BİLGİ TEKNOLOJİLERİ VE İLETİŞİM DERGİSİ (BTK DERGİ)
CİLT: 1 SAYI: 1 TARİH: TEMMUZ - EYLÜL 2023 ISSN: 2980-1311

BİLGİ VE İLETİŞİM TEKNOLOJİLERİNİN GELİŞMESİYLE DEĞİŞEN SİBER SUÇ TANIMI VE YAKLAŞIMLAR

Burak YAĞCI[1]

Özet

Bilgi ve iletişim teknolojilerinin günden güne gelişip değişmesiyle birlikte bireyler ve toplum açısından olumlu etkilerinin yanı sıra olumsuz etkileri de ortaya çıkmaktadır. Öyle ki suçlular için yeni bir faaliyet sahası oluşarak suça ilişkin yeni yöntemlerde ve suç çeşitliliğinde büyük bir artış söz konusu olmuştur. Kara, hava, deniz ve uzay ortamında meydana gelen klasik suç tiplerine ek olarak siber uzay adı verilen muğlak alanda meydana gelen suç tipleri, bilgi ve iletişim teknolojilerinin ilerlemesiyle farklı bir yöne evrilerek karmaşık bir yapıya ulaşmıştır. Bunun sonucunda siber suçların farklı teknolojilerle olan birleşiminde yeni dinamikler ortaya çıkmıştır. Öyle ki bu dinamikler devletlerin suça olan bakış açısını, mevzuatlarını ve buna ilişkin politikalarını değiştirmelerini gerekli kılmıştır. Bu ortamda karşılaşılan suçların uluslararası hukuk literatüründe kendisine henüz yer bulamadığı ve hukuki karşılığının olmadığı düşünüldüğünde, devletlerin karşılaştırmalı hukuk ve mütekabiliyet açısından yeknesak ve ortak bir siber suç tanımına sahip olması önem kazanmaktadır. Bu çalışmada siber suçun tanımı üzerine ulusal ve uluslararası literatür taranarak söz konusu alanda yer alan hukuki ve teknik boşluğun doldurulması amacıyla Birleşmiş Milletler (BM) nezdinde halihazırda çalışmaları devam eden taslak sözleşme çalışması detaylı şekilde incelenmiştir. Bu çerçevede literatür taramasıyla bilgi ve iletişim teknolojilerinin gelişmesi doğrultusunda devletlerin siber suça olan yaklaşımları ele alınmış, siber suçun değişen tanımına ilişkin hususlara değinilmiştir.

Anahtar Kelimeler: *siber suç, bilişim suçları, bilgi ve iletişim teknolojileri, siber güvenlik, siber uzay*

[1] Bilgi Teknolojileri ve İletişim Kurumu, burak.yagci@btk.gov.tr, ORCİD: 0009-0003-9787-8791

BİLGİ TEKNOLOJİLERİ VE İLETİŞİM DERGİSİ (BTK DERGİ)
CİLT: 1 SAYI: 1 TARİH: TEMMUZ - EYLÜL 2023

DEFINITION AND APPROACHES OF CYBERCRIME CHANGING WITH THE DEVELOPMENT OF INFORMATION AND COMMUNICATION TECHNOLOGIES

Abstract

As a fast evolving technology, ICTs (Information and Communication Technologies) generated benefits as well as drawbacks for individuals and society. Thus, a new field of activity has been created for criminals, and there has been a tremendous increase in new methods and crime diversity. In addition to the conventional types of crimes that occur in land, air, sea and space environments, the types of crimes that occur in the area called cyberspace have evolved into a different direction with the advancement of information and communication technologies and reached a complex structure. New dynamics, therefore, have emerged in the combination of cybercrime with different technologies. These dynamics made it necessary for states to change their perspective on crime, their legislation and their policies. Considering that the crimes encountered in this environment have not yet found a place in the international law literature and have no legal equivalent, it has become important for states to have a uniform and common definition of cybercrime in terms of comparative law and reciprocity. In this study, the national and international literature on the definition of cybercrime has been reviewed and the draft contract, which is currently in progress at the United Nations, has been examined in detail in order to fill the gap in this field. In this context, with the literature review, the approaches of states to cybercrime in line with the development of information and communication technologies were discussed and the issues related to the changing definition of cybercrime were mentioned.

Keywords: *cybercrime, ICT crime, informatıon and communication technologies, cyber security, cyberspace.*

GİRİŞ

Siber uzayın ülkesel sınırları aşan, özerk ve suç işlenmesini kolaylaştıran yapısı itibariyle bu alanda işlenen siber suçlar günden güne artış göstermektedir (AAG IT Services, 2023). Özellikle uluslararası mevzuat eksikliği ve cezai yaptırımlara ilişkin belirsizlikler siber suç faillerinin suç işleme motivasyonunu artırarak siber suç sayısındaki artışı etkilemiştir. Öyle ki bu faillerin siber alanın muğlaklığından faydalanmasıyla internet ortamındaki kullanıcıların hak kayıpları ve menfaat ihlalleri oluşmaya başlamıştır. Bunun yanı sıra kullanıcıların maddi ve manevi zararına neden olan siber tehditlerle, olumsuz sonuçların oluşturulmasına zemin hazırlanmıştır. Kullanıcıların bireysel olarak uğradığı zararlar sonrası devletler, söz konusu alanda vatandaşlarını korumak ve suçluları yakalayarak cezai yaptırıma tabi tutmak üzere koruyucu bir rol üstlenmek durumunda kalmıştır. Devletlerin hukuki sorumluluk alanında klasik suçlara ilişkin uyguladıkları yerel ve uluslararası mevzuatlar siber suçlara uygulanırken büyük sorunlarla karşılaşılmaktadır. Siyasi ve coğrafi sınırları aşan yapıdaki siber suçların faillerinin soruşturma ve kovuşturmaya tabi tutulması uluslararası alanda ortak bir mevzuat, siber suç tanımı ve müşterek yaklaşımı gerekli kılmıştır. Ancak devletlerin suça yaklaşımındaki farklılıklar müşterek bir uygulama tekniğinin önüne geçmektedir. Buradaki problem devletlerin diğer devletlerce suç sayılan hukuka aykırı fiilleri suç olarak tanımlamamış olmasından kaynaklanmaktadır. Devletler arası siyasi kutuplaşmalar ve ulusal politikaya bağlı oluşan fikir ayrılıkları, siber suçun tüm devletler tarafından kabul edilen küresel bir tanımının ve bu tanım etrafında oluşacak keskin bir çerçevesinin çizilmesine engel olmaktadır. Diğer taraftan gelişen teknolojilerin cezai suçların ölçeği, hızı ve kapsamı üzerindeki etkisi dikkate alındığında siber suçun hangi çerçevede ele alınacağı problemi ortaya çıkmaktadır. Devletlerin siber suça ilişkin yaptıkları tanımlamalar ulusal mevzuatlarındaki lafzi ve kanuni yorumları etkileyerek uygulamada farklılıklara yol açmaktadır. Söz konusu farklılıklar, birden fazla devleti etkileyen müşterek olaylarda siber suçun mülki sınırlara sığmayan yapısı itibariyle hukuki ve siyasi ihtilafların ortaya çıkmasına yol açmaktadır. Bu kapsamda siber suça ilişkin toplumu korumayı amaçlayan ve uluslararası iş birliğini destekleyen ortak bir siber suç tanımı ve politikasının oluşturulması önem arz etmektedir. Öyle ki ulusal ve uluslararası mevzuatlar çerçevesinde devletlerin karşılıklı olarak siber suça yaklaşımlarının aynı eksende olması, bu suçların faillerinin yakalanarak cezai yaptırım uygulan-

masına hizmet edecektir. Cezai yaptırım, suçluların iadesi, teknik yardım ve adli yardım gibi alanlarda devletler arası iş birliğinin hayata geçirilmesi söz konusu ortamda siber suça ilişkin ortak bir tanım üzerinde uzlaşılmasını sağlayacaktır.

Bu çalışmada siber uzay içerisinde işlenen siber saldırılar ve onların yol açtığı siber suçlara ilişkin tanımsal literatür ortaya koyularak siber suçların gelişen ve değişen teknolojilerle birlikte hangi kapsamda yorumlanması gerektiğine dair bir değerlendirme ortaya konulacaktır. Çalışmanın ilk bölümünde siber uzay ve siber suç kavramlarına dair ilgili akademik yazın ele alınacaktır. İkinci bölümde Türkiye'de siber suça olan yaklaşımlar üzerinde durulurken, üçüncü bölümde kavramın küresel ölçekte nasıl ele alındığına dair yaklaşımlara yer verilecektir. Dördüncü bölümde çalışmaları hala devam eden "Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes (Bilgi ve İletişim Teknolojilerinin Suç Amaçlı Kullanımıyla Mücadele Konusunda Kapsamlı Uluslararası Sözleşme)" isimli taslak çalışma detaylı şekilde incelenecektir. Son bölümde ise çalışmanın sonuçları tartışılarak çözüm önerilerine yer verilecektir.

I. SİBER SUÇ VE SİBER UZAY

Siber suç ifadesinin tam olarak anlaşılabilmesi, bu ifadeyi oluşturan terimlerin analiz edilmesi ile doğrudan bağlantılıdır. Siber ile suçun kesişimi zamanla gelişerek değişime uğrayan bilgi ve iletişim teknolojileri vasıtasıyla olmuştur. Bu kesişim yeni bir terim olan siber suçu ortaya çıkarmıştır. Suç terimi "törelere, ahlak kurallarına hukuki olarak da yasalara aykırı davranış, cürüm" şeklinde tanımlanmıştır (Türk Dil Kurumu, 2023). Bu tanımdan görüleceği üzere hem kanunda suç sayılan fiiller hem de toplum nezdinde suç olarak kabul edilen eylemler suç tanımına girebilmektedir. Ancak kanunsuz suç ve ceza olmaz ilkesi gereğince (kanunilik ilkesi) bu çalışmada kanunda suç sayılan ve uluslararası sözleşmelerde geçen siber suçlar üzerinden bir inceleme yapılacaktır. Diğer taraftan siber terimi ise BM tarafından yapılan tanımda "internete bağlı bilgisayarların, iletişim altyapılarının, çevrim içi iletişim yapan kişilerin, veri tabanı ve bilgi sistem araçlarının oluşturduğu küresel bir sistem" olarak ifade edilmiştir (Andress ve Winterfeld, 2013). Siber terimi bu tanıma göre bilgi ve iletişim ağlarını hatta internet kullanıcılarını da kapsayan genel bir kavram olarak ortaya çıkmaktadır. Siber suçlara ilişkin dünya üzerinde birçok farklı tanım yapılmış ancak çeşitli sebeplerle

ortak bir tanıma ulaşılamamıştır. Siber suç tanımının kesin ve yeknesak şekilde yapılamamasında belirleyici faktörler, siber uzayın genişliği ve siber suçlarla ilgili kriminolojik çalışmaların yetersizliğidir (Holt ve Bossler, 2020, s. 5-13). Siber uzay ya da diğer bir deyişle siber uzam, yapısı gereği fiziksel olmayan ve coğrafi olarak sınırları bulunmayan bir alandır. Lasky tarafından yapılan tanımda siber uzay "bilgisayarlar, bilgisayar ağları, internet ve internet ağına dahil diğer cihazlar ile bileşenler arasındaki bağlantıların neticesinde ortaya çıkan, teorik olarak var olan ve fiziksel bir şekli olmayan alan" şeklinde ifade edilmiştir (Lasky, 2022). Bu tanımdan hareketle siber uzayın geniş yapısı içerisinde birçok farklı teknolojinin kapsam dahilinde olduğu, ağa bağlanabilen cihazların internet ve internet ortamındaki içeriklerle ilişkili olarak çeşitli suçların işlenilmesinde araç olarak kullanılabileceği değerlendirilmektedir. Siber uzayın genişliğinden anlaşılması gereken bir diğer husus ise suç işlemek için esnek bir zaman aralığına sahip olunması ve faillerin bu alanda hareket edebilme kabiliyetlerinin yüksek olmasıdır. Siber suçlara ilişkin faaliyetlerde bulunan kişiler, kendilerini bu uzam içerisinde rahatlıkla gizleyerek devletlerin kolluk kuvvetlerinden ve siber güvenlikle ilgili otoritelerinden kaçabilmektedir.

