.[43] Bunun yanında yaralanan ya da ölen kişilerin devlet ajanı ya da sivil olması, zarar gören mallarınsa kamu malı ya da şahsa ait olmasının fark yaratmadığı da El Kitabı tarafından vurgulanan bir husustur.[44] Dolayısıyla siber suçlara vücut veren siber casusluk, veri hırsızlığı, bilgisayar sistemlerine izinsiz girmek amacıyla gerçekleştirilen her türlü faaliyet vs. devletler tarafından gerçekleştirilse dahi siber saldırının kapsamına girmeyeceği için, işbu faaliyetlere kuvvet kullanmaya ilişkin kurallar uygulanmayacaktır.[45]

Aynı zamanda bir siber saldırının silahlı saldırı sayılabilmesi için, salt fiziksel zarara yol açmasının da şart olup olmadığı tartışma konusu haline gelmiştir. Bir görüşe göre bilgisayar sistemlerinin etkilenmesi sonucu bir hizmetin gerektiği biçimde yerine getirilememesi ve devletin finans sisteminin ciddi derece etkilenmesi sonucu ciddi bir fiziksel zarar oluşmuşsa, siber saldırı neticesinde kuvvet kullanma yasağının ihlalinden bahsetmek mümkün olacaktır.[46] Aksi görüş uyarınca siber saldırı uzun süreli olarak finans piyasalarını çökertip bir devletin ekonomisinin aşırı ya da milli para

---

42 DINSTEIN, Yoram, *"Computer Network Attacks",* INT'L L. STUD., Vol. 76, 2002, s. 105.

43 Tallinn El Kitabı 2.0., Kural 71, para. 8. Nitekim işbu durum yazarlarca da kabul edilen bir husustur. Bkz. Guiora, s. 55.

44 Tallinn El Kitabı 2.0, Kural 71, para.22.

45 Söz konusu faaliyetler sadece siber suça vücut verecektir. GILL – DUCHEINE, s. 440.

46 Örneğin ABD'nin politikası uyarınca, siber saldırının kuvvet kullanma sayılması için önemli derecece fiziksel zarara sebebiyet vermesi gerekmektedir. Aynı şeklide Estonya'nın 2007 yılında uğradığı siber saldırının ardından Dış İşleri Bakanı'nın 2016 yılında yaptığı açıklamada, siber saldırının ülkenin hayati derecede altyapı sistemlerini ve dolayısıyla ekonomik yapısını etkileyen ve bu sayede toplum üzerinde büyük zarara yol açan siber saldırıların BM 2/IV'ün kapsamına gireceği ifade edilmiştir. Ayrıntılı bilgi için bkz. KITTICHAISAREE, ss. 163- 164.

biriminin aşırı değer kaybetmesine sebep olursa ve bu etkiler yeterince ciddi boyuta ulaşmışsa, işbu siber saldırının da silahlı saldırı olarak nitelendirilmesinin mümkün olduğu savunulmaktadır.[47] Kanımızca her ne kadar bir devletin ekonomisinin ciddi derecede etkilenmesi söz konusu olsa da siber saldırının kuvvet kullanma sayılabilmesi için, yaşanan ekonomik çöküntünün aynı zamanda ciddi fiziksel zarara sebep vermesi gerekmektedir.

3. Siber Saldırıya Karşı Meşru Müdafaa Hakkı

a. Klasik Meşru Müdafaa Hakkı ve Siber Saldırı

Siber saldırının kuvvet kullanma yasağının kapsamına girmesi ve hatta silahlı saldırıya vücut vermesi halinde uluslararası toplumun silahlı saldırıya karşı alacağı tedbirler de değişmektedir. Siber saldırının hukuki niteliği uyarınca, siber saldırı klasik anlamda saldırının kapsamına girebilecektir. İşbu durumda saldırıya uğrayan devlet karşı tedbir alabilecek, zararı devletin sorumluluğuna ilişkin kurallar uyarınca tazmin edilebilecektir.[48] Siber saldırıya karşı meşru müdafaa hakkının kullanılabilmesi için ise saldırının niteliği önem arz edecektir.[49] Ancak konuya ilişkin farklı yaklaşımlar bulunmaktadır.

Klasik uluslararası hukuk uyarınca meşru müdafaa hakkının kapsamı dar olup hak sadece silahlı saldırıya maruz kalma durumunda doğmaktadır. Bunun yanında silahlı saldırının bir devletten gelmesi, meşru müdafaanın hakkının derhal kullanılması, meşru müdafaa hakkı kapsamında gerçekleştirilecek karşı fiilin gerekli ve orantılı olması gerekmektedir. Son olarak, meşru müdafaa hakkını kullanan devlet, derhal BM Güvenlik

---

47 GILL - DUCHEINE, s. 444.
Nitekim iş bu husus kuvvet kullanma yasağına ilişkin tartışmalarda da görülmektedir, buna göre yasağın sadece silahlı kuvvetler yoluyla değil, ekonomik zorlamayla da ihlal edilebileceği ileri sürülmektedir. Bkz. GRAY, s. 30.

48 LOTRIONTE, s. 830.

49 Çalışmamızda siber saldırıya karşı meşru müdafaa hakkını ön plana çıkararak tartışmamızın nedeni, kuvvet kullanma yasağının en temel istinasının meşru müdafaa hakkı olduğu görüşüne katılmamızdır. İlgili görüş için bkz. WEE YEN, s. 2.
Bunun dışında kolektif güvenlik sistemi salt kuvvet kullanma içeren tedbirlerden oluşmamakta, salt devletler tarafından kullanılamamakta ve sistemin harekete geçirilebilmesi için BM Güvenlik Konseyi kararı ve yönetimine ihtiyaç duyulmaktadır. Dolayısıyla kuvvet kullanma yasağının istisnasını oluşturmaktan çok kanımızca BM'ye verilmiş bir yetki ve görevdir. Bkz. BM Şartı VII. bölüm.

Konseyi'ne haber vermekle yükümlüdür.[50] İşbu haliyle, siber saldırının kuvvet kullanma yasağının ihlali olarak değerlendirilmesi, devletlerin meşru müdafaa hakkının doğması için yeterli olmayıp siber saldırının silahlı saldırı boyutuna varması gerekmektedir.[51]

Kasten hedef alınan siber sistem ya da kayıtlı veriye karşı yapılan siber saldırı, kamu güvenliği ya da önemli altyapı tesislerine zarar verici nitelikte olabilir. Bu durumda, devletin ve sivillerin maruz kaldıkları zarar, klasik silahlı saldırıda oluşabilecek zararla aynı derecede sahiptir.[52] Bunun yanında, silahlı saldırının sadece devletin askeri kuvvetlerini hedef alması gerekmemekte, sivilleri etkileyen silahlı saldırılar da meşru müdafaa hakkına vücut verebilmektedir. Aynı husus silahlı saldırı seviyesine varan siber saldırı bakımından da söz konusu olacaktır.[53]

Siber saldırının silahlı saldırı boyutuna varması durumunda, siber saldırıya uğrayan devletin meşru müdafaa hakkı doğacaktır. Klasik meşru müdafaa hakkında olduğu gibi, siber saldırıya karşı meşru müdafaa hakkı, gerekli, ölçülü ve acil olmalıdır.[54] Burada en önemli mesele, kanımızca ölçülülükle alakalıdır. Doktrinde bazı yazarlar, siber saldırıya karşı kullanılabilecek meşru müdafaanın siber uzayla sınırlı olmasının daha uygun olduğunu ileri sürmektedir.[55] Ancak Tallinn El Kitabı'nda, siber saldırının silahlı saldırı boyutuna ulaşması halinde, kullanılacak tedbirin siber uzayla sınırlı olması gibi bir yaklaşım benimsenmemiştir.[56] Sonuç olarak siber saldırıya karşı kullanılan meşru müdafaa hakkı gerek siber uzayda gerek fiziksel ortam kullanılsın en nihayetinde ölçülü olmak durumundadır.[57]

---

50 BM Şartı 51. Madde ve ilgili örf ve adet hukuku kuralları. JENNINGS, R.Y. "*The Caroline and McLeod Cases"*, American Journal of International Law, Vol. 32, 1938.

51 SZABO, Kinga Tibori, *"Anticipatory Action in Self Defence Essence and Limits Under International Law",* Springer, The Netherlands, 2011, ss. 119- 123.

52 The DoD's Assessment of International Legal Issues US DoD, s. 20.

53 DINSTEIN, ss. 106 – 107.

54 Nitekim bu unsurlar meşrü müdafaa hakkının doğal olarak içerdiği ve Caroline olayından bu yana uygulanagelen unsurlardır. JENNINGS, s. 92.

55 GUIRO, ss. 64- 65.

56 Tallinn El Kitabı 2.0, Kural 72, paras. 5- 6.

57 RYAN, Daniel J./DION, Maeve/ TIKK, Eneken/RYAN, Julie JCH, *"International Cyberlaw: A Normative Approach",* Georgetown Journal of International Law, Vol. 42, 2011, s. 1172.

Siber saldırıya karşı meşru müdafaa hakkı, münhasıran kullanılabileceği gibi münferiden de kullanılabilecektir.[58] Klasik meşru müdafaada olduğu gibi, siber saldırıya karşı meşru müdafaa hakkını kullanan devlet, durumu derhal BM Güvenlik Konseyi'ne bildirmelidir.[59]

b. Farklı Meşru Müdafaa Yaklaşımları ve Siber Saldırı

Klasik meşru müdafaa hakkını dışında, meşru müdafaa hakkını genişleten farklı yorumlar da mevcuttur. Bu yorumları saldırının zamanı ve kaynağı açısından incelemek gerekmektedir.

Söz konusu meşru müdafaa hakkı, zaman ve faaliyet açısından silahlı saldırının ya da iddia edildiği üzere saldırının gerçekleşmesi ya da gerçekleşmesine ilişkin yakın bir tehlikenin varlığı halinde kullanılabilecektir. Hem silahlı saldırı şartını hafifleten yorum hem de tehlike kriteriyle önleyici meşru müdafaa hakkını getirmektedir.[60]

11 Eylül saldırılarından önce yukarıda yer verdiğimiz biçimde meşru müdafaa hakkını genişleten uygulamalarda bulunan devletler, faaliyetlerini açıkça önleyici meşru müdafaa hakkına dayandırdıklarını ileri sürmemişleridir. Sadece 1981 yılında İsrail'in İran'ın nükleer reaktörünün bombaladığı olay gibi belli olaylarda ileri sürülmüş, ancak uluslararası toplumda işbu uygulamalar hukuka uygun kabul edilmemiştir. [61] Ancak önleyici meşru müdafaa hakkına ilişkin tartışmalar özellikle 11 Eylül olayından sonra *Bush* doktrini ile birlikte yoğunlaşmıştır.

Uluslararası toplum tarafından yeterince rağbet görmeyen işbu, siber saldırıya karşı meşru müdafaa hakkının kullanılması bağlamında da tartışmaya açılmış ve aynı şekilde siber saldırı tehdidinin varlığında, önleyici meşru müdafaa hakkının kullanılması gibi bir durumun söz konusu olup olamayacağı farklı görüşlere sahne olmuştur.[62] Öncelikli görüş önleyici meşru müdafaa hakkının uluslararası hukuka aykırı olduğu ve BM Şartı'nın 51.

---

58 Tallinn El Kitabı 2.0, Kural 74.

59 Tallinn El Kitabı 2.0, Kural 75.

60 Silahlı saldırıyı saldırı şeklinde hafifleten doktrin Reagan doktrinidir. Zaman bakımından önleyici meşru müdafaa hakkını da Bush doktrini ileri sürmüştür. Ayrıntılı bilgi için bkz. BAŞEREN, Sertaç Hami, Uluslararası Hukukta Devletlerin Münferiden Kuvvet Kullanmalarının Sınırları, Ankara Üniversitesi Basımevi, Ankara 2003, ss. 1- 19.

61 GRAY, ss. 160- 165; STABO, s. 170.

62 allinnn El Kitabı 2.0, Kural 73, paras. 4- 11.

maddesiyle bağdaşmadığı görüşüdür.[63] Bu durumda, siber saldırılar bakımından yalnızca klasik meşru müdafaa hakkı uygulanacaktır. Bir taraftan da önleyici meşru müdafaanın hem uluslararası örf ve adet hukuku kuralı hem de 51. maddeye uygun olduğu da savunulmaktadır.[64] Önleyici meşru müdafaa hakkının varlığını uluslararası hukukta kabul eden yazarlar, siber saldırıya karşı da önleyici meşru müdafaa hakkının kullanılabileceğini savunmaktadır.[65]

Saldırının kaynağı açısından da önleyici meşru müdafaa hakkı uluslararası hukukta kabul edilmezken siber saldırılara karşı önleyici meşru müdafaa hakkının kabul edilmesi mümkün gözükmemektedir.[66] Nitekim devletlerin kendi sistemlerini siber ortama entegre etmeleri ile birlikte, saldırıya açık olmaları, devletlerin önleyici nitelikteki müdahalelerinin hukuka uygun olamayacağı Tallinn El Kitabında da kabul edilmiştir. [67]

Siber saldırıya karşı meşru müdafaa hakkının kullanımı ile ilgili tartışmalı bir diğer husus da siber saldırının kaynağına ilişkindir. Buna göre, siber saldırıya karşı meşru müdafaa hakkının kullanılabilmesi için, siber saldırının bir devlet tarafından ya da devlet destekli bir grup tarafından gerçekleştirilmesi gerekmektedir.[68]

Konuyu öncelikle, devlet-dışı gruplara karşı meşru müdafaa hakkı tartışması bakımından ele alırsak, hakkın kullanılabilmesi için silahlı saldırının muhakkak devletten gelmesi gerektiğini iddia etmektedir.[69] Yine

---

63 CASSESE, Antonio, International Law, Oxford University Press, UK, 2005), s. 361; GRAY, ss. 213- 216.

64 In Larger Freedom: Towards Development, Security and Human Rights for All, Report of the UN Secretary-General, UN Doc A/59/2005, 21 March 2005, s. 33.

65 DeWEESE, s. 92; GUIORA, ss. 58, 64.

66 Aksi görüş için bkz. WILMSHURST, Elizabeth, Principles of International Law on the Use of Force By States in Self-Defence, Clatham House Paper, ILP WP 05/01, 2005, ss.5 - 6.

67 GILL – DUCHEINE, s. 465.; ROSCINI, s. 79.

68 Devletle, devlet dışı aktörler arasındaki bağlantı bakımından tartışılan bir diğer husus da 11 Eylül saldırısı sonunda, Afganistan'a gerçekleştirilen operasyon öncesinde, bir devletin kendi ülkesi içinde terör faaliyetlerini önleme yükümlülüğünün olup olmadığıdır. Buna göre, devletlerin kendi yetki alanları içinde, terör örgütlerinin konuçlanmalarına ve faaliyetlerini gerçekleştirmelerine engel olma yükümlülüğünden bahsedilmektedir. İşbu yaklaşımının siber terörizmde de benimsenmesi gerektiği ileri sürülmektedir. LOTRIONTE, s. 890.

69 HALATÇI, Ülkü: "*11 Eylül Terörist Saldırıları ve Afganistan Operasyonu'nun Bir Değerlendirmesi"*, Uluslararası Hukuk ve Politika, C.2, No. 7, s. 97.

devlet-dışı aktörlerin uluslararası hukukun süjesi olmaması sebebiyle, bir terörist örgüt tarafından gerçekleştirilen saldırının başka bir devlet ile bağlantısının bulunması ve bu bağlantı üzerine meşru müdafaa hakkının kullanılması gerektiği de ileri sürülmektedir.[70]

11 Eylül olayından önce, devletle bağlantısı olmayan devlet-dışı aktörlere karşı meşru müdafaa hakkının kullanılamayacağı görüşü baskın olan görüştür. Özellikle Uluslararası Adalet Divanı'nın (UAD) Nikaragua Askeri ve Yarı-askeri Faaliyetler kararıyla birlikte de devlet-dışı aktörün silahlı saldırı seviyesine varan faaliyetinin devletle ilişkilendirilmesi hususu ortaya konulmuştur. Silahlı saldırı boyutuna varacak nitelikte faaliyette bulunan devlet-dışı grupların/örgütlerin, bir devletle ilişkilendirilmesi halinde, destekleyen devletin mağdur devlete karşı silahlı saldırıda bulunduğu, dolaylı olarak gerçekleşen silahlı saldırıdan sorumlu tutulması gerektiği kabul edilmiştir. Divan bir devlet aleyhine düzenli kuvvetlerin ika edebileceği ağırlıkta silahlı hareket gerçekleştiren silahlı grupların, düzensiz kuvvetlerin, ücretli askerlerin başka devlet tarafından veya onun adına gönderilmesi veya bu olaylara önemli ölçüde karışması halinde silahlı saldırının söz konusu olabileceğine karar vermiştir.[71] Ancak kararda dolaylı silahlı saldırının, devletle devlet-dışı aktör arasındaki ilişkinin çok yakın ve saldırının devlete ait düzenli kuvvetlerin saldırısına paralel bir ciddiyette olması durumunda gerçekleşmiş kabul edileceği ifade edilmiştir.[72] Sonuç olarak dolaylı silahlı saldırı halinin tespiti içinse, devlet ile devlet-dışı grup/örgüt arasında bir bağlantı olduğu, devlet tarafından desteklendiğinin tespiti gerekmektedir.[73]

Bu durumda bilerek kendi ülkesinin başka devletlere karşı saldırgan eylemler gerçekleştirme amacıyla kullanılmasına izin veren devlete karşı, bu eylemler boyut ve etkileri bakımından silahlı saldırı düzeyine erişmişlerse, meşru müdafaa hakkına dayanarak kuvvet kullanılabileceğini öne sürmek

---

[70] YAPICI, Utku: *"Uluslararası Hukukta Terörizme Karşı Kuvvet Kullanımı Sorunu",* Uluslararası Hukuk ve Politika, C. 2, No.7, 2006, s. 24.

[71] Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United Stataes of America), Judgement, I.C.J. Reports, 1986, paras. 195, 228.

[72] TOPAL, s. 122.

[73] Divan'ın benzer yaklaşımı için ayrıca bkz. Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory, Advisory Opinion, I.C.J. Reports 2004, para. 139; Armed Activities on the Territory of the Congo (Democratic Republic of the Congo v. Uganda), Judgement, I.C.J. Reports 2005, paras. 146, 160.

mümkün gözükmemektedir.[74] Devletin silah sağlaması, lojistik destek vermesi ve diğer yollarla örneğin kendi ülkesi üzerinde üsler sağlaması, dolaylı silahlı saldırıya vücut vermeyecektir.[75]

Ancak 11 Eylül'den sonra yaşanan olaylar, silahlı saldırının kaynağına ilişkin olarak önemli tartışmaları içermektedir.[76] 11 Eylül saldırılarından sonra BM Güvenlik Konseyi tarafından alınan 1368 sayılı ve 1373 sayılı kararlarda, BM Güvenlik Konseyi'nin uluslararası barış ve güvenliği tehdit eden her türlü terör faaliyetiyle mücadelede kararlı olduğu belirtilerek, BM Şartı uyarınca devletlerin bireysel ya da kolektif meşru müdafaa hakkının tanındığı da ifade edilmiştir. 11 Eylül'den sonra ABD ve Birleşik Krallık (BK), 11 Eylül saldırısını gerçekleştiren El-Kaide'nin, Afganistan'ın ülkesinde faaliyet gösteren örgüte müdahale etmemesi sebebiyle arasında bir bağ olduğunu, dolayısıyla Afganistan'ın yardım ve yataklık eden devlet olduğunu ileri sürmüştür.[77] Ancak görüldüğü üzere hakkın kullanımı için kanıtlaması gereken devlet-dışı örgütle devlet arasındaki güçlü ve belli derecedeki bağlantı göz ardı edilmiştir.

ABD'nin işbu uygulaması gerçekleşse de UAD 2004 yılında verdiği İşgal Altındaki Filistin Topraklarında Duvar İnşa Edilmesinin Hukuki Sonuçları başlıklı danışma görüşünde UAD, meşru müdafaa hakkına ilişkin hakkın bir devlet tarafından bir devlete karşı kullanılması gerektiğini ifade etmiştir. Dolayısıyla, UAD'nin Nikaragua kararında belirttiği devlet-dışı gruplara karşı meşru müdafaa hakkının kullanılmasının ancak ve ancak grupla devlet arasında belli bir seviyeye varan bağlantı olması durumunda kullanılabileceğini öngören klasik görüşü, bir kez daha yinelenmiştir.[78]

11 Eylül saldırından sonra dolaylı silahlı saldırının kapsamını genişleten yaklaşımlardan bir adım daha ileri gidilerek önleyici meşru müdafaa doktrini ortaya atılmıştır. Önleyici meşru müdafaa doktrini sadece silahlı saldırının gerçekleşme zamanına ilişkin değil, silahlı saldırının kaynağına ilişkin klasik

74 ROWLES, s. 314.

75 KAYA, İbrahim, Terörle Mücadele ve Uluslararası Hukuk, USAK Yayınları, Ankara, 2005, s. 174. İlgili durum ancak karışma sayılabilecektir. Ayrıntılı bilgi için bkz. Keskin, ss. 111- 121.

76 GRAY, s. 199.

77 MURPHY, Sean, "Contemporary Practice of the United States relating to International Law", American Journal of International Law, Vol. 96, 2002, s. 237.

78 I.C.J. Reports 1986, para. 139.

yaklaşımı değiştirme/aşma çabasındadır. ABD'nin o dönemki başkanı *Bush*, küresel terörizmle mücadele etmek açısından devlet dışı örgüt ya da devletlerden yakın bir saldırı tehlikesinin varlığı halinde önleyici meşru müdafaa hakkının doğacağını ileri sürmüştür.[79]

Ancak şunu belirtmek gerekir ki önleyici meşru müdafaa hakkı uluslararası toplum tarafından kabul edilmemiştir. BM nezdinde Genel Sekreter tarafından kurulan 2005 Zirve Raporu'nda (High Level Panel Report) ve Genel Sekreter'in hazırladığı Daha Geniş Özgürlükler (In Larger Freedom) Raporu'nda önleyici meşru müdafaa hakkının reddedildiği görülmektedir.[80] Aynı şekilde devletlerin çoğunluğu da önleyici meşru müdafaa hakkını kabul eden bir tavır sergilememiştir.[81] Önleyici meşru müdafaa doktrini her ne kadar II. Körfez Savaşı'nda ileri sürülmüşse de uluslararası toplumun geneli tarafından kabul görmemiştir.[82]

11 Eylül sonrası yaşanan olaylar doktrinde de farklı tartışmalara vücut vermiştir. Bir görüş uyarınca 2000 yılından sonra meydana gelen terör saldırılarının, devlet-dışı aktörlerle özellikle terörizmle mücadelede meşru müdafaa hakkının kullanılmasını etkilediği ifade edilmektedir.[83] Son dönemde devlet destekli olmayan ancak ülkesinde bulunduğu devlet tarafından tolerans gösterilen, az da olsa devlet tarafından kontrol edilen grupların silahlı saldırı boyutuna varan faaliyetlerinin meşru müdafaa hakkı kapsamında silahlı saldırı kabul edilebileceği da savunulmaktadır.[84]

---

79 2002 National Security Strategy of the United States of America, https://www.state.gov/documents/organization/63562.pdf (e.t. 15.04.2018).
2006 National Security Strategy of the United States of America, https://www.state.gov/documents/ organization/64884.pdf (e.t. 15.04.2018).

80 High-Level Panel Report, UN Doc. A/59/565, para. 189 - 192; In Larger Freedom Raporu, A/59/2005, 21 March 2005, para. 125.

81 GRAY, s. 253.

82 Aksi görüş için bkz. GILL – DUCHEINE, s. 453. *Stabo* da önleyici meşru müdafaa hakkının yeniden ortaya çıkan bir uluslararası örf ve adet hukuku kuralı olduğunu, ancak içeriğinin ve kapsamının tanımlanması gerektiğinin, aksi halde işbu hakkın kötüye kullanılacağının altını çizmiştir. STABO, s. 287.

83 MAOGOTO, Jackson, Ntamuya, *"War on the Enemy: Self-Defence and State-Sponsored Terrorism",* Melbourne Journal of International Law, Vol. 4, No. 2, 2003, s. 433. *Lotrionte,* bu sonuca yorum yoluyla ve devlet uygulamalarıyla ulaşılabileceğini ifade etmektedir. LOTRIONTE, s. 865.

84 DUCHEINE, P.A.L./ POUW, E.H., *"Legitimizing the Use of Force: Legal Bases for Operations Enduring Freedo and ISAF",* içinde Mission Uruzgan: Colloborating in Multiple Coalations for Afganistan, Pallas Publications, Amsterdam, 2012, s. 39.

Örneğin *Byer,* son dönemde meydana gelen olayların, uluslararası hukuk sisteminde değişikliklere yol açtığı ve kuvvet kullanımına ilişkin sınırlamaları ciddi oranda gevşettiği kanaatindedir. Özellikle terörist saldırılardan ciddi şekilde mağdur olmuş devletlerin teröristleri barındıran, destekleyen veya onlara tolerans gösteren başka devlet ülkelerine karşı silahlı kuvvet kullanmalarını meşru müdafaa hakkına dayandıracakları ve bunun da uygulanan hukuk olarak kabul edilmekte olduğu ifade edilmektedir.[85] Doktrinde *Kirgis* de bugün için meşru müdafaa hakkının teröristleri aktif olarak destekleyen ve onlara topraklarını açan devletlere karşı silahlı kuvvet kullanmayı içerdiğini söylemenin yanlış olmayacağını belirtmektedir. *Lowe* ise, bilerek topraklarını açmanın yanında topraklarını kontrol etmede başarısız ise de meşru müdafaa çerçevesinde ilgili devlete karşı kuvvet kullanılabileceğini, aksini düşünmenin uluslararası hukukta konseptsel değişim gerektiğinin kabulü olarak yorumlanacağını ifade etmektedir.[86]

Bush doktriniyle birlikte silahlı saldırının salt devlet-dışı aktörelerden gelebileceğini savunan görüşler ortaya atılmıştır.[87] Öyle ki meşru müdafaa hakkının teamül hukukuna dayanıyor olması, bunun sadece devlet kaynaklı silahlı saldırıya karşı kullanılabileceği şeklindeki bir kısıtlamaya imkân tanımadığı yönünde yorumlara vücut vermektedir.[88] Buna göre, günümüzde

---

[85] BYERS, Micheal: "*Terrorism, The Use of Force and International Law After 11 September*" International Law and Comparative Law Quarterly, Vol. 51, Iss. 2, 2002, s. 165.