Siber suça ilişkin literatürde birçok farklı tanım olmasına rağmen en sık karşılaşılan tanım "On The Definition And Classification Of Cybercrime" isimli makalelerinde Gordon ve Ford tarafından yapılan "bilgisayar veya bilgisayar ağları ve donanımları kullanılarak işlenen suç" şeklindedir. Bu ikili yaptıkları tanımı diğer yapılan tanımlamalardan ayrı tutarak kavramsal bir tabana oturtmak istemişlerdir. Siber suçlara ilişkin bir sınıflandırma yaparak iki tip siber suç üzerinden incelemelerde bulunmuşlardır. Bu sınıflandırmada belirleyici unsur, suçun oluşmasında ana faktörün insan etkisini içermesi ya da insan etkisinden uzak şekilde yazılımsal kodlar olmasındaki farklılıktır. Birinci tip suçları, siber suç tanımının insan unsurunu ön planda tuttuğu ve suçun oluşmasında insan faaliyetlerinin yeterli olduğu siber suçlar oluşturmaktadır. Bunlara ilişkin sosyal mühendislik faaliyetleri ve oltalama (phishing) gibi siber saldırı türleri örnek olarak verilebilecektir. İkinci tip siber suçları ise virüs, solucan veya kötücül yazılım saldırıları gibi yazılımsal kodlamaların söz konusu saldırılarda araç olarak kullanıldığı suçlar meydana getirmektedir (Gordon ve Ford, 2006, s. 13-20). Bu kapsamda değerlendirme yapıldığında farklı kategorilere ayrılan siber suçlara ilişkin yaklaşım farklılıklarının olduğu görülecektir. Kavramsal olarak beşeri veya yapay unsurlar

siber suç sınıflandırmasında etkili olmuştur. Bunun yanı sıra siber suçlarla ilgili tanımlar arasında mihenk taşı olarak kabul edilen Thomas ve Loader tarafından yapılan tanıma göre siber suç "yasa dışı olan veya belirli taraflarca yasa dışı kabul edilen ve küresel elektronik ağlar aracılığıyla gerçekleştirilebilen bilgisayar aracılı faaliyetler" şeklinde yorumlanmıştır (Thomas ve Loader, 2000). Burada meşru olmayan davranışlar söz konusu olmakla birlikte bunların yazılı veya yazısız hukuk kurallarının ihlal edilmesine yönelik bir ayrımı getirmediği görülmektedir. Öyle ki söz konusu tanımda belirli kesimlerce yasa dışı kabul edilen ifadesi toplumsal normları ifade etmektedir. Bir diğer dikkat edilecek nokta ise küresel ağlar kullanılarak yapılan ve araç olarak bilgisayarın kullanıldığı saldırıların bulunmasıdır. Burada araç bazlı yaklaşım ön planda tutularak bilgisayarın amaç olarak kullanıldığı veya bir geçiş vasıtası şeklinde yararlanıldığı diğer kategoriler tasnif dışı bırakılmıştır (Thomas ve Loader, 2000). Siber suçlara ilişkin bir diğer tanım da Brenner tarafından *"klasik suçtan farklı olarak siber ortamda bilgisayar sistemleriyle gerçekleştirilen suçlar"* şeklinde ifade edilmiştir. Brenner, klasik suç tipleri ile bilgisayar ortamında işlenen suç ayrımından yola çıkarak bir tanımlamada bulunmuştur. Bunun yanı sıra siber suçların kamu düzenini tehdit altına alan saldırılar vasıtasıyla işlenmesinden dolayı meşru olmayan davranışlar bütünü olduğunu dile getirmiştir. Geleneksel şekilde işlenen suçların bir dönüşüm içerisinde siber suçlara evrildiğini belirterek söz konusu bağlamın siber uzay olduğunu vurgulamıştır. Bu tanım etrafında siber suçlar üç farklı kategoride incelenmiştir. Bunların ilkini araç olarak bilgisayarın kullanımı oluşturmaktadır. Siber suçlar bilgisayarlar aracılığıyla gizlilik ön planda tutularak işlenebilmektedir. İkinci kategoride suçun işlenilmesinde bilgisayarın doğrudan değil dolaylı olarak tesadüfi şekilde etkisi olabileceğini değerlendirmiştir. Son kategoride ise bilgisayar hedef alınarak yapılan saldırılar kapsamında sınıflandırma yapılmıştır (Brenner, 2010, s.115). Brenner tarafından yapılan sınıflandırma bu çalışmanın uluslararası sözleşme çalışmaları kısmında incelenen taslak sözleşmede tartışma konusu olan sibere bağımlı suç *(cyber dependant),* siberle kolaylaşan *(cyber enabled)* veya siberle ilgili *(cyber related)* suçlar ayrımının kaynağını da oluşturmaktadır.

Siber suça ilişkin devletlerin genel olarak yaklaşımları da sibere bağımlı ve siberle kolaylaşan suçlar şeklindeki ayrım çerçevesinde ele alınmaktadır. Buna ilişkin devlet örneklerine bakıldığında Singapur Polis Gücü (SPF) ve Singapur Siber Güvenlik Ajansı tarafından yapılan ayrım önemli bir emsal teşkil etmekte-

dir. Öyle ki Singapur'da bu iki büyük güvenlik otoritesi siber suçları ikiye ayırarak belirgin bir ayrım yapmışlardır. İlk suç tipi olan sibere bağımlı suçlar kategorisinde, bilgisayar korsanlığı ve fidye yazılımı gibi siber saldırı türlerinin olduğu bilgisayarın hedef alındığı suçlar bulunmaktadır. Siberle kolaylaşan suç tipinde ise bilgisayarın araç olarak kullanıldığı çevrim içi dolandırıcılık, çevrim içi taciz, siber gasp ve diğer çevrim içi suçların olduğu siber özellikli suçlar yer almaktadır (SPF, 2023). Yine bunun gibi İngiltere tarafından benzer bir ayrım yapılarak siber suçlar kategorize edilmiştir. İlk tipteki suçlar, sadece çevrim içi cihazların kullanılması yoluyla işlenebilen ve bu cihazların hem suçun işlenmesinde araç hem de suçun hedefi konumunda olduğu suçlardır. İkinci tipteki suçları ise bilgisayar kullanılarak ölçeği artırılabilen geleneksel suçlar oluşturmaktadır. Söz konusu siber suçların içeriğinde bilgisayar korsanlığı, *dark web (*karanlık ağ), sosyal medyada *trolleme*, kimlik avı ve kimlik hırsızlığı, dağıtılmış hizmet reddi (DDOS) saldırıları, çevrim içi tehdit ve taciz, cinsel görüntülerin izinsiz ifşası gibi suçlar bulunmaktadır (The Crown Prosecution Service, 2022). Diğer taraftan siber güvenlikle ilgili hususlarda dünyada öncü olarak gösterilen Amerika Birleşik Devleti'nin (ABD) teknoloji ve standart enstitüsü olarak görev yapan National Institute of Standards and Technology (NIST) tarafından yapılan tanım "internet üzerinden veya bilgisayar teknolojisinin kullanılmasıyla işlenen suçlar" şeklindedir. Söz konusu suçlar ağ üzerinde de rahatlıkla işlenebilen suçlar olması nedeniyle tanımda internet vurgusu da yapılmaktadır. (NIST, 2023) Yine ABD'de federal bir kurum olarak görev yapan U.S Department of Justice (ABD Adalet Bakanlığı) nezdinde bilgisayar suçlarına ve siber suça ilişkin yaklaşım geniş bir perspektiften bakış açısı sağlamaktadır. Bakanlık nezdinde yapılan tanım "suçlanması, soruşturulması veya kovuşturulması için bilgisayar teknolojisi bilgisini içeren her türlü ceza hukuku ihlali" şeklindedir. Söz konusu tanım etrafında yapılan sınıflandırmada ilk olarak bilgisayarın suçun nesnesi konumunda olduğu, donanım ve yazılımlarının çalınması ifade edilmektedir. İkinci sınıfta bilgisayarın suçun maddesi konumunda olduğu bilgisayarlar ve sunucuları aracılığıyla mümkün kılınan meşru hizmet ve faaliyetlere kötücül şekilde müdahalelere ilişkin her türlü girişim ifade edilir. Son sınıfta ise bilgisayar bağlantılı suçlar bulunmaktadır. Burada klasik suçların işlenişinde bilgisayarın sağladığı kolaylıkla vasıta olarak kullanılması esas alınmaktadır (US Department Justice Office, 2023). Görüldüğü üzere siber güvenlik konusunda dünyada öncü olan devletler tarafından klasik siber suça yaklaşım içeren sibere bağımlı suçlar *(cyber dependant)* bir kenara bırakılarak

gelişen teknolojiyle farklı şekillerde ortaya çıkan suç tiplerini barındıran siberle kolaylaşan *(cyber enabled)* ve siberle ilgili *(cyber related)* siber suç tanımları tercih edilmektedir.

II. TÜRKİYE'DE SİBER SUÇA YAKLAŞIM

Ülkemizde siber suçlara ilişkin farklı tanımlar yapılmış olmakla birlikte, resmi olarak en son yapılan tanımlardan birisine 2020-2023 Ulusal Siber Güvenlik Strateji ve Eylem Planı'nda yer verilmiştir. Planın *"Tanımlar" kısmında siber suç; "bir bilişim sisteminin güvenliğini ve/veya buna bağlı verileri ve/veya kullanıcısını hedef alan ve bilişim sistemi kullanılarak işlenen suçlar"* olarak nitelendirilmiştir (Ulaştırma ve Altyapı Bakanlığı, 2023). Söz konusu tanım siber suça ilişkin Ülkemizin bakış açısını ve stratejik hedeflerini ortaya koymaktadır. Ulusal literatürde Emniyet Genel Müdürlüğü Siber Suçlarla Mücadele Daire Başkanlığı bünyesinde oluşturulan "SiberAy" tarafından yapılan tanıma göre siber suç; "bilişim sistemlerinin gizlilik, bütünlük veya erişilebilirliğini ortadan kaldırmak amacıyla, siber uzay kaynaklı olarak çeşitli tehdit odaklarından gelen ve kanunlara göre suç kabul edilen eylemler" şeklindedir (Emniyet Genel Müdürlüğü, 2023).

Diğer taraftan, 5237 sayılı Türk Ceza Kanunu'nda (TCK) bilişim suçları düzenlenmekle birlikte resmi olmayan ikili bir ayrıma gidildiği söylenebilir. Bu ayrım Yargıtay içtihatlarında sıklıkla yer almakla birlikte uygulamada da teamül haline gelmiştir. Ayrımda bilişim suçlarına ilişkin fiillerin doğrudan ve dolaylı olarak işlenebilecek yapıda olması etkili olmuştur. Suçun ağırlaştırıcı unsuru konumunda bulunan ve suçun işleniş şeklini değiştiren durumlarda dolaylı bilişim suçlarından bahsedilebilir. İnternet ortamında bir kişiye karşı hakarette bulunmak fiziksel olarak da işlenebilen bir suç iken sanal ortamın getirdiği kolaylıktan yararlanılarak yapılan hakaret fiili dolaylı bilişim suçuna girmektedir. Söz konusu fiil sadece bilgisayar vasıtasıyla değil diğer teknolojik aygıtlar sayesinde de işlenebilmektedir. Bu yüzden klasik olarak kullanılan "bilgisayar suçları" ifadesi yerine "bilişim suçu" ifadesi ulusal mevzuatımızda tercih edilmektedir. TCK'nın üçüncü kısım onuncu bölümünde düzenlenen "Bilişim Alanında Suçlar", mezkûr Kanun'un 243, 244 ve 245. maddelerinde yer verilen bilişim suçları ile detaylandırılmıştır. 243.maddede "Bilişim Sistemine Girme (Yetkisiz Erişim) Suçu", 243. maddenin dördüncü fıkrasında "Sisteme Girmeksizin Verileri İzleme Suçu", 244. maddede "Bilişim Sistemine ve Verilere Müdahale Suçu", 245/A'da "Yasak Cihaz

veya Programlar", yine 245. maddede "Banka veya Kredi Kartlarının Kötüye Kullanılması" düzenlenmektedir (Türk Ceza Kanunu, 2004). Bu maddelerde suçun gerçekleştiği ortam olarak yer verilen bağlam bilişim sistemleridir.

Siber suçlara ilişkin ulusal mevzuatımızda 5237 sayılı TCK'da bilişim suçları başlığı altındaki suçlara ek olarak, bilişim sistemleri kullanılarak işlenen suçlara Kanun'un "Mal varlığına Karşı Suçlar" kısmında da yer verilmiştir. TCK'nın 142. maddesinde "Bilişim Sistemlerinin Kullanılması Suretiyle Hırsızlık" suçu tarif edilmiştir. Buna benzer olarak yine 158.maddede "Bilişim Sistemlerinin Araç Olarak Kullanılması Suretiyle Dolandırıcılık" düzenlenmektedir. TCK'nın 132 ile 138. maddeleri arasında "Özel Hayata ve Hayatın Gizliliğine Karşı Suçlar" kısmında "Haberleşmenin Gizliliğini İhlal", "Kişiler Arasındaki Konuşmaların Dinlenmesi ve Kayda Alınması", "Özel Hayatın Gizliliğini İhlal", "Kişisel Verilerin Kaydedilmesi", "Verileri Hukuka Aykırı Olarak Verme veya Ele Geçirme", "Verileri Yok Etmeme" suçlarına yer verilmiştir. Sayılan suçlar bilişim suçları olarak nitelendirilerek yapıları itibariyle siber suçlar kategorisindedir. Özellikle de 135 ile 138. maddeler arasında düzenlenen kişisel verilerin korunmasına ilişkin hükümler, siber saldırı sırasında bilgisayar veya bilişim sistemlerindeki kişisel verilerin hukuka aykırı olarak ele geçirilmesi veya kullanılması gibi suç oluşturan fiillerin işlenmesinde gündeme gelecektir. TCK'nın 124 ve 125. maddelerinde "Haberleşmenin Engellenmesi" ve "Hakaret" suçları bilişim suçu olarak siber suç kategorisinde sayılmıştır. İlaveten, TCK'nın 286. maddesinde "Adliyeye Karşı Suçlar" kısmında "Ses veya Görüntülerin Kayda Alınması" suç tanımına yer verilmiştir (Türk Ceza Kanunu, 2004).

Bu kanun dışında 5846 sayılı Fikir ve Sanat Eserleri Kanunu'nda yer alan siber suçlar 71 ve 72. maddelerde "Manevi, Mali ve Bağlantılı Haklara Tecavüz" ile "Koruyucu Programları Etkisiz Kılmaya Yönelik Hazırlık Hareketleri" şeklinde düzenlenmiştir (Fikir ve Sanat Eserleri Kanunu, 1951). Usul hukuku kapsamında 5271 sayılı Ceza Muhakemeleri Kanunu'nun (CMK) 134 ve 135. maddelerinde de yine bu alanda düzenlemede bulunulmuştur. Söz konusu maddelerde "Bilgisayarlarda, bilgisayar programlarında ve kütüklerinde arama, kopyalama ve el koyma" ile "İletişimin tespiti, dinlenmesi ve kayda alınması" başlıkları altında gerekli düzenlemeler yapılmıştır (CMK, 2004). İnternet Ortamında Yapılan Yayınların Düzenlenmesi Ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun'da (5651 sayılı Kanun) da yine bilişim suçlarına ilişkin hükümlere

yer verilmiştir. Bu Kanun'da içerik sağlayıcı, yer sağlayıcı, erişim sağlayıcı, toplu kullanım sağlayıcı ve sosyal ağ sağlayıcı gibi kavramlar üzerinde durularak uygulamaya yönelik olarak "içeriğin çıkarılması ve erişimin engellenmesi" düzenlenmiştir. Diğer taraftan bahsi geçen Kanunun 10. maddesinin altıncı fıkrasında Bilgi Teknolojileri ve İletişim Kurumu'nun (BTK) görevleri arasında siber saldırılara ilişkin tespit fonksiyonunun yerine getirilmesinde yukarıda sayılan internet süjeleri ile bağlantı kurarak kullanıcı mağduriyetlerinin giderilmesi konusunda koordinasyon ve gerekli tedbirlerin alınması hususu düzenlenmiştir (5651 Sayılı Kanun, 2007). Söz konusu yasada yer verilen ve sorumlu tutulan internet özneleri 2001 tarihli Avrupa Konseyi Siber Suçlar Sözleşmesi'nin (Budapeşte Sözleşmesi) 1. maddesinde yer verilen hizmet sağlayıcı tanımı içerisinde kendine karşılık bulabilmektedir. Öyle ki bu Sözleşme'de hizmet sağlayıcı "kamu veya özel tüzel kişilerinin dışında iletişim hizmeti sunan tüzel kişiler adına veya böyle bir hizmetin kullanıcıları adına bilgisayar verisini işleyen ve depolayan her türlü kişilik" olarak nitelendirilmiştir. Bu tanıma uyarlandığında 5651 sayılı Kanun'un internet özneleri olarak yukarıda sayılan sağlayıcıların da Sözleşme kapsamında hizmet sağlayıcı olarak kabul edilmesi mümkündür (Akpek, 2015, s. 64-65). 5651 Sayılı Kanun'da yer verilen maddelere bakıldığında söz konusu internet süjelerinin siber suçlarla bağlı bir ilişkisinin olduğu görülmektedir. Avrupa Konseyi Siber Suçlar Sözleşmesi kapsamında hizmet sağlayıcı olarak karşılık bulan bu süjeler yerel mevzuatlarda da yer almaktadır. Suçların sadece siber saldırı yöntemleri değil aynı zamanda hukuka aykırı içerik oluşturma, hukuka aykırı erişim, sosyal ağlar yoluyla işlenen suçları da içermesi nedeniyle söz konusu hükümlerin de işlerlik kazandığı bir kapsam alanı oluşmaktadır. Bu kapsamda söz konusu süjeler etkiledikleri alanlar çerçevesinde sadece sibere dayalı olan klasik suç türlerini değil aynı zamanda siberle alakalı olan ve siberin kolaylaştırdığı suç tiplerini de içerisine almaktadır. Özellikle de TCK kapsamında bilişim suçları olarak Kanun'un üçüncü kısım onuncu bölümünde düzenlenen suç tipleri "bilişim sistemleri" ifadesiyle bilgisayar sistemlerini de içerisine almaktadır. Söz konusu siber suçların kapsamına aldığı hususlara bakıldığında bilgisayar ve bilgisayar teknolojilerinin araç ve amaç olarak kullanımı asli önem arz etmektedir. Siber suçlar bu teknolojiler vasıtasıyla işlenebileceği gibi bu teknolojilere karşı da işlenebilmektedir. Diğer taraftan söz konusu teknolojilerin kullanımı suçların işlenmesinde önemli bir işlevsellik görerek farklı suçların oluşmasına yol açabilmektedir (Smith, Grabosky ve Urbas, 2004, s. 5-7). Söz konusu farklılıklar tanımlamaların da dar veya geniş

yorumlanarak değişik şekillerde ifade edilmesine sebebiyet vermektedir. Bu çerçeveden bakıldığında oluşturulan tanımlarda dar yorumlu tanımıyla siber suç; "bilişim sistemlerine, verilerine, gizliliğine, bütünlüğüne ya da sistemlerin veya verilerin fonksiyonuna karşı işlenen suçlar" iken geniş yorumlu olan tanımı "bilişim sistemleri ya da verileri aracılığıyla, bilişim sistemlerine veya verilerine karşı işlenen her çeşit suçlar" şeklinde ifade edilebilecektir (Aldoori, 2020, s. 20-21).

5070 sayılı Elektronik İmza Kanunu (EİK) kapsamında da adli ve idari suçlar şeklinde düzenlemeler bulunmaktadır. EİK'nın 16. maddesi elektronik imzaların kullanımına dair imza sahiplerinin rızasını şart koşmaktadır. Öyle ki bu madde kapsamında rıza dışı imzaya ait bilgiye veya imza oluşturma aracına erişim adli para cezası ile cezalandırılmıştır. Bunun yanı sıra imzaya ilişkin bilgiyi veren, kopyalayan ve uygunsuz şekilde e-imzayı tekrar oluşturanlar da aynı cezaya tabi olmaktadır. EİK'nın 17. maddesinde elektronik sertifikada sahtekârlık düzenlenerek söz konusu e-sertifikaları oluşturan, taklit eden, tahrif eden, haberi olmasına rağmen kullanan kişiler hapis ve adli para cezası ile cezalandırılacağı düzenleme altına alınmıştır. Aynı Kanun'un 18. maddesi kapsamında e-sertifika hizmet sağlayıcılarının yükümlülüklerini yerine getirmemesi durumunda idari para cezası öngörülmüştür. 19. maddede tüzel kişilere özgü güvenlik tedbiri düzenlenmekle birlikte gerekli şartların sağlanması durumunda tüzel kişiliğin etkinliğine ilişkin iznin iptali söz konusu olabilmektedir (Elektronik İmza Kanunu, 2004).

Bununla birlikte, yapılan ikincil düzenlemelerle siber suçların düzenlendiği kanunlar desteklenmektedir. Öyle ki siber suçlara karşı mücadele hususunda siber güvenliğin sağlanması büyük önem arz etmektedir. 5809 sayılı Elektronik Haberleşme Kanunu'nda (EHK) BTK'nın yetkileri ve idari yaptırımlara ilişkin icrai kuvveti hakkında bu Kanunun 60. maddesinde çeşitli hükümlere yer verilmiştir. Mezkûr maddenin on birinci fıkrasında "Kurum, kamu kurum ve kuruluşları ile gerçek ve tüzel kişilerin siber saldırılara karşı korunması ve bu saldırılara karşı caydırıcılık sağlamak için her türlü tedbiri alır veya aldırır" ifadesine yer verilmiştir. Yine aynı maddenin on ikinci fıkrasında BTK'nın bilgi ve belge taleplerinin herhangi bir gerekçeyle geri çevrilemeyeceği belirtilirken, on üçüncü fıkrada yükümlülüklerin yerine getirilmemesi durumunda idari yaptırım yetkisinin bulunduğu hüküm altına alınmıştır (EHK, 2008). BTK tarafından düzenlenen Elektronik Haberleşme Sektöründe Şebeke ve Bilgi Güvenliği Yönetmeliği bu alanda siber suçlara ilişkin düzenleme yapılan bir başka ikincil kaynak konumundadır.

Bu Yönetmelik'te siber suçların işlenmesinde araç olarak kullanılan bazı siber saldırı unsurları düzenleme içerisinde geçirilerek şebeke ve bilgi güvenliğinin sağlanmasına ilişkin işletmecilerin sağlamakla yükümlü oluğu hususlara yer verilmiştir. Yönetmeliğin 21. maddesinde şebeke güvenliğinin sağlanması amacıyla gerekli önlemlerin işletmeciler tarafından alınması yükümlülüğü getirilmiştir. Aynı Yönetmeliğin 35. maddesinde Dos/Ddos saldırıları, zararlı yazılımların yayılması ve benzeri siber saldırı yöntemlerine karşı korunmaya ilişkin yükümlülüklerden bahsedilmiştir. Diğer taraftan kritik altyapı sektörlerine ilişkin Enerji Piyasası Düzenleme Kurumu tarafından Enerji Sektöründe Kullanılan Endüstriyel Kontrol Sistemlerinde Bilişim Güvenliği Yönetmeliği ve Bankacılık Düzenleme ve Denetleme Kurumu tarafından Bankaların Bilgi Sistemleri ve Elektronik Bankacılık Hizmetleri Hakkında Yönetmelik bu alanda ikincil düzenlemelere örnek olarak verilebilecektir. Yine Sermaye Piyasası Kurumu tarafından çıkarılan Bilgi Sistemleri Yönetimi Tebliğleri ve farklı versiyonları da siber güvenliğin sağlanmasında ulusal literatürde yer alan düzenlemeler arasında yer almaktadır.