[86] KAYA, s. 177, dn. 29'dan atfen.

[87] GREENWOOD, Christopher: *"International Law and the Pre-emtive Use of Force: Afganistan, AL-Qaiada and Iraq*", San Diego Int'l Law, Journal, 2003, s. 17; MAOGOTO, s. 431; SCHMITT, Micheal, *"Pre-emtive Strategies in International Law",* Michigan Journal of International Law, Vol. 24, 2003, s. 538.

[88] KAYA, s. 183.
Özellikle II. Körfez savaşıyla başlayan işbu tartışma, Suriye'de çıkan iç savaşa müdahale ile sahneye çıkan Irak – İslam Şam Devleti (İŞİD)'nin Suriye ve Irak'taki terör faaliyetleri dolayısıyla, işbu örgütle olan mücadele açısından daha karmaşık bir hal almıştır. Müdahalelerini kolektif meşru müdafaa hakkıyla açıklayan devletler, mevcut durumun hangi unsurları karşıladığına ilişkin ayrıntılı bir gerekçe vermekten yoksundur. Üstelik, BM Güvenlik Konseyi, 11 Eylül'den sonraki kararlarındaki gibi, 20 Kasım 2015 tarihinde verdiği kararda, bireysel ya da kolektif meşru müdafaa hakkına değinmemiştir; BM Şartı Bölüm VII.'den hiç bahsetmeksizin devletleri sadece tedbir almaya davet etmiştir. Bkz. UN. Doc. S/RES/2249 (2015), 20 November 2015. Kanımızca bu durum, devlet-dışı gruplara karşı meşru müdafaa hakkının varlığını pekiştirmemekte, zaten açık olmayan bir konuyu daha da bulandırmaktadır. O nedenle, işbu karara dayanarak, devlet-dışı gruplara karşı bireysel/kollektif meşru müdafaa hakkının meşruluğu ve hatta hukuka uygunluğu halen gri bir alan olup tartışmaya açıktır. Ayrıntılı bilgi için bkz. KAJTAR, Gabor*, "The Use of Force*

devlet-dışı/terörist örgütlerin neden olduğu zararın ve tehdidin devletlere kıyasla daha büyük olduğu dikkate alınarak, sadece devletlerin silahlı saldırı gerçekleştirme kapasitesine sahip olduğu düşüncesinin yeniden değerlendirilmesi ve meşru müdafaa hakkının devlet-dışı aktörlerin faaliyetlerini de kapsayacak şekilde yorumlanması gerektiği savunulmaktadır.[89]

Meşru müdafaa hakkının devlet dışı gruplara karşı da kullanabileceğini ifade eden yazarlar genelde meşru müdafaa hakkının örf ve adet hukukundan gelen unsurlarının oluşumuna öncülük eden *Caroline* olayına atıf yapmaktadırlar. Çünkü bu olay meşru müdafaa hakkının unsurlarını ortaya koymanın yanında, devlet dışı gruplara karşı meşru müdafaa hakkını kullanmayı da içermektedir.[90] Devlet uygulamalarına da değinen yazarlar, son dönemde devlet-dışı örgütlere karşı yapılan müdahalenin devletler tarafından tolere edildiğini, devletlerin işbu uygulamaları ne açıkça hukuka uygun kabul ettiğinin ne de hukuka aykırı olduğu gerekçesiyle kınandığının görüldüğünü ifade etmektedirler.[91] Bu durum da söz konusu devlet faaliyetlerinin giderek meşruluk kazandığı yorumuna sebep olmaktadır. [92]

Son olarak meşru müdafaa hakkının saldırının kaynağı açısından geniş yorumunu reddeden ve dolaylı silahlı saldırıyı UAD'nin Nikaragua kararında çizdiği sınırlarla yorumlayan yazarlar, ABD'nin ve BK'nın Afganistan'a karşı ileri sürdüğü meşru müdafaa hakkının varlığını reddetmektedirler. Örneğin *Paust,* dolaylı silahlı saldırı bakımından devletler devlet-dışı örgüt arasındaki

---

Against ISIL in IRaq and Syria- A Legal Battlefield", Wisconsin International Law Journal, Vol. 34, No. 3, s. 535.

89 GREENWOOD, s. 17.

90 BRING, Owe, *"The Use of Force under the UN Charter: Modification and Reform through Practice or Consensus",* içinde International Law and Changing Perceptions of Security Liber Amicorum Said Mahmoudi (EBBESSON, Jonas vd. ed.), BRILL, The Netherlands, 2014, ss. 4- 6; DINNIS, Hether Harrison, Cyber Warfare and the Laws of War", Cambridge, 2012, ss. 102–104; GILL – DUCHEINE, ss. 453- 458.

91 HAKIMI, Monika, *"Defensive Force Against Non-State Actors: The State of Play",* International Legal Studies, Vol. 91, 2015, s. 30.

92 WEE YEN, Jean, *"The Use of Force Against Non-State Actors: Justifying and Delimiting the Exersice of the Right of Self-Defence",* Singapure Law Review, Juris Illuminae, Vol. 9, 2017, s. 4.
Yazar devlet-dışı aktörlere karşı meşru müdafaa hakkının kullanılabileceğini kabul etmekle birlikte, devletlerin egemen eşitliği ilkesi bağlamında son dönemde giderek yaygınlaşan meşru müdafaa gerekçeli askeri müdahaleleri değerlendirmektedir. Bu durumda, devlet-dışı gruplara karşı meşru müdafaa hakkının herhangi bir suistimale maruz kalmaksızın, uluslararası barış ve güvenliğe hizmet edecek şekilde kullanılması gerektiğinin de altını çizmektedir. WEE YEN, s. 8.

bağı hafifleten yaklaşımların meşru müdafaa hakkının kapsamını genişletmesi dolayısıyla, kabul edilemez olduğunu ifade etmektedir.[93] Devlet-dışı gruplar veya terör örgütleri tarafından gerçekleştirilen siber saldırılar bakımından da aynı husus geçerli olacaktır.[94]

Günümüze kadar devletlerin maruz kaldıkları geniş çaplı ve etkili siber saldırıların doğrudan devlete atfedildiği bir olay gerçekleşmemiştir.[95] Dolayısıyla salt terör örgütleri ya da devlet desteği olmayan grupların, gerçekleştirdikleri siber saldırılar başka kuvvet kullanma yasağının kapsamına girmeyecek silahlı saldırı boyutuna varsa dahi saldırıya uğrayan devletin meşru müdafaa hakkının varlığından bahsetmek mümkün olamayacaktır.[96] Siber saldırıya karşı meşru müdafaa hakkının kullanılabilmesi için ise gerçekleştirilen saldırıların hangi hallerde devletlerle ilişkilendirilebileceğinin tespiti önem arz eder hale gelmektedir.[97]

---

93 PAUST, Jordan J., "Use of Armed Force against Terrorists in Afghanistan, Iraq, and Beyond", Cornell International Law Journal, Vol. 35, No. 3, 2002, s. 532.

94 Aksi görüş için bkz. LOTRIONTE, s. 865. *Lotrionte,* bu sonuca yorum yoluyla ve devlet uygulamalarıyla ulaşılabileceğini ifade etmektedir. Bu noktada, özellikle 11 Eylül öncesi devlet uygulamalarının doktrinde farklı yorumlandığı sonucuna varmamız mümkündür. Örneğin *Clatham Hause* belgelerinde bir saldırıya karşı, saldırının devletten ya da devlet dışı bir gruptan geldiğinin önemi olmaksızın meşru müdafaa hakkının kullanılabileceği görüşü ortaya atılmıştır. WILMSHURT, ss. 11- 13.

95 Sadece İran'ın nükleer reaktörünü çalıştıran sisteme kötü amaçlı yazılımın bulaştırılması olarak cereyan eden Stuxnet olayının meşru müdafaa hakkına vücut verecek unsurları taşıdığı ifade edilmektedir. DINNISS, s. 57.
Ancak İran hükümeti söz konusu saldırının reaktörü bozması neticesinde oluşabilecek hasarın Batı medyası tarafından abartıldığını ifade etmiş ve hiçbir zaman meydana gelen bu olayı meşru müdafaa hakkına vücut verecek siber saldırı olarak değerlendirmemiştir. KITTICHAISAREE, s. 167.
Tallinnn El Kitabı 2.0'da da Stuxnet saldırısıyla ilgili, uzmanlar heyetinde yer alan akademisyenlerin farklı görüşler ileri sürdükleri görülmüştür. Bkz. Kural 83- 84.

96 Tallinn El Kitabı 2.0, Kural 71, paras. 18- 19.
Aksi görüş için bkz. JUTTA, B.- STEPHEN J. T., Legitimacy and Legality in International Law: An Interactional Account, Cambridge University Press, Cambridge, 2010, s. 296; THOMAS, M. F., *"Terrorism and the Right of Self-Defense"*, AM. J. INT'L. L., Vol. 95, 2001, s. 840; Van STEENBERGHE, R., *"Self-Defence in Response to Attacks by Non-State Actors in the Light of Recent State Practice: A Step Forward?",* LEIDEN J. INT'L L., Vol. 23, 2010, s. 184; SEAN, D. M., *"Terrorism and the Concept of "Armed Attack" in Article 51 ofthe UN. Charter"*, HARV. INT'L L.J., Vol. 43, 2002, s. 50; GILL-DUCHEINE, ss. 452- 458.

97 Karşı görüş olarak önleyici meşru müdafaa hakkının varlığını kabul eden yazarlar, işbu hakkın siber faaliyetler bakımından da söz konusu olabileceğini kabul etmektedirler. GILL - DUCHEINE, s. 465.

Siber saldırıların devletlerle ilişkilendirilmesi açısından farklı görüşler ortaya atılmaktadır. Örneğin Hindistan, birbiriyle ve dünyayla sürekli iletişim halinde bir toplum haline gelinen günümüzde, devletlerin sadece kendi siber altyapılarını korumak değil; kendi siber altyapılarının başka devletlerin siber altyapılarına zarar verecek şekilde kullanılmasını engelleme yükümlülüğüne sahip olduğunu ileri sürmektedir.[98] ABD ise özellikle, siber saldırıya karşı meşru müdafaa hakkının kapsamına dair yaptığı açıklamada, devletlerin kendi ülkelerinin başka bir devlet ya da devlet-dışı grupların faaliyetleri için kullanılmaması için gerekli önlemleri alması gerektiğini savunmaktadır.[99] Rusya, Bilgi Güvenliği Sözleşmesi'nin taslak metnine ilişkin yapılan tartışmada, taraf devletlerin kendi ülkelerinde zarar verici bilgi faaliyetlerinde bulunmama ya da bilgi altyapısının zarar verici faaliyetler için kullanılmasına engel olma yükümlülüğüne sahip olması gerektiğini savunmuştur. Bunun dışında siber saldırıya engel olmak için işbirliğinde bulunmak, ilgili faaliyetleri ve faaliyetlerin sonuçlarını engellemek için de gerekli adımları atmak da devletlerin yükümlülükleri arasında bulunmalıdır. [100]

BM Genel Kurulu tarafından kurulan ve devletlerin konuya ilişkin uzmanlarında oluşan Uzmanlar Grubu tarafından 2013 yılında kaleme alınan raporda, devletlerin kendi ülkelerini devlet-dışı aktörlerin bilgi ve iletişim teknolojilerini hukuka aykırı olarak kullanılmadığını temin etmeleri gerektiğinin altı çizilmiş, devletlere işbu noktada yükümlülük verilmiştir.[101] Aynı şekilde Avrupa Konseyi'nin sınır ötesi İnternetin kullanımında uluslararası ve çok paydaşlı işbirliği hakkında raporunda, devletlerin siber suçlar için gerekli hukuki düzenlemeleri yapmak, sorumlular hakkında soruşturma ve kovuşturmada bulunmak, siber saldırıların soruşturulmasında diğer devletlerle işbirliği kurmak için gerekli özeni göstermesi gerektiği belirtilmiştir.[102]

---

98 KANUCK, Sean, *"Sovereign Discourse on Cyber Conflict Under International Law",* Texas Law Review, Vol. 88, 2010, s. 1591.

99 UN Doc A/66/152, 15 July 2011, s. 19.

100 Draft Convention on International Information Security (Concept), 2011, 6/II. md. Metin için bkz. http://www.mid.ru/en/foreign_policy/official_documents//asset_publisher/CptICkB6BZ29/content/id/191666 (e.t. 30.05.2018).

101 TOURE, Hamadoun, *"The International Response to Cyberwar",* içinde The Quest for Cyber Peace (TOURE, Hamadoun), ITU, January 2011, s. 103,.

102 LENTZ, Christopher, *"A State's Duty to Prevent and Respond to Cyberterrorist Acts"*, Chicago Journal of International Law, Vol. 10, 2010, ss. 820- 822.

Devletlerin, devlet-dışı grupların, örgütlerin ve bireylerin faaliyetlerinden haberdar olduğu ve engelleme, soruşturma ve kovuşturma yükümlülüğünü yerine getirmeleri için, sorumlu tutulmaları gerektiği savunulmaktadır. İşbu husus Uluslararası Hukuk Komitesi'nin Devletlerin Uluslararası Sorumluluğuna İlişkin Taslak Kurallar'ın özel kişilerin faaliyetlerin devletlerin sorumluluğunu doğurabileceğine ilişkin 1. maddesinin geniş yorumu olarak karşımıza çıkmaktadır. İşbu durumda devletin dolaylı siber saldırıda bulunduğunun kabul edilmesi gerektiği ve mağdur devletin meşru müdafaa hakkının doğacağı kabul edilmektedir.[103] Ayrıca klasik meşru müdafaa hakkını genişleten yaklaşımların, siber uzayda meydana gelen ve devletlere direkt ya da dolaylı olarak atfedilemeyen saldırılara karşı da yukarıda bahsettiğimiz diğer unsurların varlığının tespiti halinde, meşru müdafaa hakkının kullanılabileceği savunulmaktadır.[104]

c. Siber Saldırıya Karşı Kabul Ettiğimiz Meşru Müdafaa Hakkı

Kuvvet kullanma yasağının *jus cogens* kural olarak yasaklanması karşısında, işbu yasağın tek istisnasını teşkil eden meşru müdafaa hakkının mümkün olduğunca dar yorumlanması, uluslararası barış ve güvenliğin korunması açısından oldukça önemlidir. Bu bakımdan kanımızca ilgili yaklaşım sadece, maddi dünyada değil, siber dünyada da geçerli olmalıdır. Hatta siber dünyada meşru müdafaa hakkının kullanımı daha da kısıtlı olmalıdır, çünkü saldırının silahlı saldırıya ulaşıp ulaşmadığının tespiti muğlak ve saldırının kaynağının tespit edilmesi ve herhangi bir devlete atfedilmesi oldukça zordur. Dolayısıyla meşru müdafaa hakkının kullanılabilmesi için siber saldırının bir devlet ya da devletle güçlü bağları olan devlet dışı bir grup ya da kişiler tarafından gerçekleştirilmesi gerekmektedir. Devlet destekli olmayan gruplar ve terör örgütleri tarafından gerçekleştirilen siber saldırılarla mücadele etmek için ise meşru müdafaa hakkının kullanılamayacağı aşikardır.

---

[103] DEREK, Jinks, *"State Responsibility for the Acts of Private Armed Groups",* Chicago Journal of International Law Vol. 4, 2003, s. 83; SHARP, Sr., Walter Gary, Cyberspace and the Use of Force, Aegeis Research Corporation, USA, 1999, s. 9. SHARP Sr, Walter Gary. *"The Past, Present, and Future of Cybersecurity*", Journal of National Security Law and Policy Vol. 4, 2010, ss. 13- 26.

[104] DINNISS, ss. 95- 99.

Siber saldırının boyunun silahlı saldırı gibi ağır ve etkili olması halinde uluslararası toplumun verebileceği cevap BM sistemi içinde öngörülen kolektif güvenlik sisteminin işletilmesi olacaktır.[105] Nitekim işbu durum, Tallinn El Kitabı'nda da tespit edilmiştir. Siber saldırının, herhangi bir devletle ilişkilendirilmesi mümkün olmasa bile, bir siber ortamda yapılan bir faaliyetin uluslararası barışı tehdit etmesi, bozması veya siber saldırı durumunun BM Güvenlik Konseyi tarafından tespit edilmesi ve bu tespit neticesinde alınacak kuvvet kullanma içermeyen ya da kuvvet kullanma içeren tedbirlerin alınması mümkün olabilecektir.[106] Siber saldırıyı engellemek için gerekli önlemleri almayan ve işbirliğinde bulunmayan devlet açısından ise, işbu durum bir uluslararası yükümlülüğün ihlali olup, ilgili devletin de uluslararası sorumluluğu doğacaktır.[107]

4. Siber Suçlar

a. Genel Olarak

Kuvvet kullanma düzeyine ulaşmayan siber saldırılar bakımından, uluslararası hukukun kapsamına giren ve siber güvenliğin diğer bir veçhesini oluşturan husus, siber suçlar ve siber suçlarla mücadeledir. Siber suçlar hem siber uzay ortamında hem de siber uzay aracılığıyla işlenen suçları muhteva etmektedir.

Siber suçlar, ülkemizde diğer adıyla bilişim suçları, siber uzayda verilerin işlenmesi, saklanması, tasnif edilmesi, terkibi ve iletimi ile ilgili olarak işlenen, bilgisayara, bilgisayar ağlarına, bilişim sistemine karşı direkt saldırılar ya da bu sistemlerin araç olarak kullanılarak işlenen haksız fiiller olarak tanımlanabilir.[108] Siber suçların şimdilik böyle tanımlanmasıyla birlikte, siber uzay teknolojisinin hızla gelişmesi ile insan öldürme suçuna dahil pek çok suçun bilişim yoluyla işlenebileceğinin mümkün olabileceği göz

---

[105] LOTRIONTE, ss. 850 – 851.

[106] BENTHELEM, Sir Daniel QC, *"Principles relevant to the Scope of a State's Right of Self-Defence against an Imminent or Actual Armed Attack by Non-State Actors,"* Amer. JIL., Vol. 106, 2012, s. 776. BM Şartı md. 41 – 44; Tallinn El Kitabı 2.0, Kural 77.

[107] Tallinn El Kitabı 2.0, Kural 14.

[108] İÇEL, Kayıhan: "Avrupa Konseyi Siber Suç Sözleşmesi Bağlamında 'Avrupa Siber Suç Politikasının Ana İlkeleri', İstanbul Üniversitesi Hukuk Fakültesi Mecmuası, C: LIX, Sayı: 1-2, 2001, s. 3; KURT, Levent; Tüm Yönleriyle Bilişim Suçları ve Türk Ceza Kanunundaki Uygulaması, Ankara, 2005, s. 49-53; ÖZEN, Muharrem/BAŞTÜRK, İhsan; Bilişim – İnternet ve Ceza Hukuku, Ankara, 2011, s. 90- 91.

önüne alındığında, siber suç tipinin sınırlarını belirlemenin mümkün olamayacağı sonucuna ulaşabiliriz.[109]

Siber suçlar küresel seviyede bireysel işlenebileceği gibi organize suç çeteleri tarafından da işlenebilmektedir. Özellikle siber suçların %80'nin organize şekilde işlendiği tespit edilmiştir.[110] Organize suç örgütlerinin işledikleri siber suçların sınır aşan niteliği sebebiyle de siber güvenlik uluslararası toplumu yakından ilgilendirir hale gelmiştir. Bu noktada da siber suçlarla mücadele ve siber güvenliği tesis edilmesi için devletlerin rolü yadsınamaz. Özellikle devletler arasında işbirliği kurulması, iç hukuk düzenlerinde siber suçların düzenlenmesinin teşvik edilmesi ve mevcut iç hukuk düzenlerinin ise yeknesak hale getirilmesi önem arz eder hale gelmiştir.

Nitekim uluslararası toplumda siber suçlarla mücadele için adımlar atılmakta Birleşmiş Milletler, OECD, Avrupa Birliği, Avrupa Konseyi, Şangay İşbirliği Örgütü, Hükümetler Arası Afrika Örgütü, Arap Devletleri Ligi gibi uluslararası ve bölgesel örgütler, aşağıda daha ayrıntılı anlattığımız üzere, siber suçlarla ilgili gerekli tedbirler hakkında kararlar almakta ve hatta uluslararası antlaşmalar akdetmektedirler..

Uluslararası toplumun başat aktörlerinden olan Birleşmiş Milletler'i ele alacak olursak, BM tarafında siber suçlarla mücadele ve uluslararası işbirliği açısından atılan somut adımlar, Birleşmiş Milletler Uyuşturucu ve Suç Ofisi bünyesinde kurulan açık uçlu hükümetler arası uzmanlar heyeti oluşturulmasıyla atılmıştır. 12 – 19 Nisan 2010 tarihleri arasında on ikincisi düzenlenen Suç Önleme ve Ceza Adaleti Kongresi sonunda kabul edilen Salvador Bildirisi'nin 42. maddesinde kabul edilen uzmanlar heyeti kurulması hususu, Genel Kurul'un 65/230 sayılı kararıyla hayatıyla geçirilmiştir.[111]

Söz konusu uzmanlar heyeti, uluslararası toplumu, üye devletleri, özel sektörü bir araya getirip, ulusal düzenlemeler, uygulamalar, teknik takip ve uluslararası işbirliği hakkında bilgi alışverişini sağlayarak, mevcut mücadele

[109] ÖZDİLEK, Ali Osman, Uygulamadan Örnek Olaylarla Bilişim Suçları ve Hukuku, İstanbul, 2006, s. 112.

[110] Comprehensive Study on Cyber Crime, Draft, United Nations, February 2013, s. xvii. Metin için bkz. https://www.unodc.org/documents/organizedcrime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf (e.t. 30.05.2018). Bundan sonra draft study olarak anılacaktır.

[111] UN Doc. A/RES/65/230, 21 December 2011.

yöntemlerini güçlendirmek ve yeni ulusal ve uluslararası mücadele yöntemleri geliştirmek amacıyla 2011 yılında toplantılara başlamıştır.[112]

Kurulduğu günden bu yana üç adet toplantı gerçekleştiren grubun ilk toplantısı 17-21 Ocak 2011 tarihlerinde Viyana'da gerçekleştirilmiştir. Yetmiş sekiz üye devletin yanında, BM'nin diğer organları ve kurumlarından, özel sektörden, uzmanlık örgütlerinden, diğer uluslararası örgütlerden de katılım sağlanmıştır.[113]

İlk toplantıda, özellikle siber suçlar ve siber suçlarla mücadele için uzmanlar heyeti tarafından yürütülecek kapsamlı çalışmada yer alacak olası konular üzerinde anlaşma sağlanmıştır. Buna göre, siber suç problemi, siber suçlara karşı hukuki tedbirler, siber suçlara karşı hukuk haricinde alınabilecek tedbirler, siber suç fenomenine karşı uluslararası toplumun yaklaşımı, teknik yardım, siber suçlara karşı özel sektörün yaklaşımı konuları seçilmiştir.[114]

Uzmanlar heyetinin ele alacağı konular arasında da ulusal hukuk sistemlerinin siber suçları düzenlemek bakımından ulusal hukuk sistemleri arasında uyum[115] ve uluslararası işbirliği de ön plana çıkan hususlardandır. Uluslararası işbirliği açısından özellikle uluslararası ve bölgesel uluslararası antlaşmaların rolü ve önemi belirtilmiştir.[116]

Uzmanlar heyetinin ikinci toplantısı da 25 – 28 Şubat 2013 tarihlerinde Viyana'da gerçekleştirilmiştir. İkinci toplantıya seksen yedi üye devlet yanında, BM Genel Sekreterlik üniteleri, BM suçu önleme ve cezai adalet ağına ilişkin kurumlar, uzmanlık kuruluşu, diğer uluslararası örgütler ve özel sektörden katılım sağlanmıştır.[117] İlk toplantıda kapsamının belirlendiği kapsamlı çalışmanın, işbu toplantıda taslağı oluşturulmuştur.

Söz konusu taslak çalışmada siber suçun giderek büyüyen küresel bir sorun olduğu ve uluslararası işbirliğini gerektiğinin altı bir kez daha çizilmiştir.[118] Taslak çalışmada ayrıca siber suç oluşturacak faaliyetlere ayrıca

---

[112] Bkz. https://www.unodc.org/unodc/en/organized-crime/open-ended-intergovernmental-expert-group-meeting-on-cybercrime.html (e.t. 28.05.2018).
[113] UNODC/CCPCJ/EG.4/2011/INF/2/Rev.1, 21 January 2011.
[114] UNODC/CCPCJ/EG.4/2011/2, ss. 2- 3.
[115] Draft study, ss. 58- 63.
[116] UNODC/CCPCJ/EG.4/2011/2, ss. 8- 9, 11- 13.
[117] UNODC/CCPCJ/EG.4/2013/3, s. 4.
[118] Draft study, s. xi.

yer verilmiştir. Buna göre siber suçlar üç temel kategoriye ayrılmıştır: bilgisayar verileri ve sistemlerinin gizliliği, bütünlüğü ve elverişliliğine karşı faaliyetler, kişisel ya da finansal kazanç sağlayan ya da zarara sebep olan bilgisayarla ilişkili faaliyetler ve içerikle ilgili faaliyetler.[119]

Birinci kategoride özellikle, bilgisayara sistemlerine hukuka aykırı erişim, bilgisayar verilerine hukuka aykırı şekilde erişme, verileri ele geçirme ya da elde etme, bilgisayar sistemlerine ya da bilgisayara verilerine hukuka aykırı müdahale, bilgisayar sistemlerinin kötüye kullanımını sağlamak amacıyla gerekli araçları üretme, dağıtma ya da ilgili araçlara sahip olma, mahremiyet ve veri korumasına ilişkin kuralları ihlal, siber suçlar olarak tanımlanmıştır.

İkinci kategoride ise, bilgisayar sistemleri aracılığıyla dolandırıcılık ya da hırsızlık, kimlik hırsızlığı, fikri mülkiyet, marka ve patent ihlalleri, spam elektronik postaları yollama ya da gönderimini kontrol etme, çocuk istismarı ya da çocukların kullanılması sayılmıştır.

Son kategoride ise, bilgisayar sistemi aracılığıyla nefret suçu işleme, çocuk pornosu üretme, dağıtma ya da bulundurma, terörist faaliyetleri destekleme yer almaktadır.