III. ULUSLARARASI KURULUŞLARIN SİBER SUÇA YAKLAŞIMLARI

Siber suç için uluslararası kuruluşlar tarafından yapılan çeşitli tanımlar siber suça olan yaklaşımın ortaya konulması açısından önem arz etmektedir. Ekonomik Kalkınma ve İş birliği Örgütü (OECD) tarafından yapılan siber suç tanımı "otomatik işleme tabi tutulan verilere karşı veya verileri nakil etme işlemlerinde yasaya, ahlaki değerlere aykırı veya yetkisiz bir şekilde gerçekleştirilen her türlü eylemler" şeklindedir (Çolak, 2016, s. 4). Söz konusu tanımdan anlaşılan suça ilişkin eylemlerin sadece yasayla belirlenen sınırlı alanla kalmadığı aynı zamanda etik değerlere ve toplum ahlakına yönelik saldırılar da içerdiğidir. Bunun yanı sıra verilerin nakil sürecine ilişkin hususlara da bu tanımda değinilmiştir. Öyle ki yasa dışı erişim sağlanan sistemler üzerinden verilere müdahale edilerek verilerin silinmesi, değişikliğe uğratılması ve kullanılamayacak hale gelmesine zemin hazırlanabilmektedir. Söz konusu ifade, ileride daha ayrıntılı şekilde değinilecek olan siberle kolaylaşan ve siberle ilgili suçların ulusal ve uluslararası metinlerde kendisine yer bulmasına hizmet edebilecek bir tanım konumunda bulunmaktadır. OECD tarafından 1996 yılında kurulan ve siber saldırılarla ilgili kriptolojik politikaları yürüten Committe on Information, Communications and Computer

Policy (ICCP) söz konusu alanda önemli bir komite görevindedir (ICCP, 2010). Bunun yanı sıra "OECD Policy Guidance on Online Identity Theft" isimli rapor internette kimlik avı hırsızlığına ilişkin rapor siber saldırıların suça bakan yönüne ilişkin önemli bir kaynaktır (OECD, 2008).

Avrupa Konseyi nezdinde insan hakları ve suçların önlenmesine dair tedbirlere ilişkin yapılan birçok çalışmanın yanı sıra siber suçlar alanında da çeşitli sözleşme çalışmaları yapılmıştır. Bu kapsamda hazırlanan "Programme on Cybercrime" çerçevesinde küresel anlamda teknik ve hukuki destek sağlanmaktadır. İnternet ortamında işlenen suçların önlenmesine dair saik doğrultusunda 2005 yılında "The Convention on the Prevention of Terrorism" ile birlikte terörizmin önlenmesine dair çok önemli bir sözleşme oluşturulmuş ve bu çalışma tüm ülkelere bir atıf kaynağı teşkil etmiştir. 2007 yılında Konsey tarafından "The Lanzarote Convention" hazırlanarak internet ortamında çocukların cinsel istismarını konu edinen önemli bir sözleşme daha literatüre girmiştir. Bu kapsamda çocuk haklarının korunması ve çocukların çevrim içi yollarla suça karışmasını önlemek adına önemli bir adım atılmıştır (Council Of Europe, 2023). 2001 yılında siber suçlarla mücadele alanında tek bağlayıcı uluslararası belge olarak ortaya çıkan "Avrupa Konseyi Siber Suçlar Sözleşmesi" siber suçlarla ilgili hazırlanan mevzuatın temelini oluşturan sözleşme konumundadır. Söz konusu Sözleşme 2003 yılında kabul edilen bilgisayar sistemleri aracılığıyla işlenen ırkçılık suçlarına ilişkin ek protokol ile zenginleştirilmiştir. Avrupa Konseyi Siber Suçlar Sözleşmesi'nde yapılmış olan siber suç tanımına bakıldığında suçların tasnif edilerek tanıma işlendiği görülmektedir. Bu tanım dört kategorinin birleştirilmesiyle "bilgisayar veri ve sistemlerinin gizlilik, bütünlük ve erişilebilirliğine, dolandırıcılık ve sahteciliğe, çocuk pornografisine, telif ve benzeri haklara yönelik bilgisayarla ilgili her türlü kötü niyetli eylemler" olarak nitelendirilmiştir (Council Of Europe, 2001). Yine bu tanımda da OECD tarafından yapılan tanıma benzer olarak siber suçların klasik şekilde sibere dayalı suçlar etrafında sınırlanamayacağı aynı zamanda çocuk pornografisi, dolandırıcılık, sahtecilik ve fikri mülkiyet gibi geniş bir alanı da içine alan siberle ilgili ve siberin kolaylaştırdığı suç tiplerini kapsayan yapıda olması gerektiği anlaşılmaktadır. Diğer taraftan, söz konusu Sözleşmenin 2001 tarihli olması nedeniyle teknolojik gelişmelerin henüz zirveye ulaşmadığı, temel seviyede sadece bilgisayar üzerinden işlemlerin yapılabilir olduğu bir dönemde yürürlüğe girmesinden dolayı bilişim sistemleri ifadesi metinde kendine

yer bulamamıştır. Bu ifade yerine tanımlarda ve içerikte bilgisayar sistemi ifadesi kullanılmıştır. Bu da gelişen ve ilerleyen teknolojinin beraberinde getirdiği çeşitli cihazların karşılık bulabileceği daha kapsamlı bir ifadenin mevzuatlarda ve uluslararası sözleşme metinlerinde kendisine yer bulması ihtiyacını gerektirmiştir.

Interpol tarafından yapılan tanıma bakıldığında söz konusu alanda evrensel olarak bir niteleme yapılamayacağı görüşüne varılmıştır. Interpol, siber suçları ikili bir ayrıma tabi tutmaktadır. İlk siber suç tipi, yüksek teknoloji suçu olarak nitelenen ve teknolojinin gelişmesiyle yazılımsal olarak bilgisayarlara karşı işlenen suçlardır. İkinci tip siber suçları ise siber uzay bağlamında işlenen suçlar oluşturmaktadır (Lin ve Masys, 2018, s. 65-66). İkinci tip suçların OECD ve Interpol tanımlarına paralel şekilde daha geniş yorumlanarak siber suç tiplerinin sayıca artırıldığı gözlemlenmektedir. Tanımlamalarda farklı şekillerde ele alınan siber suç, bazı metinlerde bilgisayar ortamı ile sınırlandırılmış, bazı yerlerde ise bilişim sistemleri ile genişletilerek daha büyük çerçevede ele alınmıştır. Siber suç kavramı söz konusu tanımlardan anlaşılacağı üzere farklı yorumlamalara açık bir konumda bulunmaktadır. 2017'de Interpol tarafından hazırlanarak yayınlanan strateji siber suçlarla mücadelede siber saldırıları gerçekleştiren kişi veya grupların tespiti hakkında önemli bilgiler içermektedir. Dijital delillerin elde edilmesinden uluslararası iş birliğine kadar birçok farklı etken söz konusu strateji belgesinde yer almaktadır (Interpol, 2017).

Uluslararası Telekomünikasyon Birliği (ITU) tarafından yapılan siber suçlara ilişkin sınıflandırma dört kategori altında detaylandırılmıştır (ITU, 2009). Bunların ilki "bilgisayardaki veri ve sistemlerin gizliliğine, bütünlüğüne ve kullanılabilirliğine karşı işlenen suçlardır (yasa dışı erişim, verileri çalma, veriye müdahale vb.)". Bu kısımda klasik olarak siber suçların sibere bağımlı olarak işlendiği şekilde suçların tasnifi yöntemine gidilmiştir. İkinci kategori "bilgisayar ile ilgili suçlar (online kumar, kimlik hırsızlığı, ücret sahteciliği vb.)" kapsamında ayrıntılı şekilde düzenlenmiştir. Bu gruptaki suçlar da daha önce belirtildiği şekilde siberle ilişkili olarak nitelendirilebilir. Üçüncü kategoride "içerikle ilgili suçlar (ırkçılık, nefret söylemi, şiddeti övme, yanlış bilgi vb.)" düzenlenmiştir. Söz konusu kategorideki suçlar internet ortamında kolaylıkla işlenebilen, halkı kışkırtmaya yönelik fiillerle beraber seyredebilen bir yapıdadır. Öyle ki kimliğini gizleyerek internette dezenformasyon çalışmaları yapabilen birçok bot hesap bulunmakta hatta *deepfake* uygulamaları ile gerçekte söylenmemiş sözler, hedef alınan kişi-

lerin ağzından çıkar şekilde kurgulanabilmektedir. Son olarak "Telif hakkıyla ilgili suçlar (telif ve fikri mülkiyet haklarına saldırı)" dördüncü kategori olarak detaylandırılmıştır. Özellikle internet ortamında yayınların artmasıyla beraber fikri mülkiyet haklarını ihlal edecek nitelikte siber saldırılar meydana getirilebilmektedir (BTK, 2022, s. 24). ITU tarafından 2007 yılında siber suçlarla mücadele konusunda temel hedeflerin belirlendiği "Global Cybersecurity Agenda (GCA)" önemli bir strateji eylem planı konumundadır. GCA kapsamında siber suçlara yönelik teknik ve hukuki kapasitenin artırılması, iş birliği ve koordinasyonun sağlanması konuları üzerinde çalışmalar ve raporlar yayınlanmıştır (GCA, 2007).

Avrupa Birliği nezdinde 2013 yılında yayınlanan ve siber saldırılara karşı korunma, siber tehditlerin tespiti ve önlenmesi, siber dayanıklılık ve üye ülkelerdeki gerçek ve tüzel kişilerin güvenilir dijital teknolojilere ulaşmasını hedefleyen "The EU Cybersecurity Strategy" kapsamında yapılan siber suç tanımı "bilgisayarların ve bilgi sistemlerinin birincil araç ya da birincil hedef olarak nazara alındığı geniş bir yelpazede farklı suç faaliyetleri" şeklindedir. Burada hem bilgisayar hem bilgi sistemleri tanım kapsamına alınmıştır. Ayrıca araç ve hedef bazlı iki türlü yaklaşımın da mümkün olabileceği değerlendirilmiştir. Söz konusu strateji 2020 yılında geliştirilerek fiziksel ve kritik varlıkların siber dayanıklılık derecesinin artırılması hedeflenmiştir (European Commission, 2022). Diğer taraftan ağ ve bilgi sistemlerinin güvenliğine ilişkin kuralların toplandığı, kritik altyapı ve sistemlerin korunmasının amaçlandığı "Ağ ve Bilgi Sistemleri Direktifi" olarak Türkçeye çevrilen "The Directive On Security Of Network And Information Systems (NIS Directive)" 2020 yılı içinde "Directive On Measures For A High Common Level Of Cybersecurity Across The Union (NIS2 Directive)" ismiyle revize edilmiş, (AB) 2022/2555 sayılı karar ile onaylanarak 16 Ocak 2023 tarihinde yürürlüğe girmiştir (European Commission, 2023a). Direktif kapsamında Avrupa Siber Kriz İrtibat Organizasyonu Ağı (EU-CyCLONe) hayata geçirilerek siber suçlara ilişkin bir koordinasyon ve iş birliği ağı kurulmaktadır. Bu kapsamda bahsi geçen direktif aynı zamanda siber suçlarla mücadele noktasında siber suçluların önünde bir engel konumunda bulunmaktadır. Aynı zamanda temel ve önemli kuruluşlar tarafından sağlanan hizmetlerin yüksek düzeyde siber güvenliğinin sağlanması bu hizmetlere yönelik siber saldırılar sonucunda oluşabilecek siber suçların sayısında büyük bir azalma sağlayacaktır. EU-CyCLONe kapsamında siber suç ve suçlulara ilişkin bilgi alışverişi artarak üye ülkeler arası siber suçlarla