Birleşmiş Milletler tarafından hazırlanan söz konusu çalışmada, uluslararası hukuk sisteminde siber suçlarla ilgili hukuki düzenlemeleri içeren metinler, bağlayıcı olan ve bağlayıcı olmayan ayrımına tabi tutulmuştur. Biz de siber güvenliğin siber suçlarla mücadele veçhesini söz konusu çalışmanın sistematiğini takip ederek aktaracağız.

1. Uluslararası Toplumda Siber Suçları Düzenleyen Bağlayıcı Hukuki Metinler

Uluslararası arenada halihazırda seksen iki devlet, siber suçlarla mücadele için akdedilen bir uluslararası/bölgesel antlaşmanın tarafıdır.[120] İşbu metinler arasında Avrupa Konseyi Siber Suç Sözleşmesi ve Ek Protokolü, Avrupa Konseyi Çocukların Cinsel Suiistimal ve Cinsel İstismara Karşı Korunması Sözleşmesi, Avrupa Birliği elektronik ticaret, nakdi olmayan ödemelerde dolandırıcılık ve sahtekarlık, kişisel veri, bilgi Sistemlerine karşı

[119] Draft study, s. 16.
[120] Darft study, s. xix.

saldırı ve çocuk pornografisi hakkında direktif ve düzenlemeler, Bağımsız Devletler Topluluğu Bilgisayar Verisine Karşı Saldırıyla Mücadele Hakkında İşbirliği Sözleşmesi, Şangay İşbirliği Örgütü Uluslararası Bilgi Güvenliği Alanında İşbirliği Anlaşması, Batı Afrika Devletleri Ekonomik Topluluğu Siber Suçla Mücadele Direktifi Taslağı, Afrika'da Siber Güvenliği Sağlamak Maksatlı Hukuki Çerçevenin Oluşturulmasına İlişkin Afrika Birliği Sözleşmesi Taslağı, Arap Devletleri Ligi Bilgi Teknolojilerine Karşı Saldırılarla Mücadele Anlaşması, Çocuk Hakları Sözleşmesi Çocukların Satışı, Çocuk Fuhuşu ve Çocuk Pornografisi Hakkında Ek Protokol yer almaktadır. [121]

- Avrupa Konseyi Siber Suç Sözleşmesi: Avrupa Konseyi nezdinde Siber Suç Uzmanlar Komitesi'nin kurulmasıyla başlatılan çalışmalar, 23 Kasım 2001 tarihinde imzalanan Avrupa Siber Suç Sözleşmesi'ne vücut vermiştir. Yine aynı şekilde Bilişim Sistemleri Aracılığıyla İşlenen Irkçı ve Yabancı Düşmanı Eylemlerin Suç Haline Getirilmesi İçin Avrupa Siber Suç Sözleşmesi'ne Ek Protokol de 28 Ocak 2003 tarihinde imzaya açılıp, 1 Mart 2006 tarihinde yürürlüğe girmiştir.[122]

1 Temmuz 2004 tarihinde yürürlüğe giren Siber suç Sözleşmesi, her ne kadar bölgesel bir organizasyon tarafından akdedilse de evrensel olma iddiasındadır. Zira, sözleşmenin akdedilme çalışmaları, Konsey üyeleri haricinde, Kanada, Japonya, Güney Afrika ve Amerika Birleşik Devletleri'nin de katılımıyla gerçekleştirilmiştir. Ayrıca hazırlık çalışmalar haricinde, Konsey üyesi olmayan on dört devlet de halihazırda Sözleşme'nin tarafıdır.[123] 2010 yılında Avrupa Konseyi genel sekreterinin yaptığı açıklamada Sözleşme'nin siber suçlarla mücadelede açık ve kapsamlı yükümlülükler getirdiği, Asya-Pasifik Ekonomik İşbirliği, Avrupa Birliği, Interpol ve Amerika Devletleri Organizasyonu tarafından da oldukça desteklendiğini ifade etmiştir.[124]

---

[121] Draft study, s. 64.

[122] Halihazırda 23 Avrupa Konseyi devleti söz konusu Protokol'ün de tarafıdır. Liste için bkz. http://www.coe.int/en/web/conventions/full-list//conventions/treaty/189/signatures?p_auth=nOtm1q80 (e. t.30.05.2018).

[123] İşbu devletler Amerika Birleşik Devletleri, Avustralya, Kanada, Şile, Kosta Rika, Dominik Cumhuriyeti, İsrail, Japonya, Maritiyus Cumhuriyeti, Panama, Filipinler, Senegal, Sri Lanka, Tonga'dır. Liste için bkz. https://www.coe.int/en/web/conventions/search-on-treaties/conventions/treaty/185/signatures?p_auth=kyheDJdz (e.t. 15.05.2018).

[124] Contribution of the Secretary General of the Council of Europe to the Twelfth United Nations Congress on Crime Prevention and Criminal Justice, 16 Februrary 2010, VATIS, s. 219, dn. 100'den atfen.

Üç bölümden oluşan Sözleşme'de, ilk bölüm tanımları, ikinci bölüm siber suçlarla mücadelede alınacak ulusal tedbirleri, üçüncü bölümdeyse alınabilecek uluslararası tedbirleri içermektedir.

Ulusal hukuk sistemlerini yeknesaklaştırmak adına özel siber suç tiplerinin öngörüldüğü ikinci bölümün birinci kısmı oldukça önem arz etmektedir. Buna göre, bilgisayar verilerinin ve sistemlerinin gizliliğine, bütünlüğüne ve erişilebilirliğine yönelik suçlar (yasadışı erişim, yasadışı müdahale, verilere müdahale, sistemlere müdahale, cihazların kötüye kullanımı); bilgisayarla bağlantılı suçlar (Bilgisayarla bağlantılı sahtecilik, bilgisayarla bağlantılı dolandırıcılık); içerikle bağlantılı suçlar (çocuk pornografisiyle bağlantılı suçlar), telif hakkı ve bununla bağlantılı hakların ihlaline karşı suçlar, Sözleşme'de yer alan siber suç tipleridir.

İkinci bölümün devam eden ikinci kısım ve üçüncü kısmında ise, usul hükümlerinin kapsamı, alınabilecek tedbirler ve yargı yetkisi düzenlenmektedir.

Uluslararası toplumu özellikle ilgilendiren kısımda da siber suçlarla mücadele, uluslararası işbirliğine ilişkin hükümler öngörülmüştür. Üçüncü bölüm birinci kısmında uluslararası işbirliğine ilişkin genel ilkeler, suçluların iadesine ilişkin ilkeler, karşılıklı yardımlaşmaya ilişkin genel ilkeler (karşılıklı yardımlaşmaya ilişkin genel ilkeler, kendiliğinden bilgi verme), uluslararası andlaşmaların yürürlükte olmadığı hallerde yapılan karşılıklı yardım taleplerine ilişkin usuller (uluslararası andlaşmaların yürürlükte olmadığı hallerde yapılan karşılıklı yardım taleplerine ilişkin usuller, gizlilik ve kullanımın sınırlandırılması). İkinci kısımda ise uluslararası işbirliğine ilişkin özel hükümler kaleme alınmıştır. Buna göre; geçici tedbirlere ilişkin karşılıklı yardımlaşma (depolanan bilgisayar verilerinin acilen koruma altına alınması, korunan trafik bilgilerinin derhal açıklanması), soruşturma yetkileri konusunda karşılıklı yardımlaşma (depolanan bilgisayar verilerine erişim konusunda karşılıklı yardımlaşma, depolanmış bilgisayar verilerine izinli şekilde veya bu verilerin halka açık olduğu durumlarda sınır ötesi ulaşım, trafik verilerinin gerçek zamanlı toplanması hakkında karşılıklı yardımlaşma, içerik verilerine el konulmaması hususunda karşılıklı yardımlaşma), 7/24 iletişim ağı.

Siber suçlarla mücadeleyle siber güvenliğin tesis edilmesi için farklı yargı yerleri arasındaki işbirliği ile mümkün olabilecektir. Aksi durum siber güvenliği zedeleyip ve devletlerin egemenlik alanlarının ihlali sonuçlarına

vücut verecektir. Nitekim bu durum Amerika- Rusya olayında yaşanmıştır. ABD, Rusya'nın yardımı olmaksızın, kendi ülke sınırları dışında iki Rus hackerı Rusya serverlerı üzerinden takip etmiş, kullanıcı adları ve şifrelerini öğrenerek, yaptıkları hackerlık faaliyetlerle ilgili delil elde etmiştir. Nitekim ABD'nin kendi ülkesel sınırları dışında yürüttüğü işbu faaliyetin hukuka uygunluğu tartışma konusu olmuştur.[125] Bu bakımdan Sözleşme siber güvenliğin tesisi ve uluslararası hukukun barış ve güvenliği için önemli bir adım getirmiştir.

- Avrupa Birliği Düzenlemeleri: Avrupa Birliği elektronik ticaret düzenlemelerinde özellikle müşterilerine e-ticaret hizmeti sağlayan şirketlerin çerez politikası hakkında müşterilerini bilgilendirmeleri, aynı zamanda müşterilerinin kişisel verilerinin talep edilmesi halinde kullanıcının konuyla ilgili bilgilendirilmesi, müşterilerin kişisel verilerinin nereye kaydedileceği, müşterilerin kişisel verilerinin tutulduğu yerin her zaman müşteriler tarafından ulaşılabilir, değiştirilebilir ya da kaydın tamamen silinebilir olması gerektiği hususları düzenlenmiştir. Ayrıca e-ticaret şirketleri, kullanıcılarına, özellikle internet kanalıyla yapacakları ödemeler için yüksek derecede bir koruma sağlamakla yükümlendirilmiştir.[126]

Avrupa Birliği Konseyi tarafından nakdi olmayan ödemelerde dolandırıcılık ve sahtekarlığa ilişkin hukuki çerçeve kararında da ödeme araçlarıyla ilişkili saldırılar, bilgisayarla ilişkili ihlaller, bilgisayar sistemlerini kötüye kullanmak üzere üretilen araçlar yoluyla gerçekleştirilen ihlaller ile işbu suçlara iştirak etme, suçu azmettirme ve suça teşebbüs halleri için üye devletlere gerekli ceza ve yaptırımları düzenleme yükümlülüğü verilmiştir. [127]

Kişisel Verilerin Korunmasına İlişkin Direktif'te, elektronik iletişim sağlayıcıları hizmetlerinin güvenliğini sağlamak için gerekli teknik ve kurumsal tedbirleri almakla yükümlendirilmiştir. Aynı şekilde servis sağlayıcılar tarafından, kullanıcıların iletişim gizliliğinin temin edilmesi, kullanım neticesinde oluşan veri trafiğinin silinmesi ya da anonim hale

---

[125] WEBER, Amalie: The Council of Europe's Convention on CyberCrime, Berkeley Technology Law Journal, Vol. 18, 2003, s. 428.

[126] İlgili düzenleme için bkz. https://ec.europa.eu/growth/sectors/tourism/business-portal/understanding-legislation/legal-regulations-e-commerce_en (31.05.2018).

[127] Council Framework Decision of 28 May 2001 combatting fraud and counterfeiting of non-cash means of payment, 2001/413/JHA, 2 – 5. md. Metin için. Bkz. https://eur-lex.europa.eu/legalcontent/EN/TXT/PDF/?uri =CELEX:32001F0413&from=EN

getirilmesi, kullanıcıların ayrıntılı olmayan fatura alma hakkı, cevapsız ve gelen aramaların kimliğinin ifşası ve sınırları gibi düzenlemeler içermektedir. İşbu düzenlemeler hizmet alıcılarının kişisel verilerinin korunmasını sağlayarak bilgisayarla ilişkili herhangi bir suçun mağduru haline gelmemeleri açısından önem arz etmektedir.[128]

Bilgi Sistemlerine Karşı Saldırı Direktifi, bilgi sistemlerine karşı ihlalleri ve ilgili yaptırımları tespit etmek amacıyla kaleme alınmıştır.[129] İşbu direktif, aynı zamanda üye devletler arasında söz konusu ihlallerin önüne geçmek amacıyla işbirliğini geliştirmeyi amaçlamaktadır.[130] Direktif uyarınca bilgi sistemlerine hukuka aykırı erişim, bilgisayar sistemlerine hukuka aykırı müdahale, bilgisayar verilerine hukuka aykırı müdahale, siber suç kapsamında sayılmıştır. Ayrıca ilgili suçları işlemek için kullanılan araçların (bilgisayar programı vs. gibi) üretimi, satışı, tedariki, ithal edilmesi ve dağıtımının da suç kapsamına alınıp cezalandırılması ile ilgili suçlara iştirak eden, yardım ve yataklık eden veya teşebbüs eden kişilerin de cezalandırılması için gerekli düzenlemelerin yapılması yükümlülüğü de öngörülmüştür. [131]

Çocukların Cinsel İstismarı, Çocuk Fuhuşu ve Çocuk Pornografisi ile Mücadele Direktifi, özellikle çocuk pornografisiyle mücadele bakımından önem arz eden düzenlemeler içermektedir.[132] Direktif'in 5. maddesinde, çocuk pornosu bulundurmak, bilgi ve iletişim teknolojileri yoluyla çocuk pornosuna erişmek, çocuk pornosunun dağıtımı, yayını veya aktarımı, çocuk pornosu sunma, sağlama veya erişimi kolaylaştırma ve en sonunda çocuk pornosunu bizzat üretme, bilgi teknolojisiyle bağlantılı olarak çocuk

---

[128] Directive 2002/58/EC of the European Parliment and of The Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector, 4 – 8.md. Metin için bkz. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32002L0058&from=EN (31.05.2018).

[129] Diretive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on Attacks Against Information Systems and Replacing Council Framework Decision 2005/222/JHA. Metin için bkz. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32013L0040&from=EN (31.05.2018).

[130] Direktif 1. md.

[131] Direktif, 3- 8. md.

[132] Directive 2011/92/EU of the Europen Parliament and of the Council of 13 December 2011 on combating the sexual abuse and sexual explotitation of children and child pronography and replacing Council Framework Decision 2004/68/JHA. Metin için bkz. https://eur-lex.europa.eu/legalcontent/EN/TXT/PDF/?uri=CELEX :32011L0093&from=EN (e.t. 31.05.2018).

pornosuna ilişkin öngörülen yasak fiillerdir. Ayrıca bilgi ve bilgisayar teknolojileri ortamında bir yetişkin tarafından bir çocukla cinsel ilişkiye girme teklifi, bilgi ve bilgisayar teknolojileri ortamına çocuk pornografisi temin etmek amacıyla bir çocuğu fuhuşa teşvik etme teşebbüsü de bir suç tipi olarak tanımlanmıştır.[133]

Gerek çocuk pornografisi gerek Direktif'te öngörülen diğer suçlar bakımından da suç işleyen, suçu azmettiren, suça yardım ve yataklık eden ya da suça teşebbüs eden kişilerin cezalandırılması için üye devletlerin gerekli önlemi alması gerektiği düzenlenmiştir.

- Avrupa Konseyi Çocukların Cinsel Suistimal ve Cinsel İstismara karşı Korunmasına Sözleşme: 2007 yılında akdedilen Sözleşme, çocuk istismarı ile ilgili olarak Konsey'e üye devletler arasında ve ulusal düzenlerinde işbirliğini sağlama amacı gütmektedir.[134] Özellikle siber suçlar bakımından çocuk pornografisini düzenleyen Sözleşme, çocuk pornografisinin suç olarak düzenlenmesi için devletlerin gerekli tedbirleri alması yükümlülüğünü düzenlemiştir.

Sözleşme'nin 20. maddesinin ikinci fıkrasında çocuk pornografisi *"çocuğu gerçek veya temsili açık bir cinsel davranış içinde görsel olarak gösteren herhangi bir materyal veya çocuğun cinsel organlarının esas itibariyle cinsel amaçlarla gösterilmesi"* olarak tanımlanmıştır.

Sözleşme'nin 20. maddesi uyarınca, çocuk pornografisi üretmek, sunmak veya temin etmek, dağıtmak, tedarik etmek ve bulundurmak, bilgi ve iletişim teknolojilerini kullanarak, çocuk pornografisine erişimi sağlamak, ilgili suç tipine vücut veren fiiller olarak öngörülmüştür. Böylelikle, Sözleşme çocuk pornografisi ile bir şekilde bağlantısı bulunan kişileri cezalandırmak amacıyla kapsamlı bir düzenleme getirmiştir.

- Bağımsız Devletler Topluluğu Bilgisayar Esaslı Bilgiye Karşı Saldırıyla Mücadele Hakkında İşbirliği Sözleşmesi: 2001 yılında akdedilen Sözleşme'nin amacı, bilgisayar sistemlerine karşı yapılan saldırılarla mücadelede işbirliği sağlamak için, üye devletlerin uygulayacağı hukuki bir çerçeve oluşturmaktır.[135]

---

[133] Direktif, 6.md.
[134] Sözleşme, giriş.
[135] Sözleşme, giriş.

Sözleşme'nin 3. maddesinde tanımlanan siber suçlar hem bilgisayar sistemlerine karşı hem de bilgisayar sistemlerini kullanma yoluyla işlenen suçları muhteva etmektedir. Buna göre, bilgisayar sistemlerine hukuka aykırı erişim ve bu erişim neticesinde sistemlerin zarar görmesi, kapanması, bilginin değiştirilmesi ya da kopyalanması ya da bilgisayarın, bilgisayar sisteminin ya da ilgili ağların işlevinin bozulması; zararlı yazılımların üretimi, kullanımı ve dağıtımı; bilgisayarların, bilgisayar sistemlerinin veya ilgili ağların kullanımına ilişkin hukuk kurallarının bunlara erişimi olan kişi tarafından işbu bilgisayar, bilgisayar sistemleri veya ağlarına zarar vermek, kapatmak, sistemde yer alan verilerin değiştirilmesi veya bunlara ciddi manada zarar verebilecek herhangi bir fiil, fikri mülkiyet kurallarıyla korunan bilgisayar veya veri tabanlarının hukuka aykırı kullanımı ya da yazılım korsanlığı gibi bilgisayar sistemlerine kayda değer zarar veren faaliyetler, siber suç oluşturabilecek suçlar olarak tanımlanmıştır. Ancak kanımızca siber suçların üye devletler tarafından yeknesak olarak düzenlenmesini sekteye uğratacak bir husus, "kayda değer hasar", "ağır sonuçlar" ve "ciddi derece zarar" gibi kavramların içerik ve kapsamının tayini üye devletlerin iç hukuk düzenine bırakılmıştır.

- Şangay İşbirliği Örgütü Uluslararası Bilgi Güvenliği Alanında İşbirliği Anlaşması: 2009 yılında akdedilen anlaşmada uluslararası bilgi güvenliği için öncelikle devletler arasında karşılıklı güvenin derinleştirilmesi ve devletler arasında işbirliğinin geliştirilmesinin gerekli olduğu ifade edilmiştir.[136] Uluslararası bilgi teknolojilerini genel olarak düzenleyen Sözleşme, siber suçları uluslararası bilgi güvenliğine karşı temel tehditlerden biri olarak tanımlamış ve siber suçlarla mücadeleyi bilgi güvenliğiyle ilgili temel işbirliği alanlarından biri olarak saymıştır.[137]

Sözleşme'nin I. ekinde siber suçlar, hukuka aykırı amaçlarla bilgi kaynaklarını kullanma ve/veya onları etkileyecek nitelikte faaliyetlerde bulunma olarak tanımlanmıştır.

Ek II'de siber suçu düzenleyen maddede de siber güvenliğe karşı bir tehdit olarak görülen siber suç, bireylerin ya da grupların bilgi kaynaklarını hukuka aykırı kullanımı ya da söz konusu kaynaklara haksız müdahalenin genel olarak siber suç tipine vücut vereceği ifade edilmiştir.[138]

---

[136] Sözleşme metni için bkz. http://eng.sectsco.org/documents/ (e.t. 30.05.2018).
[137] Sözleşme 2/I-3 md., 3/I-5 md.
[138] Sözleşme, Ek-I.

Söz konusu genel tayinden sonra hangi fiillerin siber suç teşkil ettiğini düzenleyen ikinci fıkrada; bilgi sistemlerine girmek suretiyle, söz konusu sistemlerin bütünlüğüne, erişimine ve gizliliğine zarar vermek, kasten bilgisayar virüsü ve sair zararlı yazılımları üretmek ve dağıtmak; DOS saldırıları düzenlemek ve diğer olumsuz etkilere yol açmak, bilgi kaynaklarına zarar vermek; bilgi alanında şahısların, fikri mülkiyet hakları ve gizliliği de dahil olmak üzere, hak ve özgürlüklerini zedeleyici faaliyetlerde bulunmak, bilgi kaynak ve yöntemlerini kullanarak işlenen dolandırıcılık, yolsuzluk, şantaj, kaçakçılık, uyuşturucu ticareti, çocuk pornosu suçları siber suç tipleri olarak düzenlenmiştir.[139]

- **Batı Afrika Devletleri Ekonomik Topluluğu Siber Suçla Mücadele Direktifi Taslağı:** 2009 yılında kaleme alınan taslak, üç ana bölümden oluşmaktadır. Avrupa Siber Suç Sözleşmesi'ne benzer olarak, siber suç tiplerini öngören maddi ceza hukuku bölümü, usul kuralları ve yargısal işbirliği bölümleri yer almaktadır.

Bilgisayar sistemlerine hileli erişim ve sistemde bulunma, bilgisayar sistemlerine müdahale, bilgisayar sistemlerine hileli olarak veri girişi bilgisayar verilerini hileli olarak ele geçirmek, bilgisayar verilerinin hileli olarak değiştirilmesi, bilgisayar verilerinin hileli üretilmesi, bilgisayar sistemleriyle hileli yollarla yapılan müdahaleyle herhangi bir yarar elde etme, kişisel verilerin kötüye kullanılması, siber suç işlemek amacıyla gerekli araçları elde etmek, çocuk pornografisi üretimi, siber uzay yoluyla ihraç ve ithal edilmesi, bulundurulması, ırkçı ve zenofobik belgelerin bulundurulması, bilgisayar sistemleri yoluyla tehdit, bilgisayar sistemleri yoluyla küçük düşürme, maddi siber suçlar olarak öngörülmüştür.[140] Burada özellikle diğer hukuki enstrümanlardan farklı olarak ırkçı söylemlerin özellikle Afrika topluma yönelik olarak ırkçı söylemlerin siber suç teşkil etmesini öngörmesi açısından önem arz eden bir metindir.

- **Arap Devletleri Ligi Bilgi Teknolojilerine Karşı Saldırılarla Mücadele Anlaşması**: Söz konusu Anlaşma'nın yine giriş bölümünde ve 1. maddede yer aldığı üzere Arap devletleri topluluğunun güvenliğini ve çıkarlarını tehdit eden bilgi teknolojilerine karşı saldırılarla mücadelede işbirliğini geliştirmek ve güçlendirme amacı taşımaktadır.[141] Aynı şekilde,

[139] Söleşme, EK-II, md. 3.
[140] Direktif taslağı, 2-20. Md.
[141] Sözleşme metnine ulaşmak için bkz. http://itlaw.wikia.com/wiki/Arab_Convention_on_Combating_Infor mation_Technology_Offences (e.t. 30.05.2018).

işbu anlaşma da Arap devletlerinin Anlaşma'da tanımlanan siber suç tiplerinin yeknesak olarak düzenlemesi gerektiği ifade edilmektedir.[142]

Anlaşma'da siber suç tipleri olarak da bilgi teknolojilerine hukuka aykırı erişim, ele geçirme, bilgisayar verilerinin bütünlüğüne karşı saldırı, bilgi teknolojilerinin suiistimal edilmesi, sahtecilik, dolandırıcılık, pornografi, pornografiyle bağlantılı diğer saldırılar (kumar ve seks tacirliği), kişi mahremiyetine karşı saldırılar, bilgi teknolojileri yoluyla gerçekleştirilen terör faaliyetleri, bilgi teknolojileri yoluyla işlenen organize suçlar, telif hakkı ve diğer haklara ilişkin saldırılar, elektronik ödeme araçlarının hukuka aykırı kullanımı gibi fiiller siber suçlar olarak tanımlanmıştır. Söz konusu anlaşmada da farklı olarak pornografinin her türlüsü yasaklanmış olup çocuk pornografisinin ise ağırlaştırılmış şekilde cezalandırılması gerektiği öngörülmüştür.[143]

- Çocuk Hakları Sözleşmesi Çocukların Satışı, Çocuk Fuhuşu ve Çocuk Pornografisi Hakkında Ek Protokol: Söz konusu Protokol'de de yine dikkatimizi çeken önemli hususlardan birisi çocukların satışı, çocuk fuhuşu ve çocuk pornografisi ile mücadelede uluslararası işbirliğinin ön plana çıkarılmasıdır.[144] Bunun yanında söz konusu ihlallerin önüne geçebilmek adına devletlerin kendi iç hukuk düzenlerinde gerekli düzenlemelerin yapılması öngörülmüştür.[145] Çocuk pornografisi ve çocuk istismarıyla ilgili diğer hususlara ilişkin olarak Sözleşme devletler üzerinde sadece cezalandırıcı önlemleri öngörmeyip toplumu konuyla ilgili bilinçlendirme yükümlülüğü, gerekli sosyal politikaları geliştirme ve uygulama yükümlülükleri öngörmektedir. Bu durumda Protokol'ün amacı sadece gerçekleştirilen faaliyeti cezalandırmak değil, çocuk istismarının önüne geçmektir.[146]

2. Uluslararası Toplumda Siber Suçları Düzenleyen Yumuşak Hukuk Kuralları

Başka bir ifade ile bağlayıcı olmayan düzenlemeler olarak da adlandırılan işbu kurallar devletlere siber suçlarla mücadelede işbirliği kurmak ve iç hukuk kurallarını yeknesak hale getirmeleri için bir rehber işlevi görmektedir.

---

142 Anlaşma 5.md.
143 Anlaşma 12.md.
144 Protokol 10. Md. Prokol metni için bkz.http://www.ohchr.org/EN/ProfessionalInterest/Pages/OPSCCRC.aspx (e.t. 30.05.2018).
145 Protokol 3. Md.
146 Protokol 9. Md.