mücadele hususu pekiştirilecektir (ENISA, 2023). Söz konusu yeniliklere ek olarak Avrupa Birliği genelinde dijital unsurlar içeren ürünlerin siber güvenliğinin arttırılması ve halihazırda bulunan siber güvenlik tüzüklerindeki açıkların kapatılması amacıyla 15 Eylül 2022 tarihinde Avrupa Komisyonu tarafından "Cyber Resilience Act (CRA)" adlı tüzük taslağı yayınlanmıştır. Söz konusu tüzük Internet of Things (IoT) ile ilgili yapılan ilk kanuni çalışma olmakla birlikte ağa bağlanabilen ve dijital unsur içeren tüm ürünler bu çerçevede düzenleme altında olacaktır. Siber suçların sadece bilgisayarlar değil çeşitli teknolojik aygıtlar kullanılarak da işlenebildiği dikkate alındığında söz konusu çalışmanın siber suçların ve suçluların önüne bir diğer engel olduğu söylenebilecektir. Öyle ki piyasaya sunulan dijital ürünler ve cihazlar, Avrupa Siber Güvenlik Ajansı (ENISA) bünyesinde oluşturulan European Cybersecurity Certification Framework (ECCF) kapsamında belirli bir denetleme sürecinden geçtikten sonra güvenilir damgalı etiketlerle son kullanıcıya sunulması siber güvenlik açısından kritik öneme sahip olacaktır (European Commission, 2023b). Diğer taraftan 2019 yılında AB Parlamentosu tarafından çıkarılan Avrupa Birliği Siber Güvenlik Kanunu (CSA) kapsamında ENISA kendisine verilen yetkiler çerçevesinde siber saldırılara karşı etkin mücadele yetisine sahip olmuştur. Bununla birlikte siber güvenliğe ilişkin sertifikasyon süreçlerinin yönetimi kapsamında ürün güvenliğine ilişkin bir sistem oluşturulmuştur. Söz konusu yasa dolaylı olarak siber suçların işlenmesini zorlaştıran ve siber saldırılara karşı savunma yönünü güçlendiren bir çerçeve çizmiştir (European Commission, 2023c). 18 Nisan 2023 tarihinde Komisyon tarafından önerilen değişikliklerle birlikte söz konusu siber tehdit içeren olayların tespit edilmesi, önlenmesi, sızma testleri ve güvenlik denetimleri gibi "managed security services" olarak nitelendirilen sertifikasyon uygulamasının benimseneceği değerlendirilmiştir. Kritik siber güvenlik hizmetlerinin güvenilirliğinin sağlanması hususu geliştirilerek "The EU Cyber Solidarity Act" yasa teklifi kapsamında "European Cybersecurity Shield" programının hayata geçirilmesi gündeme gelmiştir. Bu kapsamda uluslararası boyutta iş birliği ve koordinasyon sağlayacak bir sistem hayata geçirilmek istenmiştir. 2024 yılından itibaren öngörülen "Security Operations Centres (SOCs)" faaliyete başlayacak olup siber saldırılara karşı acil müdahale planları uygulanacaktır (European Commission, 2023d). Bu kapsamda söz konusu öncül tedbirler siber suçluların saldırı yapmasındaki motivasyonlarını azaltan, sonraki süreçlerde üye ülkeler arasındaki iş birliği kapsamında suçluların yakalanma riskinin artmasından dolayı suça yönelik caydırıcı

bir etki sağlamaktadır. Bunun yanı sıra 2013 yılında Europol tarafından kurulan ve bir görevi de AB kapsamında siber suçlara karşı adli makam ve kolluk kuvvetlerinin (LEAs) siber saldırılarla mücadelesini güçlendirmek olan "Europol's European Cybercrime Centre (EC3)" aynı zamanda çevrim içi suçlara karşı tüm paydaşları koruyucu bir yapıdadır. Bu merkez, "EU Law Enforcement Emergency Response Protocol (EU LE ERP)" vasıtasıyla kolluk kuvvetlerine operasyonel destek sağlayarak sibere bağımlı suçlar, çocuğun cinsel istismarı, ödeme dolandırıcılığı, dark web ve diğer platformlardaki suç tiplerine yönelik mücadelede büyük katkı sağlamaktadır. Kritik altyapı ve bilgi sistemlerini etkileyen siber suçlarla mücadelede öncü olmaktadır (Europol, 2023a). Yine Joint Cybercrime Action Taskforce (J-CAT) birimi EC3 bünyesinde siber suçlara karşı sınır ötesi soruşturma ve operasyon planlamalarında icrai rol alarak istihbarat odaklı eylemleri koordine etmektedir (Europol, 2023b). Bununla birlikte 2010 yılında bu yana çalışmalarına devam eden European Union Cybercrime Task Force siber suçların ve siber destekli suçların işlenmesini önleyici tedbirler alarak suça ilişkin altyapıları ortadan kaldırma amacını taşımaktadır (Europol, 2023). Avrupa Birliği bünyesinde oluşturulan direktif ve düzenlemelerin de siber suçlar alanında bağlayıcılık taşıyan hukuki metinler olarak bu suçlara karşı mücadelede önem arz ettiği varsayılabilir. Avrupa Birliği bünyesinde söz konusu direktifler elektronik ticarete ilişkin işlenen suçlarla birlikte kişisel verilerin ihlaline ilişkin suçları ve rıza dışı erişim sağlanan bilgisayar ve bilişim sistemlerini de içine almaktadır. Yine bu alanda pos cihazı ödemeleri ve internet yoluyla güvenli ödemelere ilişkin düzenlemeler de bulunmaktadır. Çocukların cinsel istismarı, fuhşa yönlendirme ve çocuk pornografisine yönelik çalışmalar Avrupa Birliği dahilinde yürütülen direktif çalışmalarında mevcut olan düzenlemeler arasındadır. Söz konusu uluslararası düzenlemeler, Sözleşme oluşturulurken ana atıf metni görevi görmektedir. Bu düzenlemeler dikkate alınarak hazırlanacak Sözleşme dilinin yeknesak şekilde oluşturularak metin düzeyinde birlik ve bütünlük sağlanması önem arz etmektedir (EUR-Lex, 2023).

Birleşmiş Milletler'in (BM) siber suçlara ilişkin yaptığı sınıflandırmada üç kategoriye yer verilmiştir. Bunların ilki "Bilgisayar Sistemlerine ve Servislerine Yetkisiz Erişim" başlığı altında "Yetkisiz Erişim", "Yetkisiz Dinleme" ve "Hesap İhlali"dir. Yetkisiz erişimde bilgisayar sistem veya ağlarına kişi veya kişilerce rıza dışı erişilmesi söz konusudur. Dinleme ise yetkisiz şekilde erişilen bilgisayar

sistemlerindeki iletişimlere yönelik bir davranıştır. İletişim kanalıyla aktarılan veri transferleri bu şekilde takip edilmektedir. Hesabın ihlal edilmesinde amaç ödeme yapılmasından kaçınmak gayesiyle üçüncü kişilerin hesaplarını yasa dışı kullanmaktır. İkinci kategori suç sınıfına "Bilgisayar Sabotajı" girmektedir. Öyle ki bilgisayar sabotajı bu sınıflandırma içerisinde çeşitlendirilerek "mantıksal", "fiziksel", "bilgisayar yoluyla" şeklinde isimlendirilerek alt kategorilere ayrılmıştır. Bilgisayar sistemlerinin fonksiyonlarını önleyerek veri ve programlarda "truva atı", "virüs", "solucanlar" ve "zaman bombası" gibi siber saldırı türleri ile yazılımsal olarak tahribat yaratmak amaçlanmaktadır. Bu veriler söz konusu yazılımlar vasıtasıyla silinebilmekte, değiştirilebilmekte ve yok edilebilmektedir. Hedefleri doğrultusunda kişisel çıkarlar gözetilerek (örneğin ekonomik kazanç) veriler üzerinde değişiklik de yapılabilmektedir. Ekonomik kazanç kapsamında "Banka Kartı Dolandırıcılığı" suçu ön plana çıkmaktadır ki BM tarafından buna ikinci kategori suçlarda yer verilmiştir. Özellikle "Automated Teller Machine (ATM)" olarak adlandırılan kartlı ödeme sistemlerine yönelik işlenen suçlar söz konusu kartların çalınarak kopyalanması şeklinde vuku bulmaktadır. Aynı zamanda bu suçlar kurban olarak seçilen kişilerin dinlenilmesi veya haberleşme hatlarının engellenmesi yoluyla da ortaya çıkabilmektedir. Bilgisayar sistemlerine kasti olarak hatalı veri girişi yapılarak ortaya çıkan "Girdi/Çıktı/Program Hileleri" ikinci kategoride düzenlenen suçlar sınıfındadır. "İletişim Servislerini Haksız ve Yetkisiz Olarak Kullanma", "Bilgisayar Yoluyla Sahtecilik", "Bilgisayar Yazılımının İzinsiz Kullanımı", "Lisans Sözleşmesine Aykırı Kullanım" ve "Lisans Haklarına Aykırı Kiralama" bu kapsamda düzenlenen diğer suçlardır. Üçüncü kategoride ise "Diğer Suçlar" şeklinde belirli suç tipleri sıralanmıştır. Bu suçlar; "Kişisel Verilerin Suistimali", "Sahte Kişilik Oluşturma ve Kişilik Taklidi" ve "Yasa dışı Yayınlar" olarak verilmiştir. Özellikle kişisel verilerin ihlali, siber saldırılar yoluyla kurumların veri tabanlarında devletlerin vatandaşlarına ait bilgilerin alınması yoluyla ortaya çıkmaktadır. Sahte kişilikler oluşturma suçunda ise; gerçek kişilere ait kimlik bilgilerinin suçlular tarafından kendi özelliklerine haiz kimlikler gibi kamuoyuna sunulması temel hareket fiili olarak ortaya çıkmaktadır. Bunun yanı sıra hayali karakterler oluşturularak menfaat sağlama şeklinde de bu suçun görünümü bulunmaktadır (BTK, 2022, s. 18-22). BM nezdinde siber suçlarla ilgili birçok karar alınmasının yanı sıra 1995 yılında "Group of Seven (G7)" kapsamında sınır aşan organize suçlarla mücadele hususu ciddi şekilde ele alınmaya başlamıştır. 1995 yılından itibaren ekonomik suçların yanı sıra terörizm ve uyuşturucuyla

ilgili suçlar temelinde faaliyetler yürüten G7 grubu bünyesinde, "Lyon Grubu" adında yeni bir alt komisyon kurulmuştur. 1996 yılında sınır aşan organize suçların yanına siber suçlarla mücadele görevini de üstlenen bu grup devletler arası siber suçlara karşı iş birliğinde öncü bir konuma gelmiştir (Council of Europe, 2023). 1997 yılında kurulan alt komisyon "High Technology Crime Subgroup" bünyesinde "International 24/7 Point of Contact Network" ağ yapısı kurularak 7/24 esaslı çalışma hayata geçirilmiştir. Söz konusu gruplar bahsi geçen tarihlerden günümüze kadar belirli periyotlarda toplanarak siber güvenlik ve siber suçlarla ilgili küresel stratejilerin belirlenmesinde büyük rol oynamıştır (Euromed Justice Program, 2021).

IV. BİLGİ VE İLETİŞİM TEKNOLOJİLERİNİN SUÇ AMAÇLI KULLANIMIYLA MÜCADELE KONUSUNDA KAPSAMLI ULUSLARARASI SÖZLEŞME ÇALIŞMASI