İşbu bölümde Uluslararası Telekomünikasyon bünyesinde oluşturulan ve Avrupa Birliği 9. Avrupa Kalkınma Fonu ve ITU tarafından finanse edilen @CP-ICT programı kapsamında Bağımsız Devletler Topluluğu, Afrika, Karayipler ve Pasifik adalarını konu edinen üç farklı model kanun metni hazırlanmıştır. Söz konusu model kanunları temel amacı bölgede yer alan devletler arasında iç hukuk düzenlerini yeknesaklaştırmak ve devletler arasında işbirliğini teşvik etmek ve geliştirmektir. Söz konusu modeller aşağıda yer alan örgütler tarafından hayata geçirilmiştir.[147]

- Bağımsız Devletler Topluluğu Bilgisayar ve Bilgisayarla İlişkili Suçlar Hakkında Model Kanun: Söz konusu model kanun üç bölümden oluşmakta özellikle maddi siber suçları ve özellikle devletler arasında işbirliği kurulmasını sağlayacak usul kurallarını öngörülmektedir.[148] Model kanunun II. bölümünde öngörüldüğü üzere hukuka aykırı erişim, bilgisayar verilerine müdahale, bilgisayar sistemlerine müdahale, veri ve sair içeriği hukuka aykırı alıkoyma, siber suç işleme maksadıyla gerekli araçlara sahip olma ve çocuk pornografisi, siber suç tipleri olarak düzenlenmiştir.

- Doğu Afrika Topluluğu Hukuki Çerçeve Taslağı: Doğu Afrika Milletler topluluğunun da siber suçlarla mücadelede iç hukuk düzenlerinin özel olarak suç tipinin düzenlenmesini ve gerekli yaptırımların uygulanmasına ilişkin bir politika oluşturması söz konusudur.[149]

- Güney Afrika Kalkınma Topluluğu Bilgisayar Suçları ve Siber Suçları Hakkında Model Kanun: İlgili model kanun altı bölümden oluşmakta olup maddi siber suç kurallarını, yargı yetkisini, elektronik delil, usul kuralları ve devletlerin sorumluluğuna ilişkin kurallara yer verilmiştir.[150]

---

147 Cybercrime Model Laws, Discussion paper prepared fort he Cybercrime Convention Committee (T-CY), 9 December 2014, ss. 7- 29. Metin için bkz. https://rm.coe.int/1680303ee1 (et. 30.05.2018).

148 İlgili metin için bkz. http://thecommonwealth.org/sites/default/files/key_reform_pdfs/P15370_11_ROL_ Model_Law_Computer_Related_Crime.pdf (et. 30.05.2018).

149 Harmonizing Cyberlaws and Regulations: The Experinece of the East African Community, UNCTAD/STICT/2012/4, United Nations, 2012, s. 5-10.http://repository.eac.int:8080/bitstream/handle/11671/1815/EAC%20Framework%20for%20Cyberlaws.pdf?sequence=1&isAllowed=y (e.t. 30.05.2018)

150 https://www.itu.int/en/ITU-D/Cybersecurity/Documents/SADC%20Model%20Law%20Cybercrime.pdf (e.t.30.05.2018).

Özellikle maddi siber suçlara yer verilen bölümde, hukuka aykırı erişim, hukuka aykırı sistemde kalma, hukuka aykırı veri ele geçirme, hukuka aykırı veri müdahalesi, veri casusluğu, hukuka aykırı sistem müdahalesi, hukuka aykırı araçlar, bilgisayarla ilişkili sahtecilik, bilgisayarla ilişkili dolandırıcılık, çocuk pornografisi, pornografi, kimlikle ilişkili suçlar, ırkçı ve zenofobik içerik, ırkçı ve zenofobik aşağılama, soykırımın ve insanlığa karşı suçların inkarı, Spam, bir soruşturmanın ayrıntılarının açığa vurulması, yardım sağlama yükümlülüğünün yerine getirilmemesi, elektronik haberleşmenin istismar edilmesi gibi fiiller siber suçlar kapsamında değerlendirilmiştir.[151] Burada görüldüğü üzere, özellikle bilgisayar sistemleri yoluyla işlenen siber suçların oldukça geniş kapsamda düzenlenmesi, siber suçlarla mücadele açısından kanımızca önem arz etmektedir.

- Karayip Devletleri HIPCAR Model Kanunu: Siber Politikaları, Kanun ve Yönetmelikleri Yeknesaklaştırma projesi (ICT) kapsamında hazırlanan Model Kanun aşağıda yer verilen model kanunlara da örnek olacak şekilde maddi siber suç tiplerine, usul hukuku kurallarına, yargı yetkisine ve devletler arasında işbirliğine yer vermiştir.[152] Bilgisayar sistemlerine hukuka aykırı erişim, hukuka aykırı alıkoyma, veri müdahalesi, sistem müdahalesi, araçların kötüye kullanımı, bilgisayar yoluyla sahtekarlık, bilgisayar yoluyla dolandırıcılık, çocuk pornografisi, telif ve ilgili haklar bakımından hukuka aykırı saldırılar siber suç tipleri ve suç işleme yanında suça teşebbüs, yardım ve yataklık ve azmettirme cezai sorumluluk halleri olarak öngörülmüştür.[153]

- Doğu Karayip Devletleri Örgütü EGRIP Model Kanunu: Elektronik Hükümet için Bölgesel Entegrasyon Projesi kapsamında hazırlanmıştır.[154] Maddi hukuk kuralları, usul hukuku kuralları, yargı yetkisi ve uluslararası işbirliği olmak üzere toplan dört ana bölümden oluşan model kanun, hukuka aykırı erişim, hukuka aykırı alıkoyma, veri müdahalesi, sistem müdahalesi, araçların kötüye kullanımı, bilgisayar yoluyla sahtekarlık, bilgisayar yoluyla dolandırıcılık, çocuk pornografisi, telif ve ilgili haklar bakımından hukuka aykırı saldırılar siber suç tipleri olarak tanımlanmıştır. Ayrıca sadece suçu

[151] Model Kanun, 4 – 22. Md.
[152] Proje hakkında bilgi ve kanun metni için bkz. https://www.itu.int/ITU-D/projects/ITU_EC_ACP/hipcar/in-country_assistance/Grenada/HIPCAR-Grenada_Cybercrime_Report_Final_Draft_April2012.pdf (e.t.31.05.2018).
[153] HIPCAR, 3 – 12. md.
[154] Metin için bkz. http://www.oecs.org/jobs/e-gov (e. t. 31.05.2018).

işleme değil, suça teşebbüs, yardım ve yataklık ve suçu azmettirme hallerinin de cezai sorumluluğa vücut vermesi düzenlenmiştir.[155]

- **Pasifik Adası Devletleri (ICB4PAC) Model Kanunu:** Aynı dörtlü metodolojinin izlendiği model kanun, siber suç tiplerinin tayin edilmesi, usul hukuku kurallarının düzenlenmesi, yargı yetkisi ve siber suçla mücadelede uluslararası işbirliği hususları yer almaktadır. Bilgisayar sistemlerine hukuka aykırı erişim, hukuka aykırı alıkoyma, veri müdahalesi, sistem müdahalesi, araçların kötüye kullanımı, bilgisayar yoluyla sahtekarlık, bilgisayar yoluyla dolandırıcılık, çocuk pornografisi, telif ve ilgili haklar bakımından hukuka aykırı saldırılar siber suç olarak tanımlanmıştır. Ayrıca suça teşebbüs, yardım ve yataklık ve suça azmettirme halleri de cezai sorumluluk için yeterli olacaktır.[156]

III. SİBER GÜVENLİK VE TÜRK HUKUKU: ULUSAL SİBER GÜVENLİK ORGANİZASYONUNUN YAPISI

A. Genel Olarak

Ülkemizde bilgi ve iletişim sistemlerinin kullanımı hızla yaygınlaşmakta, bu sistemler hayatımızın her alanında önemli rol oynamaktadır. Kamu kurumlarına ek olarak enerji, haberleşme, su kaynakları, tarım, sağlık, ulaşım, eğitim ve finansal hizmetler gibi kritik altyapı sektörlerinde faaliyet gösteren kurum ve kuruluşlar da bilgi ve iletişim sistemlerini yoğun biçimde kullanmaktadır. Sözü edilen sistemler, verilen hizmetin kalitesini ve hızını artırmakta, dolayısıyla hem ilgili kurumun daha verimli çalışmasını sağlamakta, hem de vatandaşların yaşam standardının yükselmesine katkıda bulunmaktadır.

Kamu kurumlarının hizmet sunumlarında bilgi ve iletişim sistemlerini her geçen gün daha fazla kullanmaları ile birlikte, söz konusu bilgi ve iletişim sistemlerinin güvenliğinin sağlanması hem ulusal güvenliğin, hem de rekabet gücünün çok önemli bir unsuru haline gelmiştir. Bilgi ve iletişim sistemlerinde bulunan veya meydana gelebilecek güvenlik zafiyetleri, bu sistemlerin hizmet dışı kalmasına veya kötüye kullanılmasına, can kaybına,

[155] E-Gorvernment Interoperability Framework, 2- 12. md.
[156] https://www.itu.int/en/ITU-D/Projects/ITU-EC-ACP/ICB4PAC/Pages/default.aspx (et. 31.05.2018)

büyük ölçekli ekonomik zarara, kamu düzeninin bozulmasına veya ulusal güvenliğin ihlaline neden olabilecektir.

Bu bağlamda, ulusal güvenliğin en önemli alt bileşenlerinden olan siber güvenliğin düzenlenmesi ülkelerin en önemli tartışma başlıklarından birisidir. Birçok ülke, uluslararası gelişmelere paralel olarak, kendi ulusal siber güvenlik stratejisini belirlemiş ve buna ilişkin siber güvenlik stratejisi belgesini yayımlamış, gerekli tedbirleri almaya başlamıştır. Söz konusu strateji belgelerinde siber güvenlik salt kamu kurumlarına ve sistemlere yapılan siber saldırılara karşı koyma şeklinde ele alınmamakta, aynı zamanda bilişim ağlarının siyasi otoriteye, ulusal menfaatlere, kritik altyapılara karşı kullanılmasının engellenmesine yönelik strateji ve politika geliştirilmesi biçiminde de değerlendirilmektedir.

Siber güvenlik, siber ortamda kişi, kurum ve kuruluşların varlığını korumak amacıyla geliştirilen plan, program ve uygulamalar bütünlüğüdür. Kişi ve kurumların sistemleriyle ilgili her zaman sorun olabilir. Ancak, eğer bir sistem başka bir kişi veya grup tarafından, oradan bir kazanç elde etmek, bilgi toplamak, sistemi zayıflatmak veya sistemin işlemesini engellemek için müdahaleye uğruyorsa, buradaki siber sorun artık bir "siber güvenlik" sorunu haline gelir.[157] Bu kapsamda, ulusal siber güvenlik, bilişim sistemlerini kullanarak ulusal güvenliğine tehdit oluşturan faaliyetlere karşı geliştirdiği siber politika, strateji ve uygulama bütünlüğü iken; teknik anlamda siber güvenlik de bilişim sisteminin erişilebilirlik, bütünlük ve gizlilik özelliklerini ifade etmektedir.

Devletler, bu kapsamda, siber güvenliği tehdit edecek unsurlara karşı politikalar üretmek durumundadırlar. Siber alanda ortaya çıkan tehditler, bilişim sistemlerine verilen fiziki zararlar, bilgi hırsızlığı veya siber casusluk gibi alanlarda ortaya çıkabileceği gibi, kamu kurumlarının bilişim sistemlerindeki güvenlik açıklarının ifşası veya devletlerin son dönemlerde üzerinde durduğu karşı propaganda faaliyetleri şeklinde de meydana gelebilir[158].

---

[157] SINGER, P.W. / FRIEDMAN, Allan, Cybersecurity and Cyberwar: What Everyone Needs to Know, NewYork, 2014, s. 34.

[158] GEERS, Kenneth, "Cyberspace and the Changing Nature of the Warfare", http://www.blackhat.com/presentations/bh-jp-08/bh-jp-08-Geers/BlackHat-Japan-08-Geers-Cyber-Warfare-Whitepaper.pdf, (e.t. 09.03.2018).

"Siber tehdit" kavramı, 2012 yılında Milli Güvenlik Siyaset Belgesine de ulusal bir tehdit unsuru olarak girmiştir[159]. Bakanlar Kurulu'nun 11.6.2012 tarihli ve 2012/3842 sayılı kararı ile ulusal siber güvenlik çalışmalarının yürütülmesi, yönetilmesi ve koordinasyonuna ilişkin karar yürürlüğe konulmuştur. Bu karar ile ulusal siber güvenlikten Ulaştırma, Denizcilik ve Haberleşme Bakanlığı, Bilgi Teknolojileri ve İletişim Kurumu (BTK) ve bu karar ile oluşturulan Siber Güvenlik Kurulu sorumlu kılınmıştır. Siber Güvenlik Kurulu esasen siber güvenlikle ilgili olarak alınacak önlemleri belirlemek, hazırlanan strateji ve planları onaylamak ve bunların uygulanmasını ve koordinasyonunu sağlamakla, BTK ise onaylanan strateji ve planların uygulanması ile görevli kılınmıştır.

Ancak, ulusal güvenliği tehdit eden siber saldırılara karşı yürütülecek eylemler, bu eylemlerin hukuki altyapısının oluşturulması, bunun yanı sıra benzer bir ihtiyacın ortaya çıktığı interaktif bankacılık altyapısı, e-ticaret siteleri, kamu kurumlarının web siteleri ile İnternet servis sağlayıcılarının bilişim altyapılarının korunmasına yönelik strateji ve işbirliğinin genişletilmesi gibi konuları düzenlemesi gereken kapsamlı, doyurucu ve siber güvenlik ile kişi hak ve özgürlükleri arasında denge sağlayan bir Ulusal Siber Güvenlik Yasa Tasarısı halen söz konusu değildir.

Bu açıklamalardan sonra, Türkiye'nin 2013 yılından bu yana yayımladığı siber güvenlik stratejileri ve eylem planları ile, ulusal siber güvenliğin sağlanması kapsamında başta Türk Ceza Kanunu olmak üzere ulusal mevzuattaki düzenlemeler üzerinde durulacaktır.

B. 2013-2014 ve 2016-2019 Siber Güvenlik Stratejileri ve Eylem Planları

Siber Güvenlik Kurulu'nun oluşturulmasına ilişkin 2012/3842 sayılı Bakanlar Kurulu Kararı 20/10/2012 tarih ve 28447 sayılı Resmi Gazetede yayımlanarak yürürlüğe girmiş ve bu kararla birlikte 'Siber Güvenlik Kurulu' kurulmuştur. Kurul ilk toplantısını 20/12/2012 tarihinde yapmış ve "*Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı*"nın yürürlüğe konulması kararını almıştır. Bu Eylem Planında siber ortamda ortaya çıkan tehditlerin hızla belirlenmesi ve paylaşılması için ulusal düzeyde etkin bir şekilde

[159] GÜRPINAR, Bulut, *"Milli Güvenlik Kurulu ve Dış Politika",* Uluslararası İlişkiler, Cilt 10, Sayı 39 (Güz 2013), s. 78 vd.

çalışacak Siber Olaylara Müdahale Organizasyonu oluşturulması, Türkiye'yi etkileyebilecek tehditlere karşı 7/24 müdahale esasına göre çalışacak "Ulusal Siber Olaylara Müdahale Merkezi" (USOM) kurulması planlanmıştır.

Ulusal Siber Güvenlik Stratejisinin 4-c maddesi "Ulusal Siber Olaylara Müdahale Organizasyonu Oluşturulması" sürecini şu şekilde açıklamaktadır:

> "*Ülkemizi etkileyebilecek tehditlere karşı, 7/24 müdahale esasına göre çalışacak "Ulusal Siber Olaylara Müdahale Merkezi (USOM)" kurularak, USOM'un koordinasyonunda çalışacak sektörel "Siber Olaylara Müdahale Ekipleri (SOME)" oluşturulacaktır. Sektörel SOME'ler siber olaylara müdahalenin yanı sıra kendisine bağlı SOME'lere ve ilgili olduğu sektöre özel bilgilendirme ve bilinçlendirme faaliyetleri yürütecektir. Kurum ve kuruluşlar bünyesinde de sektörel SOME'lerin koordinasyonunda çalışacak SOME'ler kurulacaktır. USOM ve SOME'ler olaylara müdahale ederken suç soruşturmasına destek sağlayacak verilerin sağlanması için adli makam ve kolluk birimleri ile koordineli hareket edeceklerdir. USOM ulusal temas noktası olarak diğer ülkelerin eşdeğer makamlarıyla ve uluslararası kuruluşlarla yakın işbirliği yapacaktır."*

2012 yılındaki bu gelişmenin ardından, Bilgi Teknolojileri ve İletişim Kurulu tarafından 22/05/2013 tarih ve 2013/DK-TİB/278 karar numarası ile Ulusal Siber Olaylara Müdahale Merkezinin Kuruluş, Görev ve Yetkilerine Dair Usul ve Esaslar belirlenmiştir. Gerek Ulusal Güvenlik Stratejisi'nin 4/c maddesinde, gerekse BTK tarafından öngörülen usul ve esaslardan görüleceği üzere, siber olaylara müdahale organizasyonun USOM'dan sonraki bir diğer önemli ayağını Kurumsal ve Sektörel SOME'lerin kurulması oluşturmaktadır. Bu itibarla, Ulaştırma, Denizcilik ve Haberleşme Bakanlığı tarafından hazırlanan ve 11.11 2013 tarihli ve 28818 sayılı Resmi Gazete'de yayınlanan "*Siber Olaylara Müdahale Ekiplerinin Kuruluş, Görev ve Çalışmalarına Dair Usul ve Esaslar Hakkında Tebliğ*" ile Bakanlıklara ve düzenleyici ve denetleyici kurumlara SOME kurma görevi verilmiştir. Ancak istenirse diğer kamu kurum ve kuruluşlarının yanı sıra, Sektörel SOME'lerin bulunduğu sektörlerdeki özel kurumlar ve diğer kuruluşlar da kendi bünyelerinde kurumsal SOME kurabilecektir. Böylelikle, siber olaylara müdahale hizmetlerinin ulusal ve uluslararası düzeyde etkin ve verimli bir şekilde yürütülmesi amaçlanmıştır. USOM ve SOME'lerin yapıları ve işleyişleri hakkında detaylı açıklamalar aşağıdaki bölümde yapılacaktır.

Bu gelişmelerin akabinde, gelişen bilgi ve iletişim teknolojileri ve artan ihtiyaçlar doğrultusunda, 2016-2019 Eylem Planı hazırlanma gereksinimi duyulmuş ve Bakanlığın gözetim ve başkanlığında ulusal siber güvenlik stratejisinin belirlenmesi ve 2016-2019 Eylem Planının hazırlanması için yapılan bir dizi toplantıdan sonra "2016-2019 Ulusal Siber Güvenlik Stratejisi" ve "2016-2019 Ulusal Siber Güvenlik Eylem Planı" hazırlanmıştır. Söz konusu belgelerde, "*tehdit, risk, bilişim sistemleri, siber uzay, ulusal siber uzay, kamu bilişim sistemleri, siber güvenlik, siber saldırı, sınır güvenliği, siber olay, gizlilik, kritik hizmet, kritik ürün, kritik altyapılar,*" vb. konulara ilişkin önemli kavramlar tanımlanarak yeknesaklaştırılmaya, bu çerçevede, uluslararası siber güvenlik belgeleriyle de bir kavram birliği yaratılmaya çalışılmıştır. Bu stratejinin oluşturulmasındaki nedenin, ulusal siber güvenliğin sağlanması amacıyla etkin ve sürdürülebilir politikaları belirlemek, koordinasyonu ve bunların uygulanmasını sağlamak olduğunu söylemek mümkündür[160].

Bu bağlamda, Bakanlığın bu şekilde belirli periyodlarda strateji ve eylem planı hazırlama amacını, şu üç başlıkta toplayabiliriz:

- Ulusal siber uzayın tamamını kapsamak şartıyla, bilgi teknolojileri üzerinden sağlanan her türlü hizmet, işlem ve veri ile bunların sunumunda kullanılan sistemlerin güvenliğinin, gizliliğinin ve mahremiyetinin sağlanması (*siber uzay, bu belgelerde 'tüm dünyaya ve uzaya yayılmış durumda bulunan bilişim sistemlerinden ve bunları birbirine bağlayan ağlardan oluşan veya bağımsız bilgi sistemlerinden oluşan sayısal ortam; ulusal siber uzay ise, kamu bilişim sistemleri ile gerçek ve tüzel kişilerce kullanılan/işletilen bilişim sistemlerinden oluşan ortam olarak tanımlanmıştır*),
- Siber güvenlik olaylarının etkilerinin en düşük düzeyde kalması ve olayların ardından sistemlerin en kısa sürede normal işleyişine dönmesine yönelik stratejik siber güvenlik eylemlerinin belirlenmesi, bu minvalde adli makam ve kolluk kuvvetlerinin daha etkin soruşturma yapabilmelerinin sağlanması,
- Siber güvenliğin, gizliliğin ve mahremiyetin sağlanmasında kritik teknolojilerin ve ürünlerin ülkemizde üretilmesi, üretilemiyorsa dışarıdan alınan teknoloji ve ürünlerin salt bu maksatla ve güvenle kullanılmasını sağlayacak önlemlerin alınması.

[160] http://www.udhb.gov.tr/doc/siberg/2016-2019guvenlik.pdf (e.t. 01.03.2018).

Bu amaçlar doğrultusunda, Bakanlığın 2016-2019 Stratejisi ve Eylem Planında bir dizi ilkeye yer verilmiştir. Güvenli yazılım geliştirilmesinden IPv6 teknolojilerinin yaygınlaştırılmasına[161], siber güvenlikte AR-GE faaliyetlerinin arttırılarak dışa bağımlılığı azaltmaktan bu alanda yetkin personel yetiştirilmesine kadar birçok önemli husus sıralanmış olup, bu ilkelerin en önemlilerinden biri, yukarıda bahsettiğimiz ve 2013-2014 Eylem Planında da önemi vurgulanan USOM ve SOME'lerin etkinliğidir. 2016-2019 Eylem Planına göre, "*Kurumsal ve sektörel SOME'lerin etkinliğinin arttırılması için mevzuat desteğinin sağlanması, mali düzenlemelerin yapılması, yetkin personelin ihtiyacının karşılanması, bilişim altyapısının sağlanması ve ulusal siber olaylara müdahale organizasyonu kapsamında bilgi paylaşımının geliştirilmesi*", Eylem Planının en önemli maddelerinden biridir.

1. USOM'un Kuruluşu ve Yapısı

Ulusal Siber Olaylara Müdahale Merkezi'nin (USOM) çalışma usul ve esasları, 22.05.2013 tarihli ve 2013/DK-TİB/278 sayılı BTK Kararı ile belirlenmiştir. USOM faaliyetlerinde göz önünde bulundurulacak ilkeler BTK'nın ilgili kararının 5. maddesinde öngörülmüş olup, bu ilkeler şunlardır:

a) Hukukun üstünlüğü,temel insan hak ve hürriyetleri ile mahremiyetinin korunması ilkeleri temel esas kabul edilir.

b) Siber ortamda şeffaflık,hesap verilebilirlik,etik değerler ve ifade özgürlüğü desteklenir.

c) Siber güvenlik olaylarına müdahale kapsamında yürütülen iş ve işlemlerde gizlilik esastır.

d) Siber güvenliğin sağlanmasında birey,kurum,toplum ve devletin tüm hukukuki ve sosyal sorumluluklarını yerine getirmesi esas kabul edilir.

e) Siber güvenlik olayına maruz kalan birey ya da kurum olaya müdahale konusunda öncelikli olrak sorumludur.

f) Siber güvenlik olaylarında ilgili kurumlar ile işbirliği esastır.

---

[161] IPv6 hakkında detaylı bilgi için bkz. MIDOĞLU, Çise / ÖZOCAK, Gürkan, "*IPv6, Güvenlik Açıkları ve Hukuki Durum*", Bilişim 2013 – 30. Ulusal Bilişim Kurultayı Bildiriler Kitabı, Ankara, 2013, ss. - 7.

Aynı kararın 6. maddesinde ise, USOM'un kuruluşu ve yapısı düzenlenmiştir. Buna göre;

(1) USOM, Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planının 4üncü maddesine göre kurulur ve Başkanlık bünyesinde faaliyet gösterir.

(2) Kurum ve Başkanlık birimleri USOM faaliyetleri ile ilgili kendi görev alanlarına giren konularda gerekli desteği sağlar.

BTK kararıyla öngörülen yapıda, USOM'un, siber olaylara müdahalede ulusal ve uluslararası koordinasyonu yürüteceği; Siber tehditlerle ilgili olarak alarm, uyarı, duyuru faaliyetlerini ve yaşanabilecek olayların etkilerini azaltmaya ve ortadan kaldırmaya yönelik koruyucu tedbirlerin alınması hususunda koordinasyon faaliyetlerini yürüteceği; siber güvenlik olaylarına maruz kalan kritik altyapılara yönelik koruyucu tedbirlerin alınmasında koordinasyon sağlayacağı; çalışma esnasında konusu suç teşkil eden vakalarla karşılaşırsa adli makamlar ve kollukla koordinasyon sağlayacağı; sektörel ve kurumsal SOME'ler ile bilgi paylaşımı yapıp acil alınması gereken tedbirleri bunlarla kurduğu güvenli iletişim kanalı üzerinden çevrimiçi paylaşacağı; zararlı yazılımları analiz ederek, gerekmesi durumunda TÜBİTAK veya diğer kuruluşlara analiz etmek üzere göndereceği; siber güvenlik olaylarının tespit edilmesi halinde ilgililere bilgi vereceği, ilgililer tarafından talep edilmesi halinde uzaktan müdahale desteği sağlayacağı, yine talep edilmesi halinde kritik alt yapılarda ortaya çıkan siber güvenlik zafiyetlerinin giderilmesi için yerinde müdahale desteği sağlayacağı ve 7/24 esasına uygun çalışacağı gibi görev ve yetkilerinin olacağı düzenlenmiştir.

Çalışmamızın kapsamı bakımından, özellikle USOM'ların SOME'lerle işbirliği içinde hareket etmesi hususunun üzerinde durmakta fayda olduğu kanaatindeyiz.

2. SOME'lerin Yapısı, Görev ve Sorumlulukları

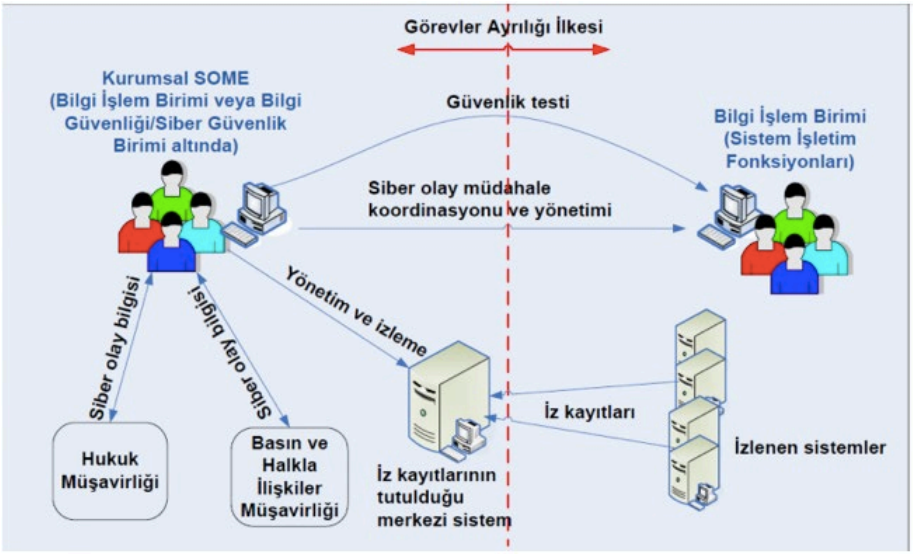
Yukarıda kuruluş mantığını ve organizasyonunu kısaca özetlediğimiz SOME'ler (Siber Olaylara Müdahale Ekipleri) "*Kurumsal*" ve "*Sektörel*" olmak üzere iki şekilde organize olmaktadır.

a. Kurumsal SOME'ler

Kurumsal SOME'ler, Bakanlıkların bünyesinde, hizmet gereklerine göre, Bakanlık birimlerine bağlı, ilgili ve ilişkili kurumları kapsayacak şekilde kurulur. Ancak Bakanlık koordinesinde Bakanlık birimleri, altyapılarının önem ve büyüklüğüne göre kendi bünyelerinde kurumsal bir SOME kurabilirler. Diğer tüm kamu kurum ve kuruluşları da kendi bünyelerinde kurumsal SOME kurabilirler. Tüm kurumsal SOME'lerin kuruluşunun eşgüdümü Ulaştırma, Denizclik ve Haberleşme Bakanlığı tarafından yürütülür.

Kurumsal SOME'ler, özetle, kurumlarına doğrudan ya da dolaylı olarak yapılan veya yapılması muhtemel siber saldırılara karşı gerekli önlemleri alma veya aldırma, bu tür olaylara karşı müdahale edebilecek mekanizmayı ve olay kayıt sistemlerini kurma veya kurdurma ve kurumlarının bilgi güvenliğini sağlamaya yönelik çalışmaları yapmak veya yaptırmakla yükümlüdürler. Bu kapsamda, kurumsal SOME'ler, siber olayların önlenmesi veya zararlarının azaltılmasına yönelik olarak, kurumlarının bilişim sistemlerinin kurulması, işletilmesi veya geliştirilmesi ile ilgili çalışmalarda teknik ve idari tedbirler konusunda öneri sunar; siber olayların önlenmesi veya zararlarının azaltılmasına yönelik faaliyetlerini varsa birlikte çalıştığı sektörel SOME ile eşgüdüm içerisinde yürütür ve durumdan gecikmeksizin USOM'u haberdar eder; bir siber olayla karşılaştıklarında, USOM ve birlikte çalıştığı sektörel SOME'ye bilgi vererek olayı kendi imkan dahilinde bertaraf etmeye çalışır; bu mümkün değilse sektörel SOME ve/veya USOM'dan yardım talep edebilir; siber olaya müdahale ederken suç işlendiği izlenimi veren bir durumla karşılaştıklarında gecikmeksizin durumu kanunen yetkili makamlara bildirir; kurumlarına yapılan siber olayları raporlar ve gecikmeksizin USOM ve birlikte çalıştığı sektörel SOME'ye bildirir; USOM ve/veya birlikte çalıştığı sektörel SOME tarafından iletilen siber olaylara ilişkin alarm, uyarı ve duyuruları dikkate alarak kurumlarında gerekli tedbirleri alır ve USOM gibi 7/24 çalıştıklarından 7/24 erişilebilir olan iletişim bilgilerini belirleyerek birlikte çalıştığı sektörel SOME'lere ve USOM'a bildirirler[162].

[162] http://www.udhb.gov.tr/doc/siberg/Kurumsal_SOME_Reh_V1.pdf (e.t. 01.03.2018).



Kurumsal SOME'nin kurum içi paydaşları ve temel fonksiyonlarını gösterir şema[163]

b. Sektörel SOME'ler

Sektörel SOME'ler ise düzenleyici ve denetleyici kurumların bünyesinde kendi sektörlerinde faaliyet gösteren kurum, kuruluş ve işletmeleri kapsayacak şekilde kurulurlar. İhtiyaç duyulması halinde, düzenleyici ve denetleyici kurumların yetki alanı dışında kalan diğer sektörlerde ilgili olduğu Bakanlık bünyesinde sektörel SOME kurulabilir. Kritik sektörlerde, sektörel SOME kurulması zorunludur. Kritik sektörlerin listesi Kurul tarafından belirlenir, ilgililere duyurulur ve güncellenir. Düzenleyici ve denetleyici kurumlardaki sektörel SOME'lerin eşgüdümü ise BTK tarafından yürütülür.

Sektörel SOME'ler, siber olayların önlenmesi veya zararlarının azaltılmasına yönelik faaliyetlerini USOM'la koordineli şekilde yürütürler. Bunun yanı sıra, sektörel SOME'ler, birlikte çalıştıkları SOME'lerde yaşanan siber olayları gecikmeksizin USOM'a bildirir; siber olaylara ilişkin USOM tarafından iletilen alarm, uyarı ve duyuruları dikkate alarak birlikte çalıştıkları SOME'lerde gerekli tedbirlerin alınmasına yönelik çalışmaları yürütür; birlikte çalıştıkları SOME'lerin yapılanması konusunda düzenleyici

[163] http://blog.normaturk.com/some-nedir/ (e.t. 01.03.2018).

faaliyetleri yürütür; ilgili oldukları sektörde, bilgilendirme, bilinçlendirme ve eğitim faaliyetleri ile siber güvenlikle ilgili kabiliyetlerinin geliştirilmesi ve önlemlerin alınması konusunda gerekli düzenleyici faaliyetleri yürütür; bunlar da 7/24 esasına uygun çalışmak zorunda olduklarından 7/24 erişilebilir olan iletişim bilgilerini belirleyerek birlikte çalıştıkları SOME'lere ve USOM'a bildirir; birlikte çalıştıkları SOME'lerde yaşanan siber olaylarda imkânları ölçüsünde gerekli desteği sağlar ve imkânlarının yetersiz olması durumunda USOM'dan destek alır; siber olaya müdahale ederken suç işlendiği izlenimi veren bir durumla karşılaştıklarında gecikmeksizin durumu kanunen yetkili makamlara bildirirler[164].

c. Siber olaylara müdahale bağlamında SOME'lerin USOM'la ilişkisi

SOME'lerin USOM ile ilişkilerini, varsa birlikte çalıştıkları sektörel SOME'ler üzerinden yürütmesi esastır. Birlikte çalıştıkları bir sektörel SOME olmayan kurumsal SOME'ler, faaliyetlerini doğrudan USOM ile koordineli biçimde yürütürler. Siber olaylar ile ilgili olarak diğer ülkelerin eşdeğer makamları ve uluslararası kuruluşlarla işbirliği USOM tarafından yerine getirilir. USOM gerekli gördüğü durumlarda kurumsal SOME'ler ve sektörel SOME'ler ile doğrudan çalışma yürütebilir. Kurumsal/Sektörel SOME'ler siber olayların tespiti, önlenmesi, zararlarının en aza indirilmesi gibi konularda USOM tarafından geliştirilen veya yürütülen projelerin gerçekleştirilmesinde USOM ile işbirliği içerisinde hareket etmek durumundadırlar.

IV. SİBER SUÇLULUKLA MÜCADELEDE ULUSAL MEVZUAT

A. Genel Olarak

Ulusal siber güvenliğin sağlanmasında, gerekli organizasyonun oluşturulması ve birimlerin kurulması kadar, suç ve suçlulukla etkin mücadele yapılabilmesi için ulusal mevzuattaki düzenlemeler de büyük önem taşımaktadır. Zira, bilişim teknolojisindeki hızlı gelişim klasik hukuki sorunlara ek olarak, daha önce hukuk düzeninin karşılaşmadığı yeni sorunların ortaya çıkmasına da sebep olabilmektedir. Özel hukuk alanında herhangi bir alanın düzenlenememesi, çıkabilecek ihtilafların çözümsüz

[164] www.udhb.gov.tr/doc/siberg/Sektorel_SOME_Reh.docx (e.t. 01.03.2018).

kalmasına yol açmayabilir. Çünkü özel hukukta hem kıyas mümkündür, böylece benzer yasal düzenlemeler baz alınarak mevcut ihtilaflara bir çözüm bulunabilir, hem de hakimin hukuk yaratma yetkisi bulunmaktadır.

Ancak ceza hukukunda kıyas söz konusu değildir. Ceza hukukunda kıyas, bir eylemi suç sayan bir yasa hükmünün o eyleme benzeyen ancak yasada açıkça suç sayılmamış olan bir başka eyleme uygulanması anlamına gelmektedir. Ne var ki, suç ve cezada kanunilik ilkesi gereği, bir eylemin suç sayılıp ceza yaptırımına tabi kılınabilmesi ancak o eylemin ceza kanunlarında suç olarak düzenlenmesi halinde söz konusu olabileceğinden, bu durum ceza hukukunda kıyasın yasaklanması sonucunu doğurmaktadır[165]. Nitekim, Türk Ceza Kanunu'nda da kıyas açıkça yasaklanmıştır. TCK'nun 2/III. maddesine göre, "*Kanunların suç ve ceza içeren hükümlerinin uygulanmasında kıyas yapılamaz. Suç ve ceza içeren hükümler, kıyasa yol açacak biçimde geniş yorumlanamaz.*"

Bu itibarla, suç ve cezada kanunilik ilkesi ve bu ilkenin bir sonucu olarak ortaya çıkan *kıyas yasağı* nedeniyle, bir fiilin kanunda açık şekilde suç sayılmamış olması, yeni ortaya çıkan fiil tiplerinin cezasız kalması sonucunu doğuracaktır. Bu nedenle, siber güvenlik söz konusu olduğunda, kanun koyucunun ceza hukuku alanında hızlı hareket etmesi, yeni ortaya çıkan suç tiplerini derhal değerlendirerek kanunda tanımlaması ve ceza yaptırımına tabi tutması gerekmektedir. Ancak bu noktada şunu da vurgulamamız gerekir ki; siber suçlulukla mücadele yalnızca yasama faaliyeti ile sağlanamaz. Zira siber dünyada "ulus" kavramı gün geçtikçe daha da ortadan kalkmakta ve bu kavramın sınırları belirsizleşmekte, siber saldırılar uluslararası nitelik kazandıkça, bu suçlulukla mücadelenin de benzer bir niteliğe kavuşma ihtiyacı artmaktadır. Dolayısıyla, ulusal mevzuatta suç tiplerinin ve usul hükümlerinin şüpheye yer vermeyecek şekilde açık, dinamik ve etkin bir suçlulukla mücadelede ağı yaratacak nitelikte düzenlenmesi gerekmektedir.

Bu kısa açıklamadan sonra, ulusal siber güvenlikle ilgili en önemli iki aşamayı incelememiz gerekmektedir. Bunlardan ilki, siber suç tiplerinin doğru ve herhangi bir boşluk bırakmayacak şekilde kanunlarda düzenlenmesi; ikincisi ise, suç ve suçluların tespitinde ve delil toplamada kullanılacak usullerin kanunda düzenlenmesi ve doğru bir biçimde uygulanmasıdır.

---

[165] CENTEL, Nur / ZAFER, Hamide / ÇAKMUT, Özlem, Türk Ceza Hukukuna Giriş, Beta, İstanbul, 2006, s. 94.

B. Bilişim Suçları

Ulusal siber güvenliğin sağlanması için, siber saldırı niteliğindeki eylemlerin eksiksiz bir biçimde kanunda suç olarak öngörülebilmesi gerekmektedir. Bu nedenle, siber suçların kanunda düzenlenmesi gerekliliği bağlamında Türk Ceza Kanunu'ndaki düzenlemelere ve bilişim suçlarının yapısına bakmak önem arzetmekte olup, TCK'daki bilişim suçları rejiminin nasıl düzenlendiğine geçmeden önce, "*bilişim suçları*" kavramından bahsetmekte fayda vardır.

Doktrinde kimi zaman birbirinin yerine de sıkça kullanılan *"bilişim suçları"* veya *"bilgisayar suçları"* ile ilgili ortak bir tanımlama yapılamamış, birçok yazar bu suçlara kendince bir sınır çizmiştir[166]. Çalışmamızın kapsamı bakımından bu tartışmaların tamamını buraya alamamakla birlikte[167], son tahlilde bilişim suçları, verilerin bilişim temelli olarak ve otomatik bir biçimde işlenmesi, saklanması, tasnif edilmesi, terkibi ve iletilmesi ile ilgili ve bilişim alanı içerisinde işlenen, bir bilgisayara veya bilgisayar ağına yahut bir bilişim sisteminin bir kısmına ya da tamamına yönelik olarak veya onları araç olarak kullanarak icra edilen haksız eylemler olarak tanımlanabilir[168].

Bugün, bilişim suçlarını "*bilişim sistemleri aracılığıyla işlenen suçlar*" ve "*bilişim alanındaki suçlar*" olarak ikiye ayırmak mümkündür. İlk gruptaki suçlar "*geleneksel*" ya da "*klasik*" suçlar olarak tanımlanan, ancak bir bilişim sistemi aracılığıyla işlenen suçlardır. Örneğin; e-posta yoluyla işlenen tehdit veya hakaret suçu, yine bilgisayar veya İnternet siteleri üzerinden işlenen cinsel taciz, halkı kin ve düşmanlığa tahrik etme, müstehcenlik (çocuk pornografisi) gibi suçlar bu grupta sayılabilir. Teknolojik imkanların müthiş bir hızla artması ve gelişmesi ile birlikte, artık insan öldürme suçuna kadar her suç bilişim yoluyla işlenebileceği için, bu gruptaki suçların sınırını belirlemek mümkün değildir[169].

---

166 BOZDOĞAN AKBULUT, Berrin, "*Bilişim Suçları*", Selçuk Üniversitesi Hukuk Fakültesi Dergisi Milenyum Armağanı, Sayı 1-2, C. 8, Konya, 2000, s. 550; KETİZMEN, Muammer, Türk Ceza Hukukunda Bilişim Suçları, Ankara, 2008, s. 32 vd.; DÜLGER, Murat Volkan, Bilişim Suçları ve İnternet İletişim Hukuku, Ankara, 2014, s. 219-310.

167 Tartışmalar için Bkz. KETİZMEN, s. 32-54; KURT, Levent; Tüm Yönleriyle Bilişim Suçları ve Türk Ceza Kanunundaki Uygulaması, Ankara, 2005, s. 49-53; SINAR, Hasan, İnternet ve Ceza Hukuku, İstanbul, 2001, s. 69- 78.

168 KURT, s. 53; ÖZEN/BAŞTÜRK, ss. 90- 91.

169 ÖZDİLEK, s. 112.

İkinci gruptaki suçlar ise, kanunda sınırlı sayıda düzenlenen ve ilk gruptaki suçlara göre teknik özellikler arzeden suçlardır. 5237 sy. TCK'da da bu suçlar, 243 ilâ 246. maddeler arasında, "Bilişim Alanında Suçlar" başlığıyla düzenlenmiştir[170].

Bu suçlar, Mülga 765 sayılı TCK'nda "mal aleyhine cürümler" olarak değerlendirilmiş ve ayrı bir bapta düzenlenmiş olup[171], 5237 sayılı TCK ile "Bilişim Alanında Suçlar" başlığıyla, Kanunun Üçüncü Kısmı olan "Topluma Karşı Suçlar" arasında düzenlenmiştir. 765 sy. Mülga TCK'nda, özel kısmın sistematiği olan hukuki konu esasından vazgeçilerek bu suçların ayrı bir bab altında düzenlenmesi, söz konusu düzenlemeyi yapan 1991 tarihli 3765 sayılı değişiklik kanunun gerekçesinde şu şekilde açıklanmıştır: "*Yabancı kanunlardan bir kısmı, bilişim alanındaki suçları ayrı bir bölümde toplayarak ilgili suç bölümlerine yerleştirmektedirler. Kanunda ise bu suçların uygulamada kolaylık sağlamak üzere ayrı bir bölümde düzenlenmesi tercih edilmiştir*."[172]

5237 sayılı TCK'nda ise, Alman ve İtalyan Ceza Kanunlarında hakim olan anlayış kabul edilerek, "Bilişim Alanında Suçlar", "Topluma Karşı Suçlar" ana başlığı altında, üçüncü kısmın onuncu bölümünde düzenlenmiş ve yapılan tasnifte, Ceza Kanununda esas alınan hukuki konu ölçütü nazara alınmıştır[173].

İtalyan Ceza Kanunu'na bakıldığında, bilişim alanında suçların hukuki konularına göre ayrıştırıldığını ve farklı başlıklarda düzenlendiği görülmektedir. Örneğin, TCK m. 243'te düzenlenen "yetkisiz erişim" suçu,

---

[170] Bunlara, kanun tarafından sınırlı sayıda öngörüldükleri için "*dar anlamda bilişim suçları*" da denilmektedir. Bkz. ÖZEN/BAŞTÜRK, s. 113.

[171] ÖZEN/BAŞTÜRK, s. 111.
Ayrıca düzenleme ve nedenleri hakkında Bkz. TAŞDEMİR, Kubilay/ÖZKEPİR, Ramazan, Mala Karşı Suçlar, Ankara, 1993, s. 507.
Değişikliğin yapıldığı dönemde, bilgisayarın giderek gündelik yaşamın bir parçası durumuna geldiği ve bu nedenle yeni suç türleri ortaya çıktığı, özellikle özel kuruluşların bilgisayar sistemlerine girilerek bu kuruluşların ticari bilgilerinin elde edilmesi ve kullanılması gibi durumlar söz konusu olduğundan, TCK'nda bilişim suçları konusunda yasal bir düzenleme yapılması gerekliliğinin ortaya çıktığı söylenmiştir. Bkz. EREM, Faruk, "*Bilgisayar Suçları ve TCY*", Yargıtay Dergisi, C. 17, Sayı 4, Ekim 1991, ss. 436- 437.

[172] TBMM Tutanak Dergisi, 6.6.1991, Dönem 18, Yıl 4, C. 61, Birleşim 119-131, s. 17, Sayfa Sayısı 513, Aktaran YAZICIOĞLU, Yılmaz, Kriminolojik, Sosyolojik ve Hukuki Boyutları İle Bilgisayar Suçları, İstanbul, 1997, s. 212.

[173] KETİZMEN, s. 60.

İCK m. 615 ter'de "*Özel Hayata Hukuka Aykırı Müdahale*" (*Interferenze illecite nella vita private*) hükmünden hemen sonra düzenlenmekte ve başkasının "*enformatik veya telematik*" sistemine giren kimsenin üç yıla kadar hapis cezasıyla cezalandırılacağı öngörmektedir[174]. Buna karşın, çalışmamızın da konusunu oluşturan "*sisteme veya veriye müdahale*" fiili, Kanunun malvarlığı aleyhine suçlar kısmında, "*Mala Zarar Verme*" (*Danneggiamento*) suçundan hemen sonra gelmek üzere, 635 bis maddesinde düzenlenmektedir. Bu hükme göre ise, enformatik ve telematik sistemlerin, programların, verilere zarar verilmesi, bozulması, tamamen ya da kısmen kullanılamaz hale gelmesi halinde fail cezalandırılmaktadır[175].

Alman Ceza Kanunu'nda da mala zarar verme suçunda eşyaya maddi etkide bulunulmasının yeterli olduğu, örneğin işlem kabiliyetinin bozulmasının bu suçun varlığına yeteceğini, bunun dışında fiziki yapısının bozulmasının gerekmediği anlayışı kabul edilerek, sisteme ve veriye müdahale suçu malvarlığına karşı suçlardan sayılmaktadır[176].

Bu anlayışla yapılan düzenleme sonucu, "Bilişim Alanında Suçlar" 5237 sy. Kanun'un 243, 244, 245 ve 245/A maddelerinde düzenlenmiştir. Ne var ki, hukuki konu ölçütüne göre tasnifte Alman ve İtalyan kanunlarını nazara alan kanun koyucu, bu suçları "Topluma Karşı Suçlar" arasında düzenlemiştir[177].

---

174 "*Chiunque abusivamente si introduce in un sistema informatico o telematico protetto da misure di sicurezza ovvero vi si mantiene contro la volontà espressa o tacita di chi ha il diritto di escluderlo, è punito con la reclusione fino a tre anni."*
İCK'nda bilgisayar veya bilişim yerine, bilişim alanındaki suçlarla ilgili "enformatik veya telematik" (*informatico o telematico*) terimleri kullanılmaktadır. "*Enformatik terimi, enformasyon kelimesinin otomatik kelimesiyle birleşmesinden ortaya çıkmaktadır. Bu haliyle, elektronik hesaplama makineleri yardımıyla enformasyonun otomatik olarak temsil edilmesi, iletilmesi, dönüştürülmesi ve hesaplanmasını ifade etmektedir. Enformatik araçlarının iletişim kurarak birbirine bağlanması ise, telematik terimini ortaya çıkarmaktadır. Her iki terimin bir araya gelmesi ise 'telekomünikasyon ve enformatik' terimini ortaya çıkarmaktadır*" Bkz. RESTA, Salvatore, Computer Crimes Tra Informatica e Telematica, Cedam, 2000, s. 7, Aktaran KETİZMEN, s. 116.

175 "*Chiunque distrugge, deteriora o rende, in tutto o in parte, inservibili sistemi informatici o telematici altrui, ovvero programmi, informazioni o dati altrui, è punito, salvo che il fatto costituisca più grave reato, con la reclusione da sei mesi a tre anni."*

176 JESCHECK, Hans-Heinrich; Alman Ceza Hukukuna Giriş, Çev. Feridun Yenisey, İstanbul, 2007, ss. 108- 109.

177 Kanun koyucunun bu tercihinin değerlendirmesi ve eleştirisi hakkında bkz. KETİZMEN, s. 58 vd.

Ceza hukukunda "*tipiklik ilkesi*" gereği[178], bir siber saldırının suç olarak soruşturulup failinin cezalandırılabilmesi için, o fiil mutlaka ceza normu öngören bir kanunda suç olarak öngörülmüş olmalıdır. Bu nedenle, ulusal siber güvenlik organizasyonunun devreye girebilmesi için, öncelikle müdahaleye konu fiilin bir suça vücut vermesi zorunludur. Bu bölümde, siber güvenlik organizasyonu bakımından özellikle önem arzeden, TCK'nda "bilişim alanında suçlar" başlığı altında düzenlenmiş suçlara değineceğiz.

1. Bilişim Sistemine Girme (Yetkisiz Erişim) Suçu (TCK m. 243)

TCK'nun 243. maddesinde "Yetkisiz Erişim" olarak da adlandırılan[179], "Bilişim Sistemine Girme" suçu düzenlenmiştir. Buna göre;

(1) Bir bilişim sisteminin bütününe veya bir kısmına, hukuka aykırı olarak giren veya orada kalmaya devam eden kimseye bir yıla kadar hapis veya adlî para cezası verilir.

(2) Yukarıdaki fıkrada tanımlanan fiillerin bedeli karşılığı yararlanılabilen sistemler hakkında işlenmesi hâlinde, verilecek ceza yarı oranına kadar indirilir.

(3) Bu fiil nedeniyle sistemin içerdiği veriler yok olur veya değişirse, altı aydan iki yıla kadar hapis cezasına hükmolunur.

Bu maddede yer alan suç ile, Avrupa Siber Suç Sözleşmesi'nin 2. maddesinde öngörülen "hukuka aykırı erişim" düzenlemesi arasında paralellik sağlanmış ve yeknesak bir düzenleme getirilmiştir. Sözleşmenin 2. maddesi düzenlemesi "*her taraf, iç hukukuna uygun olarak, bir bilişim sisteminin tamamına veya bir kısmına kasten ve haksız olarak erişimi suç haline getirmek için gerekli görülen yasal tedbirleri almayı kabul eder*" şeklinde iken, TCK m. 243'te de benzer bir düzenlemeye gidilmiştir[180]. Esasen, maddenin ilk halinde sisteme hukuka aykırı olarak girmek "ve" orada kalmaya devam etmek şeklinde bir düzenleme yapılmış, böylece yalnızca sisteme girilmesinin yeterli olmayıp sistemde bir süre kalınması da suçun unsuru olarak sayılmıştı ve madde bu haliyle Siber Suç Sözleşmesi'nin 2.

[178] KEYMAN, Selahattin, "*Tipiklik ve Ceza Hukuku",* AÜHFD, C. 37, S.1-4, 1980, s. 72; TOROSLU, Nevzat, Ceza Hukuku Genel Kısım, Ankara, 2012, s. 37 vd.
[179] Bu adlandırma için bkz. KETİZMEN, s. 79.
[180] DÜLGER, s. 320.

maddesinden ayrılmaktaydı. Ancak 24.3.2016 tarihli ve 6698 sy. Kanun'un 30. maddesi ile yapılan değişiklik neticesinde, maddedeki "*ve*" ibaresi isabetli bir şekilde "*veya*" olarak değiştirilmiş, böylece madde hükmü Siber Suç Sözleşmesi'ne de uygun hale getirilmiştir[181].

Bu suça göre, kendisinden başkasına ait bir bilişim sistemine, o kişinin rızası veya hukuka uygun bir yetkisi olmaksızın giriş yapan yahut yetkiyle girmesine rağmen burada hukuka aykırı olarak kalmaya devam eden kişi, TCK m. 243 uyarınca sorumlu olacaktır. Bu suçun muhakkak şifre kırılması, sistem açığından yararlanılması vb. yollarla, yani bilgisayar korsanlığıyla işlenmesine gerek olmayıp, yetki olmaksızın yapılan her türlü erişim suç sayılmaktadır. Zira, bu suçta failin amacı, yetkisinin bulunmadığı bir sistem üzerinde hukuka aykırı olarak kullanım sağlamaktır. Dolayısıyla, teknik olarak oturum açma (*log on*) yetkisi olarak da adlandırılan ve kimlerin sistemde oturum açabileceğini belirleyen yetkinin ihlal edilerek sistemde oturum açmanın bu suçu oluşturacağı açıktır. Bu madde bağlamında, sisteme hukuka aykırı olarak elde edilen erişim kodlarından yararlanmak suretiyle giriş yapılması ile sistemdeki açıklardan faydalanarak veya sistemde açıklar yaratarak girmek arasında ceza sorumluluğu bakımından herhangi bir fark yoktur. Aynı şekilde, maddenin düzenlemesi kapsamında, sistemin tamamına yahut bir kısmına girilmesi arasında da hiçbir fark bulunmamaktadır[182].