Avrupa Konseyi Bakanlar Komitesi onayı ile 08.11.2001 tarihinde kabul edilen ve 01.07.2004 tarihinde yürürlüğe giren Avrupa Konseyi Siber Suçlar Sözleşmesi siber suçlarla mücadele alanında yapılmış olan en önemli sözleşme hükmünde yer almaktadır. Türkiye ise söz konusu Konsey'in kurucu üyesi olarak 10.11.2010 tarihinde sözleşmeyi imzalamıştır. Bu sözleşme Ülkemizde 29.09.2014 tarihinde yürürlük kazanmıştır. Avrupa Konseyi Siber Suçlar Sözleşmesi Ülkemizde "Sanal Ortamda İşlenen Suçlar Sözleşmesi" şeklinde resmi şekilde tercüme edilmiştir. Sanal Ortamda İşlenen Suçlar Sözleşmesi 37. maddesi gereğince Konsey'e üyelik durumuna bakılmaksızın tüm ülkelere uygulanabilmektedir (Usta ve Benzer, 2018, s. 35-42). Mezkûr Sözleşme kılavuz olarak değerlendirilerek son zamanlarda siber suça ilişkin yapılan ayrımlara bakıldığında mevzuat çalışmaları içerisinde sibere bağımlı *(cyber dependant)* başlığı altında bilgisayarla ilişkili (computer system) ve siberle ilişkili *(cyber related)* başlığı altında bilgi ve iletişim teknolojileriyle ilişkili *(information and communications technology system/device)* siber suç sınıflandırması yapıldığı görülmektedir. Bu seçeneklerin ülke mevzuatlarına uygulanmasında belirleyici faktör daha önce de değinildiği üzere devletlerin siber suça ilişkin tanımlamaları, yaklaşımları ve ulusal politikalarıdır. Söz konusu düzenleme temel alınarak Birleşmiş Milletler Genel Kurulu tarafından alınan 74/247 sayılı kararla (United Nations General Assembly [UNGA], 2020) bilgi ve iletişim teknolojilerinin suç amaçlı kullanımına karşı kapsamlı şekilde uluslarara-

sı bir sözleşmenin yapılması için açık uçlu, hükûmetler arası, geniş temsil bölgesine sahip ve uzmanlardan oluşan "Bilgi ve İletişim Teknolojilerinin Suç Amaçlı Kullanımıyla Mücadele Konusunda Kapsamlı Uluslararası Sözleşme" (Sözleşme) hazırlanması amacıyla Ad Hoc Komite kurulmuştur. Siber andaki boşlukların doldurulması ve yeni teknolojik gelişmeler ışığında siber suçların kapsamının genişlemesi ile ilgili bir sözleşme hazırlanması gereği öngörülmüştür. Ulusal, bölgesel ve uluslararası düzeylerde uzmanlar grubu ile ülkeler arasında istişareler yapılarak bahsi geçen Sözleşme metninin oluşturulması amaçlanmıştır. 74/247 sayılı Genel Kurul kararı gereğince oluşturulan Ad Hoc Komite tarafından 2021 Mayıs ayında Newyork'ta organizasyonel bir oturum (United Nations Office on Drugs and Crime [UNODC], 2021) gerçekleştirmiştir. Söz konusu organizasyonel oturumda sözleşme kapsamındaki faaliyetler ve oluşturulacak metin üzerinde tematik görüşmelerde bulunulmuştur. Mayıs ayı içerisinde yapılan Genel Kurul toplantısında 75/282 sayılı karar (UNGA, 2021a) kabul edilmiştir. Bu kararda bilgi ve iletişim teknolojilerinin cezai amaçlarla kullanılmasına karşı koymak ana amaç olarak belirlenmiştir. Söz konusu ifade aynı zamanda ilgili kararın başlığını oluşturmuştur. Kararda en az altı oturum şeklinde Newyork ve Viyana'da düzenlenecek şekilde organizasyon yapılması hususu karara bağlanmıştır. Genel Kurulun 76/552 sayılı kararı (UNGA 2021b) üzerine, 2022 Şubat ve Mart ayları arasında toplanılarak Komite için oturumlarda gerçekleştirilecek çalışma şekli, izlenecek yol haritası ve çalışmalar (UNODC, 2021) üzerinde mutabık kalınmıştır (UNODC, 2022a).

Bilgi ve iletişim teknolojileriyle (ICT) işlenen klasik suçların *(cyber dependent)* yanı sıra bilgisayar sistemlerinin yapısı itibariyle suçun işleniş şeklini, sonuçlarını, yapılış anını ve süresini değiştirdiği çocuk istismarı, sahtecilik, hırsızlık ve dolandırıcılık gibi siberle kolaylaşan *(cyber-enabled)* ve terörizm, soykırım, uyuşturucu kaçakçılığı gibi diğer anlaşmalarda mevcut olan ICT'lerin kolaylaştırdığı suçlar Sözleşme kapsamında gerçekleştirilen oturumlarda tartışılmıştır. Bu suçların Sözleşme metninde yer alıp almaması üzerine süregelen oturumlarda gündeme getirilen tartışmalarda söz konusu suçlar için hangi terimlerin tercih edileceği de devletler arasında görüş ayrılığına sebep olan konular olmuştur (UNODC, 2023a). Sözleşme kapsamında ülkelerin taslak metne ilişkin verdikleri görüşlerde sibere bağımlı *(cyber dependent)* veya siberle kolaylaşan *(cyber enabled)* şeklinde iki farklı yaklaşımın olduğu görülmektedir (UNODC, 2023b). Bu Sözleşme'nin

hazırlanmasında devletler tarafından kabul olunan ortak kanı, içeriğin belirli bir alana yönelerek uluslararası ortamdaki diğer düzenlemelerin uygulama alanlarını ihlal etmemesi ve söz konusu düzenlemelerle yeknesaklığa sahip olmasıdır. Aynı zamanda Birleşmiş Milletler Sınır Aşan Suçlarla Mücadele Sözleşmesi (UNTOC) ve Birleşmiş Milletler Yolsuzlukla Mücadele Sözleşmesi (UNCAC) gibi metinlerde yer alan suç türlerinin tekrar Sözleşme'de ele alınmasının tekerrüre düşüleceği anlamına gelebileceği vurgusu yapılmıştır. Bunun aksi durumda sözleşmelerin birbiriyle uyumsuzluğu gündeme gelerek çeşitli ihtilafların ortaya çıkması sonucunu doğurabileceği belirtilmiştir. Bu kapsamda, siber suçların işleniş şekilleri gereği birçok alanı etkileyen ve gelişen teknolojilerle karmaşık bir yapıda bulunması sebebiyle sözleşme hükümlerinin geniş yorumlanmasından uzak durulması gündeme gelmiştir. Buradaki amaç sınırlı olarak tutulan hüküm yorumu vasıtasıyla iç mevzuata uyum sağlama ve uygulamaya yönelik kolaylıklar sağlamaktır (UNODC, 2022b).

Sözleşme kapsamında Ad Hoc Komite'nin konsolide şekilde oluşturduğu ve devletlerin görüşlerine açılan taslağın son haline ilişkin metinde ikinci bölümde yer verilen "Suçlaştırma (*Criminalization*)" başlıklı kısımda oldukça kapsamlı düzenlemeler bulunmakla birlikte burada tanzim edilen suçlar sibere bağımlı (*cyber dependant) ve* siberle alakalı olarak *(cyber relatd)* tasnif edilmiştir. Bilgisayar sistemlerine veya bilgi ve iletişim teknolojileri sistem veya aygıtlarında *"illegal access (*yasa dışı erişim)*", "illegal interception* (yasa dışı müdahale)*", "misuse of devices* (cihazların kötüye kullanılması)*", "forgery* (sahtecilik)*", "fraud* (dolandırıcılık)*", ve "theft* (hırsızlık)*"* gibi suçları içeren bölüm, yukarıda daha önce değinilen ve ülkelerin kendi mevzuat ve politikalarına göre görüş vermeleri beklenen bilgisayar ya da bilgi ve iletişim teknolojileri ayrımı ile birlikte 2001 tarihli Avrupa Konseyi Siber Suçlar Sözleşmesi'ne paralel olarak düzenlenmiştir. Diğer taraftan metinde yer alan bazı suçlar siberle alakalı (*cyber related)* olarak düzenlemeye tabi tutulmuştur (UNODC, 2023a). Bu bölümdeki suçlara "çevrim içi çocuk cinsel istismarıyla veya istismara yönelik materyallerle ilgili suçlar" örnek olarak verilebilir. Taslak metnin bu kısmında düzenlenen bazı suçlar seçimlik hareketli suç kategorisindedir. Seçimlik hareketli suçlar yapısı gereğince birden fazla farklı fiille aynı suça meydan verebilmektedir. Öyle ki kanunda gösterilen farklı fiillerden birisi işlenerek oluşan suça içtima hükümleri uygulanmayarak sadece tek bir suç oluşturmaktadır (Alacakaptan, 1975, s. 47). Örneğin çocuğun istismarına yol

açacak fiiller bilişim sistemleri aracılığıyla işlenebileceği gibi fiziki olarak fiilen de işlenebilen suçlardandır. Öyle ki TCK'da çocuğun her türlü cinsel istismarı yasaklanmış olup söz konusu fiiller mevzuatımızın muhtelif maddeleri altında bilişim sistemleri aracılığıyla işlenip işlenmediğine bakılmaksızın düzenlenerek suç olarak kabul edilmiştir.

Taslak haldeki Sözleşme'nin ilk kısmında düzenlenen *cyber dependant* suçlar Avrupa Konseyi Siber Suçlar Sözleşmesi'nde mevcut olan suçlardır. Ancak bu metinde yer alan birçok *cyber enabled* suçunun Avrupa Konseyi Siber Suçlar Sözleşmesi'nde yer almadığı görülmektedir. Söz konusu kısımda düzenlenen maddelerde ifade edilen fiiller fiziki şekilde işlenebileceği üzere bilişim sistemleri vasıtasıyla da işlenebilmektedir (UNODC, 2023a). Bu kısımda düzenlenen suç tipleri bilgi ve iletişim teknolojisi kullanılarak işlenen suçlar konumunda bulunmaktadır. Tartışma konusunu oluşturan husus ise bu suç tiplerinin ayrıntılı hükümler içermeyen muğlak şekilde çerçevesi çizilmiş bir yapıda olmasıdır. Mezkûr suç tiplerinin belirsiz şekilde düzenlenmiş olmasından ötürü yerel mevzuatlara aktarılması aşamasında hangi suç tipleri açısından geçerli olacağı hususunda tartışmalar söz konusu olacaktır. Suç olarak taraf devletlerce kabul edilmesi öngörülen eylemlerin kapsamının, seçenek hareketlerinin ve bu hareketlere ait hukuki boyutların sınırlarını tespit etmek oldukça güçtür. Nitekim, mezkûr maddelerde tanımlanan eylemler bilişim sistemleri aracılığıyla gerçekleştirilebileceği gibi fiziki olarak da gerçekleştirilebilmektedir. Bu sebeple fiziki ve çevrim içi olarak işlenen suçlar noktasında ilgili suç tipi ayrımının yapılması konusunda da problemler ortaya çıkmaktadır.

Sözleşme'nin bağlayıcılığı konusunda bir kesinlik olmasa dahi uygulayıcı ülkelerin bu sözleşmeyi temel alarak iç mevzuatlarına Sözleşme hükümlerini aktarmaları öngörülmektedir. Bu kapsamda söz konusu Sözleşme'de *cyber related ve cyber enabled* suçların düzenleniyor olması yerel mevzuatların da bu yönde şekillenmesinde etkili olacaktır. Sınıflandırma yapıldığında bazı ülkeler siber suçların bilişim sistemleri vasıtasıyla işlenmesini temel alarak sınırlı bir kategorizasyon yapmasına rağmen, bazı ülkeler siberin araç şeklinde kullanılarak işlendiği çok daha geniş yelpazedeki suç türünü siber suçlar kapsamına almaktadır. Örneğin internet ortamında çocuğun cinsel istismarı suçu da bazı ülkelere göre *cyber related* olarak kabul edilip siber suçlar kapsamına alınmaktadır. Uluslararası sözleşmelerde tartışılan *cyber enabled* terimi siberle kolaylaşan suçları ifade etmektedir.

Birçok suç türü siber araçlar vasıtasıyla kolay bir şekilde işlenebilmektedir. Burada kastedilen normal şartlarda işlenmesinde zorluk bulunan veya suçun faillerinin yakalanmasının daha kolay olduğu belirli suç tiplerinin, siber araç olarak kullanılmak suretiyle rahatlıkla işlenebilmesidir. Siberin kolaylaştırdığı bu yolla failler kolluk kuvvetleri ve sorgulama mercilerinden rahatlıkla kaçarak söz konusu suçları işleyebilmektedir. Kendilerini gizleme konusunda başarılı olarak suçu işleme motivasyonlarını giderek artırmaktadırlar. Bahse konu ifadesel ayrımlara bakıldığında dünya üzerindeki siyasi kutuplaşmaların ülkelerin görüşlerini belirtmesinde etkili olduğu gözlemlenmektedir.

Sözleşme'nin oluşturulması aşamasında gerçekleştirilen toplantı oturumlarında siber suça ilişkin devletler arası ifade ayrımları dikkat çekmektedir (UNODC, 2022b). Öyle ki ABD ve AB ülkelerinin başını çektiği grup tarafından, Sözleşme'ye ilişkin ortak görüşlerinde kısa bir sözleşme metni olmasını istemelerinin yanı sıra evrensellik ve uygulanabilirlik açısından esnek bir yapının inşa edilmesi gerekliliğini belirtilmiştir. Sözleşme'nin ilk evrede *cyber dependent* suçlar ekseninde düzenlenmesinin faydalı olacağı fakat *cyber enabled* suçların daha sonraki evrelerde *cyber dependant* suçlara ilişkin işleniş biçimlerini önemli oranda etkilemesi veya sonuca tesir etmesi halinde sözleşmenin içeriğine eklenmesi şeklinde görüş bildirilmiştir. Sözleşme'nin ilk aşamasında yer verilmeyen suç tiplerinin UNTOC gibi sözleşmelerde olduğu gibi ek protokol şeklinde sonradan eklenebileceği ifade edilmiştir. *Cyber enabled* suç tiplerinin söz konusu sözleşmeye dahil edilmesine olumsuz bakılmasının bir sebebinin de ilgili suç tiplerinin kabulüne ilişkin görüşmelerin sözleşmenin kabul edilme süresini uzatacak olması olduğunu bildirmişlerdir (UNODC, 2021a ve 2022d).