Ulusal siber güvenlikle ilgili en sık görülen eylemlerden birisi bilişim sistemlerine yetkisiz erişim olduğundan, bu suça konu eylemlerin herhangi bir boşluk yaratmayacak biçimde ulusal kanunlarda düzenlenmesi ve uluslararası siber güvenlikle mücadelede işbirliği için de bu hükümlerin mümkün olduğunda yeknesaklaştırılması elzemdir.

Yukarıda zikrettiğimiz 24.3.2016 tarihli ve 6698 sy. Kanun'un 30. maddesi ile yalnızca 1. fıkradaki "ve" ibaresi düzeltilmemiş, ayrıca 243. maddeye eklenen 4. fıkra ile, yeni bir bilişim suçu da öngörülmüştür. Bu suçun ayrı bir başlık altında incelenmesi gerektiği kanaatindeyiz.

---

[181] Maddenin eski haline ilişkin eleştiriler için bkz. DÜLGER, s. 321-323, KARAGÜLMEZ, Ali, Bilişim Suçları ve Soruşturma-Kovuşturma Evreleri, 3. Bası, Ankara,2011, s. 182.

[182] KETİZMEN, s. 103.

2. Sisteme Girmeksizin Verileri İzleme Suçu (TCK m. 243/4)

24.3.2016 tarihli ve 6698 sy. Kanun'un 30. maddesi ile, TCK'nun 243. maddesine yeni bir fıkra eklenmiş ve bu düzenleme ile, yeni bir bilişim suçu öngörülmüştür. Her ne kadar bu suç 'Bilişim Sistemine Girme' suçunu düzenleyen 243. maddenin altında düzenlenmekteyse de, bu hüküm ile esasen bilişim sistemine girmeksizin veri nakillerini izleme eylemi suç olarak düzenlenmiştir. Bu itibarla, kanımızca bu suça "Sisteme Girmeksizin Verileri İzleme Suçu" denilmesi yerinde olacaktır.

İlgili suç TCK m. 243/4'te şu şekilde düzenlenmiştir:

(4) Bir bilişim sisteminin kendi içinde veya bilişim sistemleri arasında gerçekleşen veri nakillerini, sisteme girmeksizin teknik araçlarla hukuka aykırı olarak izleyen kişi, bir yıldan üç yıla kadar hapis cezası ile cezalandırılır.

Bu düzenleme ile kanun koyucu, uygulamada sık rastlanılan ancak kanunda düzenlenmediğinden bugüne dek cezalandırma olanağı pek bulunmayan bir eylemi ceza sorumluluğu kapsamına almıştır. Özellikle uygulamada çok yaygın olan, *sniffing* gibi yöntemlerin, bu düzenleme ile cezalandırılması öngörülmüştür. Ulusal siber güvenliği de ciddi biçimde tehdit eden *sniffing* yöntemiyle saldırgan, en basit tabiriyle, iki veya daha fazla network arasında gidip gelen verileri izlemekte, bu verileri süzmekte ve kaydetmektedir. Bu hacking yöntemi, çoğu kez şifreleri yakalamak için kullanılmaktadır ve saldırgan, sisteme girmeksizin iki nokta arasındaki veri nakillerini izlemektedir.

Yapılan düzenleme ile ağ trafiğinin hukuka aykırı izlenmesi suç kapsamında sayılmıştır. Yukarıda basitçe ifade ettiğimiz gibi, bir ağ trafiğini hukuka aykırı olarak, teknik araçlarla izleyen kişi, bu ağ üzerinden mevcut veri paketlerine ulaşma imkanına sahip olur ve buradaki şifreleri kaydetme, sosyal medya ve e-posta yazışmalarını elde etme gibi şansını yakalar. Şunu vurgulamamızda fayda var ki, ağ trafiğini izleyerek buradaki verileri kaydetme eylemi, ayrıca kaydedilen verilerin niteliğine göre haberleşmenin gizliliğini ihlal, kişisel verilerin hukuka aykırı kaydedilmesi, özel hayatın gizliliğini ihlal gibi suçlara vücut verebilir ve fail bu suçları işlemişse, bu suçlar uyarınca ceza sorumluluğu ortaya çıkar. Ne var ki, bu düzenlemeden önce bir suç söz konusu olması için muhakkak sisteme giriş yapılması veya

sisteme giriş yapılmamışsa buradaki veriler üzerinde bir eylemede bulunulması zorunlu iken, TCK m. 243/4 ile birlikte, bir ağ trafiğinin hukuka aykırı olarak izlenmesi başlı başına bir suç olarak düzenlenmiş ve veriler yahut sistem üzerinde başka bir müdahalede bulunulmamış olsa dahi, ağ trafiğinin izlenmesinden ibaret eylem ceza yaptırımına konu edilmiştir.

3. Bilişim Sistemine ve Verilere Müdahale Suçu (TCK m. 244)

TCK m. 244, birinci ve ikinci fıkrasında, şu düzenlemeyi yapmaktadır:

(1) *Bir bilişim sisteminin işleyişini engelleyen veya bozan kişi, bir yıldan beş yıla kadar hapis cezası ile cezalandırılır.*

(2) *Bir bilişim sistemindeki verileri bozan, yok eden, değiştiren veya erişilmez kılan, sisteme veri yerleştiren, var olan verileri başka bir yere gönderen kişi, altı aydan üç yıla kadar hapis cezası ile cezalandırılır.*

Yasal düzenlemeden görüleceği üzere, TCK m. 244, "sisteme ve veriye müdahale" şapkası altında, birçok fiili suç kapsamına almaktadır. Bu bağlamda, failin bir bilişim sisteminin işleyişini engellemesi veya bozması (sisteme müdahale), bununla beraber bilişim sisteminin içerisindeki verileri bozması, yok etmesi, değiştirmesi, erişilmez kılması, bunun yanında sisteme veri yerleştirmesi yahut mevcut verileri başka bir yere göndererek sisteme zarar vermesi (veriye müdahale) suç sayılmaktadır.

Madde gerekçesine göre "*Maddenin birinci fıkrasında bir bilişim sisteminin işleyişini engelleme, bozma, sisteme hukuka aykırı olarak veri yerleştirme, var olan verileri başka bir yere gönderme, erişilmez kılma, değiştirme ve yok etme fiilleri, suç olarak tanımlanmaktadır. Böylece sistemlere yöneltilen ızrar fiilleri özel bir suç hâline getirilmiştir. Aracın fizik varlığı ve işlemesini sağlayan bütün diğer unsurları, söz konusu suçun konusunu oluşturmaktadır*." Bu gerekçeden ve kanun koyucunun eğiliminden hareketle, konulan bu hükümle, günümüz dünyasında kişilerin hemen her işini yaptıkları bilgisayar ve bilişim sistemlerinin ve bunların içinde yer alan verilerin sıhhatinin korunmasının amaçlandığı söylenebilir. Nitekim, kanunun yapıldığı dönemde, sosyo-ekonomik yapı içerisinde faaliyetlerin ağırlıklı olarak bilgisayar sistemleri aracılığıyla veri işleme şeklinde gerçekleştirilmeye başlanması ve günden güne bu işlemlerin yoğunlaşması, verilerin gizliliğine ve içeriğine ilişkin koruma yanında, mevcut verilerin

varlığının, bütünlüğünün ve erişilebilirliğinin de korunmasını gündeme getirmiştir[183]. Bu nedenle, kişisel verilerin korunmasına ilişkin mevzuatın yanında, özellikle bilişim sistemlerinin ve verilerin bütünlüğünün korunması amacıyla TCK m. 244 düzenlenmiştir.

Yukarıda ifade ettiğimiz üzere, TCK m. 244'te "bilişim sistemi" ve "sistemin içerisindeki veriler" olmak üzere iki koruma alanı söz konusudur. Bu koruma sisteminde Avrupa Konseyi Siber Suç Sözleşmesi'nin esas alındığını söylemek doğru olacaktır. Nitekim, Siber Suç Sözleşmesi'nde de bilişim sistemine ve verilere müdahale hususu baz alınmış, veriye müdahale 4., sisteme müdahale ise 5. maddede düzenlenmiştir. "Veriye Müdahale" *(Data interference)* başlıklı 4. maddeye göre,

> "*Her bir taraf devlet, bir kimsenin bilgisayar verisine hakkı olmadığı halde, bilerek ve isteyerek zarar verme, silme, bozma, değiştirmeye ya da ortadan kaldırma fiilleri işlemesini suç olarak düzenlemek üzere gerekli kanuni düzenlemeyi yapmalı ve gerekli diğer önlemleri almalıdır*."

"Sisteme Müdahale" *(System interference)* başlıklı 5. maddede ise şu düzenleme yer almaktadır:

> "*Her bir taraf devlet veri yükleyerek, aktararak zarar vererek, silerek, bozarak, değiştirerek veya müdahale ederek bilgisayar sisteminin kullanımında hakkı olmadığı halde bilerek ve isteyerek bilgisayarın sisteminin çalışmasını sekteye uğratma fiilini ulusal kanununda suç olarak düzenlemeli ve gerekli diğer düzenlemeleri yapmalıdır."*

Sözleşmenin sisteme müdahaleyi düzenleyen 5. maddesine bakıldığında, bilgisayar sisteminin fiziken zarar görmesi aranmadığı, yalnızca sistemin işleyişinin ciddi bir biçimde engellenmesinin yeterli olacağının söylendiği, bu bağlamda da bilişim sisteminin maddi varlığını oluşturan donanımına yönelik fiziksel müdahalenin kapsam dışı bırakıldığı ifade edilmiştir[184].

TCK m. 244 de sisteme müdahale ile veriye müdahaleyi birbirinden ayırmış ve 1. fıkrasında sisteme müdahaleyi, 2. fıkrasında sistem içerisindeki

[183] KETİZMEN, s. 112.
[184] KETİZMEN, ss. 114- 115.

veriye müdahaleyi düzenlemiştir. Maddedeki düzenlemeye bakıldığında, bunların iki ayrı suç tipi olduğu ve bu iki suç tipinin de seçimlik hareketli olarak düzenlendiği, ayrıca her iki suç tipinde yer alan hareketlerin de ayrı ayrı yalnızca suçun gerçekleşmesi için gerekli olan sonuçların gösterilmesi suretiyle düzenlendiği, dolayısıyla bunların serbest hareketli suçlar olarak öngörüldüğü görülmektedir[185].

Bilişim sistemleri nazara alındığında, bu sistemlerin esas özelliklerini klavyesi, monitörü, faresi gibi fiziksel varlıklarını oluşturan donanımından çok, verileri, programları, sunucusu gibi soyut varlıklarını ihtiva eden yazılım unsuru belirlemektedir. Ancak, bahsi geçen yazılım unsurunun doğru bir biçimde çalışması, örneğin verilerin işlenmesi ya da saklanması, donanım unsurunun da işlevini yerine getirmesini sağlamaktadır. İşte birbirine bağlı olarak işleyen bu süreç, kanun koyucu tarafından "*bilişim sisteminin işleyişi*" olarak formüle edilmiştir.

Bilişim sistemi, hem somut hem de soyut varlıkları ifade ettiğinden ve bunların işlemesi birbirine bağlı olduğundan, bunlardan birisine yapılan müdahale diğer unsuru da temelden etkilemektedir. Bu itibarla, sistemin maddi varlığını oluşturan donanıma yönelik fiziksel saldırılar da bu madde kapsamında olup, bunun şartı ise bahsi geçen fiziksel saldırının amacının bilişim sisteminin işleyişine yönelmesidir. Buradan hareketle, bilişim sisteminin işleyişine yönelmeyen donanıma yönelik fiziksel saldırılar, TCK m. 244/1 kapsamında değerlendirilmeyecektir. Örneğin, sistemin işleyişini engelleme amacı gütmeden bir bilgisayara fiziksel saldırıda bulunan fail TCK m. 244/1'den değil, TCK m. 151'deki "Mala Zarar Verme" suçundan sorumlu olacaktır. Bu bağlamda, sisteme müdahale suçunun maddi unsurunu, bir bilişim sisteminin işleyişinin engellenmesine yönelmiş, o bilişim sisteminin donanımına veya yazılımına yapılan saldırılar olarak tanımlamak mümkündür.

Bu fiil, teknolojik gelişmelerin artmasına paralel bir biçimde, sınırsız sayıda yöntemle gerçekleştirilebilir. Örneğin, bir web sayfasına erişim, genel olarak o web sayfasını barındıran sunucu bilgisayara (*hosting*) bağlantı kurulması ve sunucuda bulunan web sayfasının içeriğinin yer aldığı verinin kopyalanması anlamına gelmektedir. Web sayfasının yer aldığı sunucu ise,

[185] DÜLGER, s. 395.

belli bir zaman diliminde, ancak belli sayıda bağlantı sağlayabilecek ve veri kopyalamasına izin verebilecek bir kapasiteye sahiptir. Sunucunun bu kapasitesine "bant genişliği" adı verilmektedir. İşte, bu sunucunun birim zamandaki işlem kapasitesinin aşılmasını sağlayacak şekilde ve bu amaçla sistemle bağlantı kurulması yönünde gönderilecek çok sayıda talep, sistemin taleplere cevap verememesini ve kilitlenmesine sebep olacaktır. Bu durumda web sayfasına erişim sağlanamayacak ve söz konusu bilişim sisteminin işleyişi engellenecektir.

Bu kapsamda, TCK m. 244/1'de öngörülen "engelleme" fiili, bilişim sisteminin genel olarak çalışmasına ilişkin olabileceği gibi, bu işleyişe katkısı yahut etkisi olan herhangi bir unsurun işleyişine engel olunarak da örneğin Ethernet kart işlevsiz hale getirilerek sanal ağlara bağlantı yapılmasının engellenmesi şeklinde de işlenebilir. Fiil bakımından önemli olan, çalışması engellenen unsurun sistemin işleyişini kısmen veya tamamen önleyebilmesidir[186].

Özellikle TCK m. 244/1 bağlamında DDoS saldırılarının üzerinde dikkatle durulması gerekmektedir. Siber güvenlik ile ilgili olarak, bilişim sistemine müdahale suçunun en sık görülen yöntemi DoS *(Denial of Service)* ve DDoS *(Distributed Denial of Service)* saldırılarıdır. DoS saldırısı, kısaca, belli bir sunucunun belli bir şekilde hizmet bekleyen kullanıcılara hizmet verememesini sağlamak amacıyla, o bilgisayarın işlem yapmasını engellemek, bir başka deyişle hedef bilgisayarı bilişim sisteminin içerisine girmeksizin kilitlemektir[187]. DoS işlemi, birden çok sayıda bilgisayar üzerinden yapıldığında, yani "dağıtık" (*distributed*) bir şekilde gerçekleştirildiğinde ise ortaya DDoS saldırısı çıkmaktadır.

DDoS saldırısında, saldırgan, *hacking* yoluyla daha önceden ele geçirmiş ve hazırlamış olduğu birçok makina üzerinden, seçmiş olduğu hedef sistemin trafiğini arttırarak, o sistemin işleyemez hale gelmesini sağlamaktadır. Saldırganın *hacking* yoluyla ele geçirmiş olduğu ve görünürde hedef bilgisayarların sistemlerine saldıran bu makinalara "*zombi*" adı verilir. *Zombi*ler esasen saldırganın daha önce bir açığını bularak ele geçirdiği (*hack* ettiği) ve saldırı sırasında kullanmak üzere içlerine program yerleştirdiği

[186] DÜLGER, s. 395.

[187] ALTUNDAL, Ömer Faruk, "DDoS Nedir, Ne Değildir?" http://www.academia.edu/14209169/SİBER_GÜVENLİK_DERNEĞİ_DDo_S_nedir_ ne_değildir, (e.t. 01.04.2018).

bilgisayarlardır. Bir başka deyişle, *zombi*ler saldırının merkezinde bulunan, ancak saldırı fiilinden haberdar dahi olmayan ve güvensiz olduğu için saldırgan tarafından ele geçirilmiş makinalardır. *Zombi* programları, genellikle güvenliği zayıf olan sistemlere yerleştirilir.

Saldırgan tarafından *zombi*ler üzerinde kurulan programlar (*daemon*) belirli bir kaynaktan gelecek DDoS komutlarını dinlemekte ve bu yolla hedef sisteme saldırıları gerçekleştirmektedir. Binlerce bilgisayara yerleştirilen bu programlar, bilgisayarlara uzaktan kontrol (*remote*) imkanı vermekte, böylece saldırganın bu bilgisayarlar üzerinden istediği *server*'a istediği sayıda veri göndererek o *server*'ı çalışamaz hale getirmesine olanak sağlamaktadır.

İfade ettiğimiz gibi saldırgan, bu *zombi* bilgisayarları kullanarak hedef olarak belirlediği sisteme (bilgisayara ya da *hosta*) aynı anda giriş yapmaya çalışmakta ve bu yolla kapasitesinin çok üzerinde istek gelen sistem tamamen kilitlenerek çalışamaz hale gelmektedir. Örneğin, barındırma hizmeti veren bir firmadan belirli bir bant genişliği edinen ve buna göre azami olarak aynı anda 2 bin kişinin girebileceği bir web sitesine, aynı anda 20 bin kişinin girmeye çalıştığı ve girmeye çalışırken bu 20 bin kişinin ayna anda komut yolladığı durumda, bu web sitesine ulaşılması mümkün olmamaktadır. İşte DDoS saldırısı, aynı anda binlerce kişinin belli bir sisteme sürekli giriş yapmaya çalışması gibi, bu işi otomatize eden bir yazılımla hedef sistemi kilitlemekte ve çalışamaz duruma getirmektedir[188]. DDoS saldırısı, özellikle son yıllarda, Devlet kurumlarına ait web sitelerine ve sistemlere saldıran hacker gruplarının en çok kullandığı yöntemlerin başında gelmektedir.

TCK m. 244'ün ikinci fıkrasında ise, bilişim sistemindeki veriler üzerinde işlenebilecek hemen her türlü hareket suç kapsamına alınmıştır. Buna göre, bir bilişim sisteminde bulunan verileri bozan, yok eden, değiştiren, erişilmez kılan, bu sisteme yeni bir veri yerleştiren, sistemde mevcut verileri bir başka yere gönderen failin eylemi TCK m. 244/2 kapsamında ceza sorumluluğuna tabi olacaktır[189].

---

[188] ÖZOCAK, Gürkan; "*DDoS Saldırısı ve Failin Cezai Sorumluluğu*", Bilişim 2012 – 29. Uluslararası Bilişim Kurultayı Bildiriler Kitabı, Ankara, 2012.

[189] Detaylı açıklama için bkz. DÜLGER, s. 397- 403.

4. Yasak Cihaz veya Programlar (TCK m. 245/A)

24.3.2016 tarihli ve 6698 sy. Kanun'un 30. maddesi ile Türk Ceza Kanunu'na eklenen 245/A maddesinde yeni bir bilişim suçu daha düzenlenmiştir. 'Yasak Cihaz veya Programlar' adı verilen bu yeni suç tipi, kanunda şu şekilde tanımlanmıştır:

> *"Bir cihazın, bilgisayar programının, şifrenin veya sair güvenlik kodunun; münhasıran bu Bölümde yer alan suçlar ile bilişim sistemlerinin araç olarak kullanılması suretiyle işlenebilen diğer suçların işlenmesi için yapılması veya oluşturulması durumunda, bunları imal eden, ithal eden, sevk eden, nakleden, depolayan, kabul eden, satan, satışa arz eden, satın alan, başkalarına veren veya bulunduran kişi, bir yıldan üç yıla kadar hapis ve beş bin güne kadar adli para cezası ile cezalandırılır."*

Kanun koyucu bu düzenleme ile, TCK'ndaki bilişim suçlarına ek olarak, zararlı yazılımları, TCK'nda yer alan bilişim sistemine hukuka aykırı olarak girme, bu sistemin işleyişini engelleme veya sistemdeki verilere müdahale etme (*yok etme, bozma, veri alma, verileri başka yere nakletme vb.*), banka ve kredi kartlarına kartlarının kötüye kullanılması eylemlerini yahut bilişim vasıtalı diğer suçları işlemek amacıyla cihaz ve program imal edilmesi, alınması, depolanması, satılması, satın alınması, başkasına verilmesi veya bulundurulması gibi eylemleri suç kapsamına almış ve bunlara ciddi cezalar öngörmüştür.

Özellikle son yıllarda, *crack, keylogger, trojan* vb. hacking yazılımlarının İnternet üzerinden, çeşitli İnternet forumlarında ve web sitelerinde son derece kolay bir biçimde paylaşılması, temin edilmesi, kullanılması ve bu nedenle siber suçluluğun sayısal olarak katlanarak artması dolayısıyla, bu suçlulukla mücadele için, bahsi geçen kötücül yazılımların imal edilip yayılmasını önleyici ceza normlarının düzenlenmesinde herhangi bir sorun olmadığı kanaatindeyiz. Ne var ki, madde metninin suç teşkil eden hareketleri çok geniş kapsamlı olarak düzenlemesi ve özellikle bu tür yazılımların "bulundurulmasını" da suç kapsamına alması nedeniyle, maddenin uygulanmasında birçok sorun ve tartışmayla karşılaşılması muhtemeldir. Nitekim, bu suçla ilgili en çok tartışma yaratacak hususlardan birisi, hemen her bilişim firmasının yaptığı "*pentest*" adı da verilen penetrasyon (sızma) testleridir. Bu testler, müşteriler tarafından belirlenen

bilişim sistemlerine mümkün olabilecek her yolun denenerek sızma çalışma çalışması veya DoS yahut DDoS saldırıları yapılmasını kapsamaktadır. Testin yapılmasındaki amaç, müşterinin bilişim sistemindeki güvenlik açığını bulmak olduğu kadar, bulunan açıkların değerlendirilip sorunun çözülmesi ve sistemlere yetkili erişimler elde edilebilmesinin sağlanmasıdır. Bir başka deyişle, pentestler ile, belirlenen veya belirsiz zamanlarda sisteme "tatbikat" mahiyetinde saldırılar yapılmakta ve bu şekilde sistemin güvenlik açıklarının tespit edilip kapatılması sağlanmaktadır. Ancak, pentest yapılması için kullanılan yazılımların "bir bilişim sistemine girme, sistemin işleyişini engelleme" amaçlı yazılımlar olması ve doğrudan bu amaçla kullanılması sebebiyle, bu yazılımı elinde bulunduran kişinin elinde bulundurma amacı, söz konusun bulundurma eyleminin suç olup olmadığını belirleyecektir.

TCK m. 245/A'daki yeni düzenleme ile, pentest yazılımlarını uhdesinde bulunduran kişiler, bu yazılımları hukuka uygun amaçlarla bulundurduğunu ispat etmekte zorluk yaşamaları durumunda, ceza sorumluluğu tehlikesiyle karşı karşıya kalacaklardır. Benzer bir biçimde, *phishing* yazılımları, DDoS programları, ağ izleme araçları gibi siber saldırı amaçlı yazılımların imal edilmesi, satılması, temin edilmesi gibi durumların yanı sıra, eğer amaç TCK m. 243 ilâ 245'te öngörülen suçların işlenmesi ise, yalnızca bulundurulması dahi ceza sorumluluğu doğuracaktır[190].

5. Banka veya Kredi Kartlarının Kötüye Kullanılması (TCK m. 245)

TCK'nun *Bilişim Alanında Suçlar* başlığı altında düzenlediği diğer suç tipi ise banka ve kredi kartlarının kötüye kullanılması suçudur. Bu suç, esasen teknik anlamda bir bilişim suçu olmayıp, bilişim sistemlerinin kullanılması yoluyla işlenen dolandırıcılık suçunun bir özel görünüşü şeklinde düzenlenmiştir. Buna göre;

(1) Başkasına ait bir banka veya kredi kartını, her ne suretle olursa olsun ele geçiren veya elinde bulunduran kimse, kart sahibinin veya kartın kendisine verilmesi gereken kişinin rızası olmaksızın bunu kullanarak veya kullandırtarak kendisine veya başkasına yarar sağlarsa, üç yıldan altı yıla kadar hapis cezası ve adlî para cezası ile cezalandırılır.

[190] ÖZOCAK, Gürkan, "*Penetrasyon Testlerinin (Pentestlerin) Hukuki Durumu ve Zararlı Yazılımlar*", http://www.bilisimdergisi.org.tr/yazarlar/konuk-yazarlar/penetrasyon-testlerinin-pentestlerin-hukuki-durumu-zararli-yazilimlar.html, (e.t. 02.04.2018).

(2) Sahte oluşturulan veya üzerinde sahtecilik yapılan bir banka veya kredi kartını kullanmak suretiyle kendisine veya başkasına yarar sağlayan kişi, fiil daha ağır cezayı gerektiren başka bir suç oluşturmadığı takdirde, dört yıldan yedi yıla kadar hapis cezası ile cezalandırılır.

(3) Sahte oluşturulan veya üzerinde sahtecilik yapılan bir banka veya kredi kartını kullanmak suretiyle kendisine veya başkasına yarar sağlayan kişi, fiil daha ağır cezayı gerektiren başka bir suç oluşturmadığı takdirde, dört yıldan sekiz yıla kadar hapis ve beşbin güne kadar adlî para cezası ile cezalandırılır.[191]

6. Kişisel Verilerin Korunmasına İlişkin Suçlar (TCK m. 135-138)

Kişisel veri, en geniş tanımıyla, belirli ya da belirlenebilir nitelikteki bir kişiye ilişkin her türlü bilgidir. O halde, kişisel veriyi, kişisel olmayan veriden ayırabilmek için temelde iki kriterden yararlanıldığı söylenebilir. Bu bağlamda, kişisel veriden söz edebilmek için, veri (i) *bir kişiye ilişkin* ve (ii) bu kişi de *belirli ya da belirlenebilir nitelikte* olmalıdır. Bu temel ayrımın şöyle basit bir örnekle açıklanması mümkündür: Bir kimsenin adı, onun belirli ya da belirlenebilir olması için akla gelen ilk bilgidir. Bu anlamda ad, pek çok durumda kişisel veri niteliğindedir. Ancak, yaygın bir ad ve soyada sahip olan bir kimseye ilişkin olarak yalnızca bu bilgiye yer verilmesi onu belirlenebilir kılmaz. Aynı şekilde, bazen bir kişinin, tam adı bilinmese de belirlenebilir olduğu görülür. Bu durumda, yukarıda belirttiğimiz iki ölçüte dikkat ederek ve bu ölçütler nazara alınarak, hangi bilgilerin kişisel veri niteliğinde olduğunun tespit edilmesi gerekmektedir[192].

Kişisel verilerin korunması hususu, Avrupa Birliği başta olmak üzere uluslararası toplumun önemli konu başlıklarından birisidir. Bu bağlamda Avrupa Birliği'nin 95/46/EC Kişisel Veri Koruma Direktifi, üye ülkelere kişisel verilerin korunması ile ilgili birçok yükümlülük getirmekte olup, diğer uluslararası hukuk metinleri de kişisel verilerin korunması ile ilgili önemli hükümleri ihtiva etmektedir. Nitekim, Anayasamızın 20/3. maddesinde de kişisel verilerin korunması anayasal ilke haline getirilmiş, buna rağmen kişisel verilerin korunmasına ilişkin kanun tasarısı uzun yıllar boyunca TBMM'de

[191] Bu suça ilişkin detaylı açıklama için bkz. DÜLGER, ss. 427- 524.
[192] KÜZECİ, Elif, Kişisel Verilerin Korunması, 2. Bası, Ankara, 2018, ss. 9 -10.

"tasarı" halinde durmuş ve bir türlü yürürlüğe girememiştir[193]. Nihayet, 24 Mart 2016 tarihinde TBMM'de kabul edilen 6698 sayılı Kişisel Verilerin Korunması Kanunu, 7 Nisan 2016'da Resmi Gazete'de yayımlanarak yürürlüğe girmiş ve Türkiye'de de kişisel verilerin korunması rejimi yasalaşabilmiştir[194].

Kişisel verilerin korunmasına ilişkin suçlar TCK'nun 135 ilâ 138. maddelerinde düzenlenmiştir. Buna göre, bir siber saldırı durumunda sistemde bulunan kişisel verilere ilişkin olarak bu hükümler uygulama alanı bulacaktır. TCK'nun yürürlüğe girdiği 2005 yılından 6698 sayılı Kişisel Verilerin Korunması Kanunu'nun yürürlüğe girdiği 2016 yılı arasında geçen onbir yıl boyunca, yasa uygulayıcıların karşılaştığı en ciddi sorunlardan biri, "kişisel veri"yi ve buna ilişkin temel ilkeleri düzenleyen bir yasal düzenlemenin bulunmamasıydı. Bu nedenle, TCK'nun bu hükümlerinin uygulanmasında problemler yaşanmış, birçok durumda suça vücut veren eylemin kapsamının belirlenememesi ve hatta suç tipine uygun fiillerin cezalandırılamaması durumu söz konusu olmuştu[195]. Aynı şekilde, kişisel verilerle ilgili bir mevzuatın bulunmaması, TCK hükümleri uyarınca hapis cezası yaptırımına bağlanmış veri işleme eylemlerinin niteliği, hangi durumlarda hukuka aykırılık değerlendirmesinin yapılacağı, somut olayda "kişisel veri" ile ilgili bir durumun bulunup bulunmadığı gibi soru ve sorunları da beraberinde getirmişti[196]. 6698 sayılı Kanun ile kişisel veri gibi birçok temel kavram tanımlanmış ve veri işlemedeki temel ilkeler düzenlenmiştir. Bunun yanı sıra, TCK'nun ilgili hükümlerine de atıfta bulunulmuş ve doğrudan TCK ile Kişisel Verilerin Korunması Kanunu arasında bağlantı kurulmuştur[197].

Kişisel verilerin korunması ile ilgili düzenlenen ilk suç, TCK m. 135'teki kişisel verilerin kaydedilmesidir. Buna göre;

---

193 Buna ilişkin ilk tasarı Adalet Bakanlığınca 2003 yılında hazırlanmış, ilk kez 22 Nisan 2008 tarihinde TBMM'ye sevk edilmiştir. Bu tarihten sonra farklı taslaklar gündeme gelmiş ve 2003 yılında başlayan kişisel verilerin korunmasına ilişkin kanun çalışması süreci, ancak 13 yıl sonra, 7 Nisan 2016'da sona ermiştir. Detaylı bilgiler için bkz. KÜZECİ, ss. 311- 312.

194 Kanunlaşma süreci, kanunun getirdiği yenilikler, benimsediği sistem ve kapsamlı tartışmalar için bkz. KÜZECİ, s. 304- 377.

195 Değerlendirme hakkında bkz. ÖZTÜRK, Bahri/ERDEM, Mustafa Ruhan, Uygulamalı Ceza Muhakemesi Hukuku, 11. Baskı, Ankara, 2007, s. 623.

196 KÜZECİ, s. 401.

197 KÜZECİ, s. 402.

(1) Hukuka aykırı olarak kişisel verileri kaydeden kimseye bir yıldan üç yıl a kadar hapis cezası verilir.

(2) Kişisel verinin, kişilerin siyasi, felsefi veya dini görüşlerine, ırki kökenlerine; hukuka aykırı olarak ahlaki eğilimlerine, cinsel yaşamlarına, sağlık durumlarına veya sendikal bağlantılarına ilişkin olması durumunda birinci fıkra uyarınca verilecek ceza yarı oranında artırılır.

Burada dikkat çeken husus, bazı kişisel veriler için kaydın "hukuka aykırı" olması aranırken, ikinci fıkrada "*kişilerin siyasi, felsefi veya dini görüşlerine, ırki kökenlerine*" ilişkin bilgilerin kaydedilmesi için hukuka aykırılığın özel bir şart olarak aranmamasıdır. O halde, bu nitelikteki kişisel verilerin kaydının her durumda, mutlak olarak hukuka aykırı olacağını söylemek mümkündür[198].

TCK'nun kişisel verilerin korunmasına ilişkin öngördüğü diğer suç, TCK m. 136'da düzenlenen verilerin hukuka aykırı olarak verilmesi veya ele geçirilmesidir. Bu hükme göre;

(1) Kişisel verileri, hukuka aykırı olarak bir başkasına veren, yayan veya ele geçiren kişi, iki yıldan dört yıla kadar ha pis cezası ile cezalandırılır.

Kanun burada seçimlik hareketli bir suç öngörmüş ve "*verme*", "*yayma*" ve "*ele geçirme*" eylemlerinin her birini ayrı ayrı suç olarak düzenlemiştir. Ancak, bu hareketlerin tam olarak neyi ifade ettiği tanımlanmamıştır. Bu husus, özellikle bazı dijital veri işleme etkinlikleri bakımından şüpheye sebep olabilir[199].

TCK'nda kişisel verilerin korunmasına yönelik düzenlenen bir diğer suç ise, 138. maddede tanımlanan Verileri Yok Etmeme suçudur:

(1) Kanunların belirlediği sürelerin geçmiş olmasına karşın verileri sistem içinde yok etmekle yükümlü olanlara görevlerini yerine getirmediklerinde bir yıldan iki yıla kadar hapis cezası verilir.

(2) Suçun konusunun Ceza Muhakemesi Kanunu hükümlerine göre ortadan kaldırılması veya yok edilmesi gereken veri olması hâlinde verilecek ceza bir kat artırılır.

---

198 HAFIZOĞULLARI, Zeki/ÖZEN, Muharrem, Türk Ceza Hukuku Özel Hükümler, Kişilere Karşı Suçlar, Ankara, 2010, s. 269.

199 KÜZECİ, s. 407.

Buna göre kişisel veriler, amaç için gerekli olandan daha uzun süreyle tutulmamalıdır. Kişisel verilerin ancak belli bir süre için tutulması ve artık ihtiyaç duyulmayan verilerin silinmesi veya anonimleştirilerek kişisellik niteliklerinin ortadan kaldırılması keyfi uygulamaların da önüne geçilmesi adına son derece önemli ve yerindedir[200]. Nitekim, Kişisel Verilerin Korunması Kanunu da bu konuda TCK m. 138'e doğrudan atıf yapmaktadır. Kanun'un 17/2. maddesinde, KVKK m. 7'ye aykırı biçimde "*kişisel verileri silmeyen veya anonim hale getirmeyenler 5237 sayılı Kanunun (TCK) 138inci maddesine göre cezalandırılır*" denilmektedir. KVKK'nun 7. maddesine göre de, KVKK m. 7 ve diğer ilgili hükümlere "*uygun olarak işlenmiş olmasına rağmen, işlenmesini gerektiren sebeplerin ortadan kalkması halinde kişisel veriler resen veya ilgili kişinin talebi üzerine veri sorumlusu tarafından silinir, yok edilir veya anonim hale getirilir.*"

Son olarak, TCK'nun 137. maddesinde ağırlaştırıcı nedenler öngörülerek, yukarıda belirttiğimiz suçların kamu görevlisi tarafından ve kamu görevi kötüye kullanılarak işlenmesi yahut belli bir meslek ya da sanatın sağladığı kolaylıktan yararlanmak suretiyle işlenmesi durumunda, verilecek cezanın ağırlaştırılacağı düzenlenmiştir.

B. Adli Bilişim

Kanunda suç olarak öngörülmüş bir eylem söz konusu ise, ikinci aşama, bu suça ilişkin delillerin sağlıklı bir biçimde toplanması ve ceza soruşturması ve yargılaması süreçlerinde, fiil ve faili tespit için kullanılmasının sağlanmasıdır. Bu delilleri toplamaya ve değerlendirmeye yarayan, disketlerden, sabit disklerden ve çıkartılabilir disklerden delil elde etme amacıyla veri kurtarma işlemi olan ve elektronik delillerin muhteva ettiği bilgileri, delil inceleme süreçlerini, hukuki ve etik sorumlulukları göz önünde bulundurarak, delilin bütünlüğünü koruyarak ve maddi gerçeği açığa çıkarmak amacıyla; kopyalama, belirleme, çözümleme, yorumlama ve belgeleme süreçlerinin bütününe '*adli bilişim'* adı verilmektedir[201]. Adli bilişim, genel olarak dört alt dala ayrılmakta olup, bunlar; bilgisayar adli

[200] KÜZECİ, s. 408.

[201] BARRY, Sean, "*Smoking Microchips Tells It All : Computer Forensic Experts Mine Hard Drives For Data That Too-Clever Users Thought Long Deleted",* http://www.dataforensics.com/articles/ smoking_microchip_ tells_it_all.pdf, (e.t. 15.10.2017); KESER BERBER, Leyla; Adli Bilişim, Ankara, 2004, s. 39.

bilişimi, ağ ve İnternet adli bilişimi, gömülü cihazlara ait adli bilişim ve son zamanlarda dördüncü bir alt dal olarak kabul edilen sosyal ağ adli bilişimidir[202].

Özellikle delil elde edilen alanlar son derece hassas ve kolaylıkla zarar görebilir nitelikte olduklarından, delil toplama işlemi, teknik gerekliliklerin çok sayıda olduğu, hassas bir süreçler bütünü olarak kabul edilmelidir. Bu süreç işletilirken, el konulacak bilgisayarlardan veri alınmasından, bilgisayarın dondurulması, verilerin kopyalanması, klonlanması, bilgisayarın kapatılması ve laboratuvara götürülmesine kadar bütün süreçler çok titiz bir biçimde yerine getirilmeli ve eldeki delillerden hiçbirinin kaybolmaması veya zarar görmemesi sağlanmalıdır. Aynı zamanda, bir suç şüphesiyle bu yola başvurulduğundan, bilgisayarı veya bilişim sistemi incelenen kişinin mahremiyeti bir nevi kamu gücü kullanılarak ihlal edildiğinden, bu yola son derece istisnai hallerde ve sıkı bir rejime tabi olarak başvurulmalıdır.

Bu nedenle, Ceza Muhakemesi Kanunu'nun 134. maddesinde, bilgisayar ve bilgisayar kütüklerinde yapılacak arama ve el koyma işlemlerinin sınırları ve nasıl yapılacağı düzenlenmiştir. Buna göre; ancak bir suç soruşturmasında ve somut delillere dayanan kuvvetli şüphe sebeplerinin varlığı halinde, yalnız şüphelinin kullandığı bilgisayarda, Cumhuriyet Savcısının istemi üzerine ve ancak hakim kararıyla, üstelik başka surette delil elde etme imkanının bulunmaması halinde arama ve el koyma yapılabilir. El koyma işlemi sonunda, el konan cihazların kopyaları (imajları) alınıp orijinalleri derhal sahibine iade edilir ve sistemdeki tüm verilerin –talebe gerek olmaksızın- yedekleri alınarak yedekten bir kopya şüpheli veya vekiline verilir[203].

Kanun maddesinde yer almasa dahi, ceza muhakemesinde delillerin sağlıklı olması esas alındığından ve delil üzerinde oynama yapılma ihtimalinde (delil *kanuna aykırı delil* haline geleceği için) o delilin ceza muhakemesinde kullanılamayacak olmasından, uygulamada el konulan harddisklerin *hash* değeri de alınmakta ve bu *hash* değeri harddiskin yedeği

---

[202] ÖZEN, Muharrem/ÖZOCAK, Gürkan, "*Adli Bilişim, Elektronik Deliller ve Bilgisayarlarda Arama ve El Koyma Tedbirinin Hukuki Rejimi (CMK m. 134)",* Ankara Barosu Dergisi, S. 2015/1, s. 45 vd.

[203] ÖZBEK, Veli Özer/KANBUR, M. Nihat/DOĞAN, Koray/ BACAKSIZ, Pınar / TEPE, İlker, Ceza Muhakemesi Hukuku, Ankara, 2012, s. 381. Ayrıca, ceza muhakemesinde elektronik delillerin niteliklerine dair detaylı bilgi ve yasal düzenlemeye ilişkin tartışmalar için bkz. ÖZEN/ÖZOCAK, s. 56 vd.

ile birlikte Şüpheliye verilmektedir. Bu sayede, siber saldırı nedeniyle yapılan delil tespiti işleminin sağlıklı ve doğru biçimde yapıldığı teminat altına alınmakta ve delile herhangi bir müdahalede bulunulduğu şüphesi de ortadan kaldırılmaktadır[204].

C. Siber Güvenlik Yasa Tasarısı

Her ne kadar henüz ortada yasalaşmış bir çalışma olmasa da, özellikle ulusal siber güvenliğin sağlanması ve kurumsallaşması için 'Siber Güvenlik Yasası' tasarı halinde uzun süredir TBMM'de bulunmakta ve yakın zamanda yasalaşması beklenmektedir. Ulaştırma, Denizcilik ve Haberleşme Bakanlığı'nın hazırladığı Yasa Tasarısı ile, USOM ve SOME'lerin işlevlerinin daha da arttırılması öngörülürken, etkin denetim, sır saklama yükümlülüğü, siber olaylara müdahale ekiplerinin görevleri gibi hususların detaylı düzenleneceği, ayrıca özel kuruluşlara da siber güvenlikle ilgili ek yükümlülükleri getirileceği ve siber saldırılara karşı güvenlik açıklarını kapatmayan şirketlere de çeşitli yaptırımlar uygulanacağı söylenmektedir.

Buna göre, yasalaşacak olan Siber Güvenlik Yasası Tasarısı'nda,

- Başta "*siber güvenlik*" olmak üzere, "*bilgisayar verisi", "kritik altyapılar", "kritik sektörler", "gizlilik", "bütünlük", "erişilebilirlik*" gibi siber güvenliğe ilişkin kavramların açık ve tartışmaya yer vermeyecek biçimde tanımlanması,
- "Kurumsal SOME" ve "Sektörel SOME"lerin tanımlanması ve bunların görev ve sorumluluklarının yine açık bir şekilde belirlenmesi,
- Kritik altyapıların ve Siber Güvenlik Kurulu'nun bunlar üzerindeki yetki alanlarının kapsamlı bir biçimde belirlenmesi,
- Siber güvenlikle ilgili uzman personelin yetiştirilmesi için ilgili meslek kuruluşları ve üniversiteler ile işbirliği ve görüş alışverişinin özel olarak yasaya eklenmesi ve bununla ilgili düzenlemelerin yapılması hususlarına yer verilmesinin, ulusal siber güvenliğin sağlanması adına yararlı olacağı kanaatindeyiz.

---

[204] ÖZOCAK, Gürkan; "*Ceza Muhakemesinde Elektronik Delillerin Tespiti ve Toplanması*", 2. Uluslararası Bilişim Hukuku Kurultayı Bildiriler Kitabı, İzmir, Kasım 2011, s. 114; ÖZEN/ÖZOCAK, s. 66.

V. SONUÇ: SİBER GÜVENLİĞİN SAĞLANMASINDA YÖNTEMLER

Çalışmamızda yer verdiğimiz üzere siber güvenlik hem uluslararası hukuk hem de bir iç hukuk meselesidir. Dolayısıyla siber güvenlik ancak ve ancak uluslararası barış ve güvenliğin sağlanmasına ilişkin hukuki düzen, uluslararası toplumun işbirliği ve devletler arasında yeknesak düzenlemelerin varlığı halinde mümkün olabilecektir.

Uluslararası hukuk bakımından sonuçları ağır siber saldırı durumunda uygulanacak hukuki rejim uluslararası barış ve güvenliğin tesisi için getirilen hukuki rejimle aynıdır. Çünkü işbu nitelikteki saldırılar, sadece mağdur devlete değil, uluslararası topluma yapılmış haksız fiillerdir. İşbu nedenle siber saldırıları kuvvet kullanma yasağı ve meşru müdafaa hakkı kapsamında değerlendirmek mümkündür.

Siber suç seviyesindeki siber saldırılar bakımından uluslararası toplum nezdinde akdedilen bütün anlaşmalar, devletlerin aynı suçları siber suç olarak düzenlemesi ve adli yardımlaşma yoluyla birbirleriyle iletişim halinde olmaları hususlarına yoğunlaşmaktadır. Ancak uluslararası hukuk tarafından dikkat çekmek istediğimiz husus, bağlayıcı ve bağlayıcı olmayan metinlerin sayısı ve bazılarının farklı siber suç tipleri içermesidir. Dolayısıyla uluslararası toplumda yeknesak siber suç tipleri yokken devletlerin yeknesak düzenlemelere sahip olmaları pek mümkün gözükmemektedir.

İşbu noktada, BM nezdinde siber güvenlik bakımından atılması gereken bir sonraki adımın, evrensel bir siber saldırıyla mücadele metninin kaleme alınması olduğu söylenebilir.[205] Tabi bunun için devletlerin, BM nezdinde atılacak işbu adım için gerekli motivasyona sahip olmaları oldukça önemlidir.

---

[205] Nitekim bu husus gerek doktrinde gerek devletler tarafından da dile getirilen bir hususdur. Doktrin açısından bkz. MARION, Nancy, *"The Council of Europe's Cyber Crime Treaty: An Exercise in Symbolic Legislation",* International Journal of Cyber Criminology, Vol. 4, Issue: 1&2, 2010, s. 708
Nitekim Birleşmiş Milletler Uyuşturucu ve Suç Ofisi tarafından hazırlanan raporda, siber suçlulukla mücadelede uluslararası bir sözleşme akdedilmesinin göz önüne alınması gerektiği ifade edilmiştir. Bkz. Working Paper on Recent Developments in the Use of Science and Technology by Offenders and by Competent Authorities in Fighting Crime, Including the Case of Cybercrime, 12- 19 April, 2010. http://www.unodc.org/documents/crime-congress/12th-CrimeCongress/Documents/A_CONF.213_9/V1050382e.pdf (e.t. 27.01.2016).

Ulusal hukuk açısından ise ulusal siber güvenliğin sağlanması ve kurumsallaşması için, dinamik bir yapıya sahip siber suç tanımlarının ceza kanunlarında eksiksiz ve bu dinamik yapıya uygun biçimde tanımlanması, ayrıca suç delillerinin elde edilmesine ilişkin yasa hükümlerinin buna paralel düzenlenmesinin yanı sıra ve bunlara ek olarak, bazı teknik ve yasal mücadele yöntemlerinin belirlenmesi çok önemlidir.

Bununla ilgili en çok çalışma yapılan ülkelerden birisi Amerika Birleşik Devletleri'dir. ABD'de bilişim suçları ve siber güvenlikle ilgili yasal düzenlemelerin yanı sıra, siber suçlulukla mücadele eden özel birimler kurulmuş ve bu birimlerin teknik araçlarla donatılarak yapılandırılmaları sağlanmıştır. Bunların en önemlilerinin arasında, *FBI National Infrastructure Protecture Center, Information Technology Association of America, Trap and Trace Center Authority, Carnegie Mellon's Emergency Response Team* gibi organizasyonlar sayılabilir. Bunun yanı sıra, üniversitelerde de bu hususla ilgili çalışmalar yapılmakta, sadece akademik ortamda değil, birçok kamu kurum ve kuruluşunda da siber suçlarla mücadele etmek için eğitim veren birimler çalışmaktadır. Bu hususla ilgili en üst merci olan Adalet Bakanlığı bünyesinde teşekkül eden '*Computer Crime and Intellectual Property Section'* (CCIPS) adlı birim de yine siber güvenlik alanında çalışmakta, eğitim faaliyetleri vermekte, siber güvenlikle ilgili uzman yetiştirmekte ve diğer kamu kurumlarıyla işbirliği içerisinde siber suçluluğun önlenmesi çalışmaları yapmaktadır[206].

Devletlerin ulusal siber güvenlik alanında, siber suçlulukla mücadele yöntemleri uzun zamandır tartışılmaktadır. Ne var ki, bu tartışmalar yapılırken, bir yandan güvenliğin korunması adına suçlulukla mücadelede kararlılık gösterilmesi gerekirken, bir yandan da kişi hak ve özgürlüklerinin son derece hassas bir biçimde gözetilmesi gerekmektedir. Dolayısıyla, örneğin, siber suçlulukla mücadele için devletin siber alanı denetlemesi gerektiği ileri sürülmekte ise de, bu yapılırken, kişi mahremiyeti ve iletişim özgürlüğü gibi demokratik, insan haklarına saygılı bir hukuk devletinin olmazsa olmazı olan temel ilkelerin korunması zorunludur. Suçla mücadele yöntemleri geliştirilirken, bireyin temel hak ve özgürlüklerinin özüne dokunulmamasının esas alınması birincil ilke olmalıdır[207].

[206] DÜLGER, s. 724; KARAGÜLMEZ, s. 93.
[207] Bu konudaki tartışmalar için bkz. DÜLGER, s. 726 vd.

Bu bağlamda, bilişim suçları ve siber güvenlik alanında çalışan hâklim, savcı ve kolluk güçlerinin teknik açıdan donanımlı hale getirilmeleri gibi zaten zorunlu olan yöntemlerin yanı sıra, kişi hak ve özgürlüklerine aykırılık tartışmasının alanında olan hususlara değinmeksizin, siber suçlulukla mücadele için gerekli olduğunu düşündüğümüz bazı teknik ve yasal tedbirlere ilişkin, aşağıdaki tedbirlerin alınması gerektiği kanaatindeyiz:

- **Öncelikle gerek var olan gerekse yeni koruma tedbirleri için teknolojik altyapı kurulması ve işletilmesi gerekmektedir**. Türkiye'deki Internet talebi ve ülkenin bulunduğu coğrafya göz önüne alındığında (Türkiye üzerinden geçen transit trafik), trafik hacminin yüksek olduğu değerlendirilebilir. Bu hacimde bir siber güvenlik altyapının kurulması yüksek maliyet oluşturmaktadır. Maliyetin kimin tarafından nasıl karşılanacağının sağlıklı bir şekilde çözüme kavuşturulması gerekmektedir. Ancak, bu maliyeti İSS'lere yüklemek ister istemez abone fiyatlarının dolaylı olarak artması anlamına gelmektedir.

- **Koruma tedbirlerinin uygulanabilmesi için trafik istatistiklerinin takip edilmesi gerekmektedir. Sofistike koruma yöntemleri için daha çok bilginin izlenmesi ve takip edilmesi zaman zaman zorunluluk haline gelmektedir**. Böyle bir durumda trafiğin genel olarak takip edilmesi düzleminden abonelerin kişisel bilgilerinin izlenmesi ve saklanması düzlemine geçiş yapılabilmektedir. Oysa ki kişisel bilgilerin işlenmesi ve gizliliğin korunması hak ve özgürlükler bakımından hayati hassasiyete sahip kavramlar olduğundan geniş düzlemde tartışılmalı ve fikir birliği aranmalıdır. Öte yandan bu bilgilerin yokluğunda, saldırıların tam anlamıyla tespit edilmesi ve suçluların yakalanması, bugünkü teknoloji ile çok mümkün görünmemektedir.

- **Teknolojik gelişmeler Internet üzerindeki içeriğin git gide konsolide olmasına yol açmaktadır** (örneğin bulut bilişim). İçeriğin git gide merkezi hale gelmesi (örneğin tüm haber portallarının Amazon bulut bilişim altyapısı üzerinden hizmet vermesi gibi) teknik takip ve tedbirler açısından yaptırımların daha kolay uygulanabilir hale gelmesine yol açacaktır.

- **Yönetmelik ve mevzuattaki tanımların muğlak olması teknik düzlemde problem yaratmaktadır**. Örneğin "*yönetimce kabul görmüş*" gibi tartışmaya açık tanımların olması tedbirler anlamında uygulamalarda farklılıklara yol açabilecek potansiyele sahiptir. Mevzuatta yer alan buna benzer muğlak ifadelerin yeniden ele alınması ve uygulayıcıları şüpheye düşürmeyecek, kesin ve net terim ve tabirler kullanılması gerekmektedir.

- **Koruma tedbirlerinden söz edildiğinde düşünülmesi gereken en önemli hususlardan biri de çalışmaların hızlı bir şekilde yürütülmesidir**. Siber dünyada zaman çok önemli bir boyuttur. Müdahalenin zamanında yapılmadığı durumda deliller ortadan kaybolabilir ve sonradan bilgi edinilmesi imkansız hale gelebilir. Bu tür durumların engellenmesi için ilişkide olunan ekiplerle (*SOME, USOM, diğer İSS'ler, kurum ve kuruluşlar gibi*) haberleşmenin belli standartlara bağlanması gerekmektedir. Standardın kapsamında, haberleşmenin doğasına bağlı olarak, sürekli (vardiyalı) çalışan müdahale ekipleri, basit bilgi formları, güvenli hatlarla ve/veya telefonla iletişim sıralanabilir.