Buna karşılık ABD ve AB üyesi ülkelerin karşıt görüşünde yer alan Rusya Federasyonu, İran, Çin Halk Cumhuriyeti ve Hindistan gibi ülkeler, BM Genel Kurulu'nun 74/247 sayılı kararı esas alınarak Sözleşme'nin *cyber enabled* suçları da kapsayacak şekilde hibrit formatta oluşturulmuş bir sözleşme olması gerektiğini ifade etmiştir. Bu kapsamda bilişim sistemleriyle işlenen suçların yanı sıra bilişim sistemleri tarafından kolaylaştırılan suçların da etkin şekilde tartışılması gerektiği vurgusu yapılmıştır. Bu görüş gerekçesinde *cyber dependant* olarak nitelendirilen suçların yanı sıra *cyber enabled* suçların bilgi ve iletişim teknolojileri vasıtasıyla işlenebildiği ve zarar verici nitelikte bir boyutta olduğu dile getirilmiştir (UNODC, 2021b)(UNODC, 2022e). Bu görüşün gerekçesini sunan İran tarafı, bilgi ve

iletişim teknolojileri vasıtasıyla meydana getirilen siber suçların Sözleşme kapsamında mücadeleye yönelik hareket alanının görülmesinde fayda sağlayacağını ve bu suçların verdiği zarar çemberinin daraltılabileceğini ifade etmiştir (UNODC, 2021a ve 2022d).

Sözleşmeye ilişkin toplantı oturumlarında terimlere ilişkin tartışma konularından bir tanesi *"computer systems* (bilgisayar sistemleri)*"* ve *"information and communication technology* (bilgi ve iletişim teknolojileri)*"* ayrımı noktasında olmuştur. Bu ifadesel ayrımda müşterek görüş birliği çerçevesinde Rusya Federasyonu, İran, Çin Halk Cumhuriyeti ve Hindistan'ın içerisinde bulunduğu grup Sözleşme'de *cyber dependant* kapsamında ele alınan "bilgisayar sistemleri" ifadesine karşılık *cyber enabled* kapsamında ele alınan "bilgi ve iletişim teknolojileri" ifadesinin kullanılmasını uygun görmüşlerdir. Burada amaç siber suçların daha geniş yoruma mahal verecek şekilde Sözleşme'ye dahil edilmesidir (UNODC, 2022f). Bahsi geçen ülkelerin söz konusu terimin kullanılmasında ısrarcı olmasının bir sebebi de sürekli olarak gelişen teknolojilere ayak uydurabilecek genel ve esnek ifadelerin gerekliliğidir. Öncül olarak siber suçları kapsamına alacak esnek bir ifade, teknolojik ilerlemeler doğrultusunda ileriye dönük farklı suç tipleri oluşsa dahi ulusal ve uluslararası mevzuatlarda tekrar bir düzenleme yapma külfeti oluşturmadan kolaylıkla uygulanma olanağı sunacaktır. Sözleşme'nin geniş yorumlanarak kapsamlı şekilde ele alınmasının söz konusu düzenlemenin her ne kadar ülkelerin birbirlerinin hakimiyetindeki suçlu konumunda bulunan kişileri talep edebilmesine olanak tanısa da devletlerin egemenlik bakımından eşitliği ilkesine aykırı uygulamalara mahal verilmemesi gerektiğine vurgu yapılmıştır. Bunun yanı sıra toprak bütünlüğü, siyasi bağımsızlık ve iç işlerine karışmama ilkelerine de saygı gösterilmesi gerektiği hususu ifade edilmiştir. Yine İSS'ler de dahil olmak üzere özel sektör yetkililerinin Sözleşme'nin ortaya çıkarılmasında önemli rol üstleneceği belirtilmiştir (UNODC, 2022b).

Sözleşme metninde geçen *"any criminal offence* (cezai siber suç)*"* ve *"serious crimes* (ciddi siber suç)*"* ifadelerinin arasında yapılan seçim ülkeler arasında tartışılan bir diğer konu olmuştur. Sözleşme toplantılarına katılan bazı ülkeler, bu ifadelerin ülkesel yorum farklılıkları sebebiyle uygulamada da sıkıntılılara yol açabileceğini ve yeknesak olmayan uygulamaların karşılıklı iş birliği konularında sıkıntı doğurabileceğini ifade etmiştir. Öyle ki bu ifadelerin yerine *"offenses set forth in this Convention* (sözleşmede belirtilen siber suçlar)*"* ifadesinin metne

işlenebileceği fikri diğer devletler nezdinde paylaşılmıştır. Özellikle ciddi siber suçların hangi suç tiplerini içereceği, hangi fiillerin ciddi suça mahal verecek yapıda olduğu üzerinde fikir birliği olmaması söz konusu seçenekler arasında kalınmasında önemli bir etken konumundadır. Sözleşme'nin temel olarak ciddi siber suçların tespiti, araştırılması ve soruşturulmasına yönelik olması gerektiği belirtilmiş ve insan haklarının adaletin merkezinde yer aldığı ifadeyle metinde insan haklarına saygı gösterilmesinin önemine değinilmiştir (UNODC, 2023d). Microsoft Corporation tarafından, Sözleşme metninde yer verilen terminolojinin kesin ve açık şekilde düzenlenmesi gerektiği ve "açık suç kastı" atfında bulunulabilen ciddi siber suçların metin kapsamında değerlendirilmesi gerektiği hususları ifade edilmiştir. Öyle ki söz konusu ciddi suç kategorisine girmediği halde bu kategoriye sokulabilecek sızma testi gibi test faaliyetlerinin yanlış anlaşılarak suç olarak nitelendirilebileceği tehlikesi gündeme getirilmiştir (Microsoft Corporation, 2022). United Kingdom International Chamber of Commerce (ICC) tarafından toplantının üçüncü oturumunda talep konusu edilen hususlar arasında Sözleşme hükümlerinin ciddi siber suçlara uygulanması da bulunmaktadır (ICC, 2022). Burada amaç kapsamın daraltılarak belirli ciddi suçlarla bir sınırlandırmaya gidilmesi olmuştur. Uygulamada netlik kazandırması ve ileride oluşabilecek hukuki ihtilafların önüne geçilmesi adına toplantı raporlarında Siber Barış Enstitüsü de bunun önemine vurgu yapmıştır (The CyberPeace Institute, 2023). Söz konusu Sözleşme'nin ön söz kısmında (UNGA, 2023) siber suçlara maruz kalan kişilerin korunmasının amaçlandığı, öncül ve ardıl tedbirlerin düzenleneceği, siber suçla etkin bir şekilde mücadelede bulunularak gerekli caydırıcılığın sağlanacağı, devletler arası teknik yardıma ilişkin araçların geliştirileceği, siber güvenliğe ilişkin kapasitelerin inşası ve güvenlik düzeyinin artırılması için gerekliliklerin sağlanacağı belirtilmiştir.

Aralarında ABD, Kanada, AB üyeleri, İsviçre ve Singapur'un olduğu ülkeler söz konusu Sözleşme bağlamında yer verilecek suçların dar yoruma tabi tutulması ve suç tanımlarının belirgin şekilde yapılması gerektiğini, bu suçların dışındaki suçların ise kısıtlı olarak metine aktarılabileceği görüşlerini belirtmişlerdir. Söz konusu suçlarla mücadelede Sözleşme görüşmeleri sırasında ikili bir ayrıma tabi tutulan siber suçlar için *"fight against the use of information and communications technologies for criminal purposes* (bilgi ve iletişim teknolojilerinin suç amaçlı kullanımıyla mücadele)*"* ve *"fight against cybercrime* (siber suçlarla mücadele)*"*

ifadelerinin kullanılması tartışma konusu olmuştur. Öyle ki bu ülkeler dar yorum kapsamında "siber suçlarla mücadele" ifadesinin kullanımının daha doğru olacağını değerlendirmişlerdir. Siber suçlarla mücadele ifadesi bilgi ve iletişim teknolojilerinin suç amaçlı kullanımı ifadesinin içerisinde barındırdığı suç tiplerini kapsamayan dar bir içeriğe sahiptir. Taslak Sözleşme metninde bu husus üzerinde iki farklı görüş etrafında kümeleşen ülkeler arasında tartışmalar yaşanmıştır. Karşı görüşte yer alan Rusya Federasyonu, İran, Çin, Mısır ve Hindistan'ın başını çektiği ülkeler Sözleşme'deki "bilgi ve iletişim teknolojilerinin suç amaçlı kullanımıyla mücadele" ifadesinin geniş yorum gerektiren bir ifade olduğunu belirterek metinde yer alması gerektiğini değerlendirmişlerdir. Bu ifadenin diğerine göre daha esnek bir yapıda olduğu, özellikle de bilgi ve iletişim teknolojilerinin gelişmesiyle ileride farklı suç tiplerinin de oluşabileceği ve bunların da söz konusu ifadenin içeriğinde kendisine yer bulabileceği ifade edilmiştir. Devletlerin toprak bütünlüğü, siyasi olarak özerklik ve iç işlerine karışılmama ilkelerine itaat edilmesi hususuna vurgu yapılmıştır. Bu kapsamda söz konusu ülkeler klasik siber suçların (bilgisayar ve sistemlerine yetkisiz girme, sistemlere yasa dışı müdahale ve siber saldırı türlerinin kullanımı, verilerin deformasyona uğratılması, içeriğinin değiştirilmesi veya silinmesi, teknolojik cihazların özellikle de bankacılık sistemlerinin kötücül amaçlarla kullanımı) yanı sıra siberin kolaylaştırdığı, internet ortamında işlenilmesiyle suçun sonucunun hızlandığı, niteliksel olarak farklı bir yöne evrildiği ve etki düzeyinin de farklılaştığı; çocukların cinsel istismarı, siber zorbalık, dolandırıcılık, fikri mülkiyete ilişkin suçlar gibi *cyber enabled* kategorisinde olan suç tiplerinin de Sözleşme'de düzenlenmesi gerektiği hususunda görüş bildirmişlerdir (UNODC, 2022b).

SONUÇ VE DEĞERLENDİRME

Siber suça ilişkin yapılan tanımlara bakıldığında sadece sibere bağımlı olan klasik suçların Sözleşme metninde olması, değişen ve gelişen teknolojilerle işlenebilen siber suç tiplerini dışarıda bırakmaktadır. Halbuki siberin kolaylaştırdığı (*cyber enabled*) ve siberle alakalı (*cyber related*) suç tipleri birçok farklı suç türünü de kapsamına alarak geniş çerçeveden bu suçlara ilişkin soruşturma, kovuşturma ve cezai yaptırım imkânı sunmaktadır. Bu kapsamda değerlendirme yapıldığında siberin kolaylaştırdığı ve siberle alakalı suçların da Sözleşme'de yer alması isabetli olacaktır. Geniş yorum vasıtasıyla siberle alakalı suçlar kapsama alınarak söz konusu terimlere ilişkin fikir birliği oluşturulmalıdır. Her ne kadar devletlerin çekince koydukları hususlara dair iç hukukta uygulanabilirlik hususunda sıkıntılar yaşanabilecek olsa da ayrıntılı şekilde hazırlanacak hükümler herhangi bir belirsizliğe yol açmadan iç hukuka aktarılabilecektir. Bununla birlikte Sözleşme görüşmeleri sırasında tartışılan "bilgi ve iletişim teknolojileri" terimi de metne dahil edilmesi gereken ifadelerdendir. Öyle ki siber suçların 2000'li yılların başında sadece bilgisayar sistemleri ile işlendiği teknoloji, yerini geniş çapta cihazlarla işlenebilen ve ağ üzerinden yıkıcı etki bırakabilen siber saldırı teknolojisine bırakmıştır. Diğer taraftan, hangi suçların Sözleşme kapsamı dahilinde değerlendirileceğine ilişkin devletler arasında yaşanan ihtilaflara bakıldığında siber suçlarla ilgili tespit faaliyetlerinin yürütülmesi ve adli makamlar tarafından soruşturma ve kovuşturma yapılabilmesi olanağının bu hususta belirleyici olduğu görülecektir. Öyle ki ciddi siber suçların soruşturma ve kovuşturmaya tabi tutulması konusunda devletler arasında anlaşmazlıklar yaşanabilecektir. Burada önemli olan mesele ise ciddi siber suçun kapsamı ve devletlerin hangi kıstaslara göre bir suçu ciddi siber suç sayacak olmasıdır. Devletlerin yerleşik hukuk kuralları ve mevzuatları kapsamında yazılı olarak suç atfedilmeyen fiiller ile toplum nezdinde suça sebebiyet vermeyecek fiillerin ciddi olarak nitelendirilmesinde amaç ve kapsam problemi yaşanacağı ortadadır. Bu sebeple siber suçların "ciddi" ifadesi yerine "Sözleşme'de belirtilen suçlar" ifadesiyle tamamlanabileceği değerlendirilebilir. Öyle ki metinde düzenlenmeyen suç tiplerinin kapsama dahil edilmesi devletler açısından uygulamada farklılıkların oluşmasına yol açarak belirsizliklerin doğmasına sebebiyet verecektir.