- Ülkemizde, siber güvenlik hukuku konusunda daha fazla uzman yetiştirilmesine ihtiyaç bulunduğundan, bu hususta üniversitelerin ve kurumların gerekli eğitim, sertifikasyon ve tez çalışmaları yapılmasına imkan sağlaması gerekmektedir.

- Son olarak, ulusal siber güvenliğin en önemli hukuki altyapısını oluşturacak olan "*Ulusal Siber Güvenlik Yasa Tasarısı*"nın ivedilikle gündeme alınması ve kamu ile özel sektörün ve üniversitelerin işbirliği ile somut ihtiyaçları karşılayacak şekilde yasalaştırılması gerekmektedir.

KAYNAKÇA

Kitap ve Makaleler

ALTUNDAL, Ömer Faruk, *"DDoS Nedir, Ne Değildir?"* http://www.academia.edu/14209169/SİBER_GÜVENLİK_DERNEĞİ_DDo_S_nedir_ne_değildir, (e.t. 01.04.2018).

BARLOW, John Perry, A Declaration of the Independence of Cyberspace, ELECTRONIC FRONTIER FOUND., 8 February 1996), bkz. https://www.eff.org/ cyberspace-independence (e.t. 15.04.2018).

BARRY, Sean; "*Smoking Microchips Tells It All : Computer Forensic Experts Mine Hard Drives For Data That Too-Clever Users Thought Long Deleted",* http://www.dataforensics. com/articles/ smoking_ microchip_ tells_it_all.pdf, (e.t. 15.10.2017).

BAŞEREN, Sertaç Hami, Uluslararası Hukukta Devletlerin Münferiden Kuvvet Kullanmalarının Sınırları, Ankara Üniversitesi Basımevi, Ankara 2003, ss. 1- 19.

BENTHELEM, Sir Daniel QC, *"Principles relevant to the Scope of a State's Right of Self-Defence against an Imminent or Actual Armed Attack by Non-State Actors,"* Amer. JIL., Vol. 106, 2012.

BOOTHBY, William H., *"Methods and Means of Cyber Warfare"*, International Law Studies, Vol. 89, 2013.

BOZDOĞAN AKBULUT, Berrin; "*Bilişim Suçları*", Selçuk Üniversitesi Hukuk Fakültesi Dergisi Milenyum Armağanı, Sayı 1-2, C. 8, Konya, 2000.

BRING, Owe, "The Use of Force under the UN Charter: Modification and Reform through Practice or Consensus", içinde International Law and Changing Perceptions of Security Liber Amicorum Said Mahmoudi (EBBESSON, Jonas vd. ed.), BRILL, The Netherlands, 2014.

BROWN, Gary, "International Law Applies to Cyber Warfare! Now What?, Southwestern Law Review, Vol. 46, 2017.

BYERS, Micheal: "*Terrorism, The Use of Force and International Law After 11 September*" International Law and Comparative Law Quarterly, Vol. 51, Iss. 2, 2002.

CASSESE, Antonio, International Law, Oxford University Press, UK, 2005.

CENTEL, Nur/ZAFER, Hamide/ÇAKMUT, Özlem, Türk Ceza Hukukuna Giriş, Beta, İstanbul, 2006.

"Cybercrime Model Laws", Discussion paper prepared fort he Cybercrime Convention Committee (T-CY), 9 December 2014, https://rm.coe.int/ 1680303ee1 (e.t. 30.05.2018).

"Cyberspace in Peacetime Regime for State Activities in Cyberspace International Law", International Relations and Diplomacy NATO CCD COE Publication, Tallinn, 2013.

"Defense Department Cyber Efforts: Definitions, Focal Point and Methodology Needed for DOD to Develop Full-Spectrum Cyberspace Budget Estimates", US Department of Defense, Memo CM-0477-08" 2011, bkz. http://www.gao.gov/ assets/100/97674.pdf (e.t. 01.04.2018)

DEREK, Jinks, *"State Responsibility for the Acts of Private Armed Groups",* Chicago Journal of International Law Vol. 4, 2003.

DeWEESE, Geoffrey S., "*Anticipatory and Preemtive Self-Defence in Cyberspace: The Challange of Imminence",* in the 7th International Conference on Cyber Conflict: Architectures in Cyberspace, (MAYBAUM, M./OSULA, A. A./LINSTRÖM, M. L. ed.), NATO CCD COE Publications, Tallinn, 2015.

DINNIS, Hether Harrison, Cyber Warfare and the Laws of War", Cambridge, 2012.

DINSTEIN, Yoram, *"Computer Network Attacks",* INT'L L. STUD., Vol. 76, 2002.

DUCHEINE, P.A.L./ POUW, E.H., "Legitimizing the Use of Force: Legal Bases for Operations Enduring Freedo and ISAF", içinde Mission Uruzgan: Colloborating in Multiple Coalations for Afganistan, Pallas Publications, Amsterdam, 2012.

DÜLGER, Murat Volkan; Bilişim Suçları ve İnternet İletişim Hukuku, Ankara, 2014.

EICHENSEHR, Kristen E., *"Cyberwar & International Step-Zero",* Texas Law Journal Vol. 50, Iss. 2, 2015.

ERDEM Merve/ ÖZOCAK Gürkan, *"Sınıraşan Bir Suç Olarak Siber Suçlarla Mücadelede Uluslararası İşbirliği*", 19. Akademik Bilişim Konferansı, 8-10 Şubat 2017, Aksaray Üniversitesi, Aksaray.

EREM, Faruk; "*Bilgisayar Suçları ve TCY*", Yargıtay Dergisi, C. 17, Sayı 4, Ekim 1991.

GEERS, Kenneth, "Cyberspace and the Changing Nature of the Warfare", http://www. blackhat.com/presentations/bh-jp-08/bh-jp-08-Geers/ BlackHat-Japan-08-Geers-CyberWar fare-Whitepaper.pdf, (e.t. 09.03.2018).

GERVAIS, Michail, *"Cyber Attacks and the Laws of War",* Berkeley J. Int'l L., Vol. 30, 2012.

GILL, Terry D. – DUCHEINE, Paul A.L., "Anticipatory Self Defence in the Cyber Context", "*Int'l L. Stud.",* Vol. 89, 2013.

GRAY, Christine, International Law and the Use of Force, Oxford University Press, Third Edition, the UK, 2008.

GREENWOOD, Christopher: *"International Law and the Pre-emtive Use of Force: Afganistan, AL-Qaiada and Iraq*", San Diego Int'l Law, Journal, 2003.

GUIORA, Amos, Cybersecurity, Geopolitics, Law and Policy, Routhledge, NewYork, 2017.

GÜRPINAR, Bulut, "Milli Güvenlik Kurulu ve Dış Politika"*, Uluslararası İlişkiler*, Cilt 10, Sayı 39, 2013.

HAFIZOĞULLARI, Zeki /ÖZEN, Muharrem, Türk Ceza Hukuku Özel Hükümler, Kişilere Karşı Suçlar, Ankara, 2010.

HAKIMI, Monika, *"Defensive Force Against Non-State Actors: The State of Play",* International Legal Studies, Vol. 91, 2015.

HALATÇI, Ülkü: "*11 Eylül Terörist Saldırıları ve Afganistan Operasyonu'nun Bir Değerlendirmesi"*, Uluslararası Hukuk ve Politika, C.2, No. 7.

HATHAWAY, Oana vd., *"The Law of Cyber-Attack,"* CALIF. L. REV., Vol. 100, 2012.

İÇEL, Kayıhan: "Avrupa Konseyi Siber Suç Sözleşmesi Bağlamında 'Avrupa Siber Suç Politikasının Ana İlkeleri', İstanbul Üniversitesi Hukuk Fakültesi Mecmuası, C: LIX, Sayı: 1-2, 2001.

JENNINGS, R.Y. "*The Caroline and McLeod Cases"*, American Journal of International Law, Vol. 32, 1938.

JENSEN, Eric Talbot Jensen, *"The Future of the Law of Armed Conflict: Ostriches, Butterflies, and Nanobots",* 35 MICH. J. INT'L L., Vol. 35, 2014.

JESCHECK, Hans- Heinrich, Alman Ceza Hukukuna Giriş, Çev. Feridun Yenisey, İstanbul, 2007.

JUTTA, B.- STEPHEN J. T., Legitimacy and Legality in International Law: An Interactional Account, Cambridge University Press, Cambridge, 2010.

KAJTAR, Gabor, *"The Use of Force Against ISIL in Iraq and Syria- A Legal Battlefield",* Wisconsin International Law Journal, Vol. 34, No. 3.

KANUCK, Sean, *"Sovereign Discourse on Cyber Conflict Under International Law",* Texas Law Review, Vol. 88, 2010.

KARAGÜLMEZ, Ali, Bilişim Suçları ve Soruşturma-Kovuşturma Evreleri, 3. Bası, Ankara, 2011.

KAYA, İbrahim, Terörle Mücadele ve Uluslararası Hukuk, USAK Yayınları, Ankara, 2005.

KESKİN, Funda, Uluslararası Hukukta Kuvvet Kullanma: Savaş, Karışma ve Birleşmiş Milletler, Mülkiyeliler Birliği Vakfı Yayınları, Tezler Dizisi: 4.

KETİZMEN, Muammer; Türk Ceza Hukukunda Bilişim Suçları, Ankara, 2008.

KEYMAN, Selahattin, *"Tipiklik ve Ceza Hukuku",* AÜHFD, C. 37, S.1-4, 1980,

KITTICHAISAREE, Kriangsak., Public International Law of Cyberspace, Springer, Switzerland, 2017.

KURT, Levent, Tüm Yönleriyle Bilişim Suçları ve Türk Ceza Kanunundaki Uygulaması, Ankara, 2005.

KURT, Levent; Tüm Yönleriyle Bilişim Suçları ve Türk Ceza Kanunundaki Uygulaması, Ankara, 2005.

LENTZ, Christopher, *"A State's Duty to Prevent and Respond to Cyberterrorist Acts",* Chicago Journal of International Law, Vol. 10, 2010.

LOTRIONTE, Catherine, *"State Sovereignity and Self Defence in Cyberspace: A Normative Framework for Balancing Legal Rights",* Emory International Law Review, Vol. 26, 2012.

MAOGOTO, Jackson, Ntamuya, *"War on the Enemy: Self-Defence and State-Sponsored Terrorism",* Melbourne Journal of International Law, Vol. 4, No. 2, 2003.

MARION, Nancy, *"The Council of Europe's Cyber Crime Treaty: An Exercise in Symbolic Legislation",* International Journal of Cyber Criminology, Vol. 4, Issue: 1&2, 2010.

MIDOĞLU, Çise / ÖZOCAK, Gürkan; "*IPv6, Güvenlik Açıkları ve Hukuki Durum*", Bilişim 2013 – 30. Ulusal Bilişim Kurultayı Bildiriler Kitabı, Ankara, 2013.

MURPHY, Sean, *"Contemporary Practice of the United States Relating to International Law",* American Journal of International Law, Vol. 96, 2002.

MÜLLERSON, Rein, *"Jus ad Bellum: Plus ça Change (Le Monde) Plus C'est L Même Chose (Le Droit)?",* J. CONFLICT & SECURITY L., Vol. 7, 2002.

NYE, Joseph S., *"The Regime Complex for Managing Global Cyber Activities",* The Centre for International Governance; Global Commission on Internet Governance: Paper Series No. 1, 2014.

O'CONNEL, Mary, *"Cyber Security and International Law"*, Clatham Hause International Law: Meeting Summary, 29 May 2012.

OSTROM, Elinor. vd., Revisiting the Commons: Local Lessons, Global Challenges, Science, 1999.

OWENS William A./ DAM, Kenneth W./ LIN, Herbert S., Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities, The National Academies Press, Washington, 2009.

ÖZBEK, Veli Özer / KANBUR, M. Nihat / DOĞAN, Koray / BACAKSIZ, Pınar / TEPE, İlker; Ceza Muhakemesi Hukuku, Ankara, 2012.

ÖZDİLEK, Ali Osman, Uygulamadan Örnek Olaylarla Bilişim Suçları ve Hukuku, İstanbul, 2006.

ÖZEN, Muharrem / ÖZOCAK, Gürkan; "Adli Bilişim, Elektronik Deliller ve Bilgisayarlarda Arama ve El Koyma Tedbirinin Hukuki Rejimi (CMK m. 134)", Ankara Barosu Dergisi, S. 2015/1.

ÖZEN, Muharrem/BAŞTÜRK, İhsan, Bilişim – İnternet ve Ceza Hukuku, Ankara, 2011.

ÖZOCAK, Gürkan "*DDoS Saldırısı ve Failin Cezai Sorumluluğu*", Bilişim 2012 – 29. Uluslararası Bilişim Kurultayı Bildiriler Kitabı, Ankara, 2012.

ÖZOCAK, Gürkan, "*Penetrasyon Testlerinin (Pentestlerin) Hukuki Durumu ve Zararlı Yazılımlar*", http://www.bilisimdergisi.org.tr/yazarlar/konuk-yazarlar/penetrasyon-testlerinin-pentestlerin-hukuki-durumu-zararli-yazilimlar.html, (e.t. 02.04.2018).

ÖZOCAK, Gürkan; "*Ceza Muhakemesinde Elektronik Delillerin Tespiti ve Toplanması*", 2. Uluslararası Bilişim Hukuku Kurultayı Bildiriler Kitabı, İzmir, Kasım 2011.

ÖZTÜRK, Bahri / ERDEM, Mustafa Ruhan, Uygulamalı Ceza Muhakemesi Hukuku, 11. Baskı, Ankara, 2007.

PALOJARVI, Pia, *"A Battle in Bits and Bytes: Computer Network Attacks and the Law of Armed Conflict",* Erik Castrén Institute of International Law, Helsinki, 2009.

PAUST, Jordan J., "Use of Armed Force against Terrorists in Afghanistan, Iraq, and Beyond", Cornell International Law Journal, Vol. 35, No. 3, 2002.

RAYMOND Mark, *"Puncturing the Myth of the Internet as a Commons",* Georgetown Journal of Internet Affairs, Special Issue, 2013.

Remarks on the Department of Defense Cyber Strategy, As Delivered by Deputy Secretary of Defense William J. Lynn, III, 14 July 2011, http://archive.defense.gov/speeches /speech.aspx?speechid=1593 (e.t. 15.04.2018).

RID, Thomas, "*Cyber War Will Not Take Place",* Journal of Strategic Studies, Vol. 35, Iss. 1, 2012.

ROBERTSON, Horace B. Jr., "Self-Defense Against Computer Network Attack Under International Law", 76 INT'L L. STUD., Vol. 76, 2002.

ROSCINI, Marco, Cyber Operations and the Use of Force in International Law, Oxford University Press, the UK, 2014.

RYAN, Daniel J./DION, Maeve/ TIKK, Eneken/RYAN, Julie JCH, *"International Cyberlaw: A Normative Approach",* Georgetown Journal of International Law, Vol. 42, 2011.

SCHMIT, Michael, "*Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework*", COLUM. J. TRANSNAT'L L. Vol. 37, 1999.

SCHMITT, Michael/VIHUL, Liis (ed.), Tallinn Manual 2.0 On the International Law Applicable to Cyber Operations, Cambridge University Press, UK, 2017.

SCHMITT, Micheal: *"Pre-emtive Strategies in International Law",* Michigan Journal of International Law, Vol. 24, 2003.

SEAN, D. M., *"Terrorism and the Concept of "Armed Attack" in Article 51 ofthe UN. Charter"*, HARV. INT'L L.J., Vol. 43, 2002.

SHARP Sr, Walter Gary. *"The Past, Present, and Future of Cybersecurity*", Journal of National Security Law and Policy Vol. 4, 2010.

SHARP, Sr., Walter Gary, Cyberspace and the Use of Force, Aegeis Research Corporation, USA, 1999.

SINAR, Hasan, İnternet ve Ceza Hukuku, İstanbul, 2001.

SINGER, P.W. / FRIEDMAN, Allan, Cybersecurity and Cyberwar: What Everyone Needs to Know, NewYork, 2014.

SZABO, Kinga Tibori, *"Anticipatory Action in Self Defence Essence and Limits Under International Law",* Springer, The Netherlands, 2011.

TAŞDEMİR, Kubilay/ÖZKEPİR, Ramazan; Mala Karşı Suçlar, Ankara, 1993.

THOMAS, M. F., *"Terrorism and the Right of Self-Defense"*, AM. J. INT'L. L., Vol. 95, 2001.

TOROSLU, Nevzat; Ceza Hukuku Genel Kısım, Ankara, 2012.

TOURE, Hamadoun, *"The International Response to Cyberwar",* içinde The Quest for Cyber Peace (TOURE, Hamadoun), ITU, January 2011.

Van STEENBERGHE, R., *"Self-Defence in Response to Attacks by Non-State Actors in the Light of Recent State Practice: A Step Forward?",* LEIDEN J. INT'L L., Vol. 23, 2010.

WAXMAN, Matthew C., *"Cyber-Attacks and Use of Force: Back to the Future of Article 2(4)",* Yale Journal of International Law, Vol. 2, Iss. 2, 2011.

WEBER, Amalie: The Council of Europe's Convention on CyberCrime, Berkeley Technology Law Journal, Vol. 18, 2003.

WEBER, Rolf H., *"Elements of a Legal Framework for Cyber Space",* Swiss Review of International and European Law, Vol. 26, No. 2, 2016.

WEE YEN, Jean, *"The Use of Force Against Non-State Actors: Justifying and Delimiting the Exersice of the Right of Self-Defence",* Singapure Law Review, Juris Illuminae, Vol. 9, 2017.

WILMSHURST, Elizabeth, Principles of International Law on the Use of Force By States in Self-Defence, Clatham House Paper, ILP WP 05/01, 2005.

YAPICI, Utku: *"Uluslararası Hukukta Terörizme Karşı Kuvvet Kullanımı Sorunu",* Uluslararası Hukuk ve Politika, C. 2, No.7, 2006.

YAZICIOĞLU, Yılmaz; Kriminolojik, Sosyolojik ve Hukuki Boyutları İle Bilgisayar Suçları, İstanbul, 1997.

ZIOLKOWSKI, Katharina, *"General Principles of International Law as Applicable in Cyberspace",* in Peacetime Regime for State Activities in Cyberspace International Law, International Relations and Diplomacy NATO CCD COE Publication, Tallinn, 2013.

Belgeler

2002 National Security Strategy of the United States of America, https://www.state.gov/documents/organization/63562.pdf (e.t. 15.04.2018).

2006 National Security Strategy of the United States of America, https://www.state.gov/documents/organization/64884.pdf (e.t. 15.04.2018).

2010 National Security Strategy of the United States of America, http://www.whitehouse.gov/sites/default/files/rss_viewer/national_security_strategy.pdf, (e.t. 30.03.2018).

Comprehensive Study on Cyber Crime, Draft, United Nations, February 2013, s. xvii. https://www.unodc.org/documents/organizedcrime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf (e.t. 30.05.2018).

Council Framework Decision of 28 May 2001 combatting fraud and counterfeiting of non-cash means of payment, 2001/413/JHA, https://eur-lex.europa.eu/legalcontent/EN/TXT/PDF/?uri=CELEX:32001F0413&from=EN (e.t. 31.05.2018).

Directive 2002/58/EC of the European Parliment and of The Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector, https://eur-lex.europa.eu/legalcontent/EN/TXT/PDF/?uri=CELEX:32002L0058&from=EN (e.t. 31.05.2018).

Directive 2011/92/EU of the Europen Parliament and of the Council of 13 December 2011 on combating the sexual abuse and sexual explotitation of children and child pronography and replacing Council Framework Decision 2004/68/JHA, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32011L0093&from=EN (e.t. 31.05.2018).

Diretive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on Attacks Against Information Systems and Replacing Council Framework Decision 2005/222/JHA, https://eur-lex.europa.eu/legalcontent/EN/TXT/PDF/?uri=CELEX:32013L00 40&from=EN (e.t. 31.05.2018).

Draft Convention on International Information Security (Concept), 2011, http://www.mid.ru/en/foreign_policy/official_documents//asset_publisher/CptICkB6BZ29/content/id/191666 (e.t. 30.05.2018).

E-Gorvernment Interoperability Framework, https://www.itu.int/en/ITU-D/Projects/ITU-EC-ACP/ICB4PAC/Pages/default.aspx (e.t. 31.05.2018).

Group of Govermental Experts on Developments in the Field of Information and Telecommunicatipns in the Context of International Security, A/68/98, 24 June 2013, S. 7.

Group of Govermental Experts on Developments in the Field of Information and Telecommunicatipns in the Context of International Security, A/68/98, 24 June 2013.

Group of Govermental Experts on Developments in the Field of Information and Telecommunicatipns in the Context of International Security, A/70/174, 22 July 2015.

Harmonizing Cyberlaws and Regulations: The Experinece of the East African Community, UNCTAD/STICT/2012/4, United Nations, 2012, http://repository.eac.int:8080/bitstream/handle/11671/1815/EAC%20Framework%20for%20Cyberlaws.pdf?sequence=1&isAllowed=y (e.t. 30.05.2018).

High-Level Panel Report, UN Doc. A/59/565, 21 March 2005.

In Larger Freedom Raporu, UN Doc. A/59/2005, 21 March 2005.

In Larger Freedom: Towards Development, Security and Human Rights for All, Report of the UN Secretary-General, UN Doc A/59/2005, 21 March 2005.

Memorandum for Chefs of the Military Services Commanders of the Combatant Commands Directors of the Joınt Staff Directorates, Joint Terminology for Cyberspace Operations, bkz. http://www.nsci-va.org/CyberReferenceLib/2010-11joint%20Terminology%20for%20Cyber space%20Opera tions.pdf (e.t. 01.04.2018).

UN Doc. A/RES/29/3314, 14 December 1974

UN Doc. A/RES/53/70, 4 December1998.

UN Doc. A/RES/54/49, 1 December1999.

UN Doc. A/RES/55/28, 20 November 2000.

UN Doc. A/RES/56/19, 29 November 2001.

UN Doc. A/RES/57/53, 22 November 2002.

UN Doc. A/RES/58/32, 8 December 2003.

UN Doc. A/RES/59/61, 3 December 2004.

UN Doc. A/RES/60/45, 8 December 2005.

UN Doc. A/RES/61/54, 6 December 2006.

UN Doc. A/RES/62/17 5 December 2007.

UN Doc. A/RES/63/37, 2 December 2008.

UN Doc. A/RES/64/25, 2 December 2009.

UN Doc. A/RES/65/41, 8 December 2010.

UN Doc A/66/152, 15 July 2011.

UN Doc. A/RES/66/24, 2 December 2011.

UN Doc. A/RES/65/230, 21 December 2011.

UN Doc. A/RES/67/27, 3 December 2012

UN Doc. A/RES/68/243, 27 December 2013.

UN Doc. A/RES/69/28, 2 December 2014.

UN Doc. A/RES/70/237, 23 December 2015.

UN Doc. A/RES/ 71/28, 9 December 2016.

UNODC/CCPCJ/EG.4/2011/2, 21January 2011.

UNODC/CCPCJ/EG.4/2011/INF/2/Rev.1, 21 January 2011.

UNODC/CCPCJ/EG.4/2013/3, 1 March 2013.

Strategic Concept fort he Defence and Security of the Members of the North Atlantic Treaty Organization, Adopted by Heads of State and Governments at the NATO Summit in Lisbon, 19- 20 November 2010, https://www.nato.int/cps/ua/natohq/official_texts_68580.htm (e.t. 15. 04. 2018).

Working Paper on Recent Developments in the Use of Science and Technology by Offenders and by Competent Authorities in Fighting Crime, Including the Case of Cybercrime, 12- 19 April, 2010. http://www.unodc.org/documents/crime-congress/12thCrimeCongress/ Docu ments/A_CONF.213_9/V1050382 e.pdf (e.t. 31.05.2018).

Mahkeme Kararları

Armed Activities on the Territory of the Congo (Democratic Republic of the Congo v. Uganda), Judgement, I.C.J. Reports 2005.

Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory, Advisory Opinion, I.C.J. Reports 2004.

Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion, 8 July 1996, I.C.J. Reports 1996.

Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United Stataes of America), Judgement, I.C.J. Reports, 1986.

Linkler

http://blog.normaturk.com/some-nedir/ (e.t. 01.03.2018).

http://www.coe.int/en/web/conventions/full-list//conventions/treaty/189/ signatures?p_auth=n Otm1q80 (e. t.30.05.2018).

http://eng.sectsco.org/documents/ (e.t. 30.05.2018).

http://itlaw.wikia.com/wiki/Arab_Convention_on_Combating_Infor mation_ Technology_Offences (e.t. 30.05.2018).

http://thecommonwealth.org/sites/default/files/key_reform_pdfs/P15370_11 _ROL_ Model_Law_Computer_Related_Crime.pdf (e.t. 30.05.2018).

http://www.oecs.org/jobs/e-gov (e.t. 31.05.2018).

http://www.ohchr.org/EN/ProfessionalInterest/Pages/OPSCCRC.aspx (e.t. 30.05.2018).

http://www.udhb.gov.tr/doc/siberg/2016-2019guvenlik.pdf (e.t. 01.03.2018).

http://www.udhb.gov.tr/doc/siberg/Kurumsal_SOME_Reh_V1.pdf (e.t. 01.03.2018).

https://ec.europa.eu/growth/sectors/tourism/business-portal/understanding-legislation/legal-regulations-e-commerce_en (e.t. 31.05.2018).

https://www.coe.int/en/web/conventions/search-ontreaties/conventions/treaty/185/signatures? p_auth=kyheDJdz (et. 15.05.2018).

https://www.itu.int/en/ITUD/Cybersecurity/Documents/SADC%20Model%20Law%20Cybercrime.pdf (e.t. 31.05.2018).

https://www.itu.int/ITUD/projects/ITU_EC_ACP/hipcar/incountry_assistance/Grenada/HIPCARGrenada_Cybercrime_Report_Final_Draft_April2012.pdf (e.t.31.05.2018).

https://www.tbmm.gov.tr/komisyon/insanhaklari/pdf01/3-30.pdf (e.t.15.04.2018)

https://www.unodc.org/unodc/en/organized-crime/open-ended-intergovernmental-expertgrou p-meeting-on-cybercrime.html (e.t. 28.05.2018).

www.udhb.gov.tr/doc/siberg/Sektorel_SOME_Reh.docx (e.t. 01.03.2018).