Son zamanlarda internet ortamında çocukların siber zorbalığa maruz kalması, sanal ortamda cinsel tacize uğramaları, dolandırıcılık, sahtecilik ve hırsızlıkla

ilgili siber suçların artışı siberin araç olarak kullanıldığı suçlar için açık bir düzenlemeye ihtiyaç duyulduğunu göstermektedir. Bu sebeple söz konusu Sözleşme bu konuda uluslararası alandaki hukuk boşluğunu doldurabilecek konumdadır. Siberle alakalı suçlarla ilgili düzenlemeler bu suçların gerçekleştirilmesine yönelik davranışları kısıtlayıcı bir etki yaratacaktır. Söz konusu düzenleme ile suçun faillerine yönelik caydırıcılık hususu gündeme gelecektir. Aynı zamanda suçluların soruşturulması, kovuşturulması ve iadesine ilişkin hususlarda siber suça müşterek bir yaklaşım sağlanarak uygulamada devletler arası yaşanabilecek ihtilafların önüne geçilmesi sağlanacaktır. Sınır tanımayan siber saldırıların ve siber suçluların tespitinde devletler arası hukuki ve teknik yardımlaşma geliştirilerek 7/24 bilgi ve veri akışı ağı sağlanabilecektir. Ortak bir siber suç yaklaşımı sonrasında siber uzayda birden çok devletin yargı yetkisine giren olayların çözüme kavuşturulmasını sağlayacak uluslararası adalet mekanizmaları ve mahkemelerin de oluşturulması gerekli olacaktır. Bu kapsamda bağlayıcı konumda olan uluslararası siber uzay mahkemeleri ve ara buluculuk merkezlerinin hayata geçirilmesi büyük önem arz etmektedir. Yine, ortaya çıkan hukuk boşlukları doldurularak siber suçluların kendilerini mahkeme önünde avukat marifetiyle savunabileceği sistemler de doğal olarak oluşacaktır.

KISALTMALAR

BM	Birleşmiş Milletler
BTK	Bilgi Teknolojileri ve İletişim Kurumu
CMK	Ceza Muhakemesi Kanunu
EC3	European Cybercrime Centre
EHK	Elektronik Haberleşme Kanunu
EİK	Elektronik İmza Kanunu
ENISA	European Unıon Agency For Cybersecurity
ICC	United Kingdom International Chamber of Commerce
ICCP	Committee on Information, Communications and Computer Policy
ICT	Information and Communication Technologies
ITU	International Telecommunication Union
J-CAT	Joint Cybercrime Action Taskforce
NIST	National Institute of Standards and Technology
OECD	The Organisation For Economic Cooperation and Development
SPF	Singapur Polis Gücü
TCK	Türk Ceza Kanunu
UNGA	United Nations General Assembly
UNODC	United Nations Office on Drugs and Crime

KAYNAKÇA

AAG IT Services. (2023). The Latest 2023 Cyber Crime Statistics. https://aag-it.com/the-latest-cyber-crime-statistics/ adresinden 22 Eylül 2023 tarihinde erişildi.

Akpek, N. O. (2015). Siber Suçlar Sözleşmesinin Getirdikleri ve İç Hukuk Açısından Konuya Yaklaşım [Yüksek Lisans tezi, İstanbul Bilgi Üniversitesi]. https://tez.yok.gov.tr/UlusalTezMerkezi/tezDetay.jsp?id=GswZ7stjY2LTwxeBF7XsrQ&no=uR2ojMmxzbc0TS5hxDlpAQ adresinden 6 Haziran 2023 tarihinde erişildi.

Alacakaptan, U. (2022). Suçun Unsurları. Ankara Üniversitesi Hukuk Fakültesi Yayınları.

Aldoori, A. (2020). Uluslararası Hukukta Siber Suçla Mücadele. [Yüksek Lisans tezi, İstanbul Üniversitesi]. http://nek.istanbul.edu.tr:4444/ekos/TEZ/ET002065.pdf adresinden 13 Haziran 2023 tarihinde erişildi.

Andress, J. ve Winterfeld, S. (2013). Cyber Warfare: Techniques, Tactics and Tools for Security Practitioners (2.Baskı). Syngress Press.

Bilgi Teknolojileri ve İletişim Kurumu Sektörel Araştırma ve Strateji Geliştirme Dairesi Başkanlığı. (2022). Dijitalleşen Dünyada Bilişim Suçları ve Mücadele Yöntemleri. https://www.btk.gov.tr/uploads/pages/arastirma-raporlari/dijitallesen-dunyada-bilisim-suclari-ve-mucadele-yontemleri-6218e2417eaea.pdf adresinden 12 Haziran 2023 tarihinde erişildi.

Brenner, S. W. (2010). Cybercrime: Criminal Threats From Cyberspace, School Of Law Faculty Publications, 115. https://ecommons.udayton.edu/law_fac_pub/115 adresinden 2 Haziran 2023 tarihinde erişildi.

Ceza Muhakemesi Kanunu. Kanun Numarası: 5271. sayılı Kabul Tarihi: 04.12.2004. RG 17.12.2004/25673.

Committee on Information, Communications and Computer Policy. (2010). OECD ICCP Committee. https://www.oecd.org/digital/ieconomy/37328586.pdf adresinden 14 Temmuz 2023 tarihinde erişildi.

Council Of Europe. (2001). Convention On Cybercrime. https://www.europarl.europa.eu/cmsdata/179163/20090225ATT50418EN.pdf adresinden 15 Ha-

ziran 2023 tarihinde erişildi.

Council of Europe. (2023). Council of Europe action against Cybercrime. https://www.coe.int/en/web/portal/coe-action-against-cybercrime adresinden 10 Ağustos 2023 tarihinde erişildi.

Çolak, H. (2016). Siber Terörizmin Önlenmesinde Kurumsal Yapılanma ve Uluslararası Adli Yardımlaşma. Türk Hukuk Araştırmaları Dergisi, 1(1), 4.

Elektronik Haberleşme Kanunu. Kanun Numarası: 5809. sayılı Kabul Tarihi: 05.11.2008. RG 10.11.2008/27050.

Elektronik Haberleşme Sektöründe Şebeke ve Bilgi Güvenliği Yönetmeliği. Bilgi Teknolojileri ve İletişim Kurumu. https://www.mevzuat.gov.tr/File/GeneratePdf?mevzuatNo=19880&mevzuatTur=KurumVeKurulusYonetmeligi&mevzuatTertip=5

Elektronik İmza Kanunu. Kanun Numarası: 5070. sayılı Kabul Tarihi: 15.01.2004. RG 23.01.2004/25355

Emniyet Genel Müdürlüğü Siber Suçlarla Mücadele Daire Başkanlığı. (2023). SiberAy Sözlüğü. https://www.siberay.com/kurumlar/Siberay.com/SIBERAY-Sozluk.pdf adresinden 9 Haziran 2023 tarihinde erişildi.

Eur-Lex. (2023). Accesss To European Unıon Law. https://eur-lex.europa.eu/search.html?scope=EURLEX&text=d%C4%B1rective&lang=en&type=quick&qid=1694697439782 adresinden 10 Ağustos 2023 tarihinde erişildi.

Euromed Justice Program. (2023). The G7 24/7 Cybercrime Network. https://euromedjustice.eu/wp-content/uploads/2021/05/G7_Network.pdf adresinden 10 Ağustos 2023 tarihinde erişildi.

European Unıon Agency For Cybersecurity (ENISA). (2023). EU CyCLONE. https://www.enisa.europa.eu/topics/incident-response/cyclone adresinden 10 Temmuz 2023 tarihinde erişildi.

European Commission. (2022). New EU Cybersecurity Strategy And New Rules To Make Physical And Digital Critical Entities More Resilient. https://digital-strategy.ec.europa.eu/en/library/eus-cybersecurity-strategy-digital-decade-0 adresinden 14 Temmuz 2023 tarihinde erişildi.

European Commission. (2023a). Directive on measures for a high common level of cybersecurity across the Union (NIS2 Directive). https://digital-strategy.ec.europa.eu/en/policies/nis2-directive adresinden 8 Ağustos 2023 tarihinde erişildi.

European Commission. (2023b). Cyber Resillience Act. https://digital-strategy.ec.europa.eu/en/library/cyber-resilience-act adresinden 8 Ağustos 2023 tarihinde erişildi.

European Commission. (2023c). The EU Cybersecurity Act. https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-act adresinden 8 Ağustos 2023 tarihinde erişildi.

European Commission. (2023d). The EU Cyber Solidarity Act. https://digital-strategy.ec.europa.eu/en/policies/cyber-solidarity adresinden 6 Ağustos 2023 tarihinde erişildi.

Europol. (2023a). European Cybercrime Centre – EC3. https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3 adresinden 8 Ağustos 2023 tarihinde erişildi.

Europol. (2023b). Joint Cybercrime Action Taskforce (J-CAT). https://www.europol.europa.eu/operations-services-and-innovation/services-support/joint-cybercrime-action-taskforce adresinden 9 Ağustos 2023 tarihinde erişildi.

Europol. (2023c). European Union CYBERCRIME TASK FORCE (EUCTF). https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3/euctf adresinden 10 Ağustos 2023 tarihinde erişildi.

Fikir ve Sanat Eserleri Kanunu. Kanun Numarası: 5846. sayılı Kabul Tarihi: 05.12.1951. RG 13.12.1951/7981.

Gordon, S. ve Ford, R. (2006). On the Definition and Classification of Cybercrime. Journal in Computer Virology, 2, 13-20. https://doi.org/10.1007/s11416-006-0015-z adresinden 4 Haziran 2023 tarihinde erişildi.

Holt, T. J. ve Bossler, A. M. (2020). The Palgrave Handbook of International Cybercrime and Cyberdeviance. Palgrave Macmillan Press.

International Telecommunication Union. (2007). Global Security Agenda (GCA). https://www.itu.int/en/action/cybersecurity/Pages/gca.aspx adresinden

17 Temmuz 2023 tarihinde erişildi.

International Telecommunication Union. (2009). Understanding Cybercrime: A Guide For Development Countries. https://www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-understanding-cybercrime-guide.pdf adresinden 14 Haziran 2023 tarihinde erişildi.

İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun. Kanun Numarası: 5651. Sayılı Kabul Tarihi: 04.05.2007. RG 23.05.2007/26530.

INTERPOL. (2017). Global Cybercrime Strategy. https://www.interpol.int/content/download/5586/file/Summary_CYBER_Strategy_2017_01_EN%20LR.pdf?inLanguage=eng-GB adresinden 5 Ağustos 2023 tarihinde erişildi.

Lasky, J. (2022). Cyberspace. Salem Press Encyclopedia of Science. https://public.stacksdiscovery.com/eds/detail?db=ers&an=93787497 adresinden 13 Haziran 2023 tarihinde erişildi.

Lin, L. S. F. ve Masys, A. J. (Ed.). (2018). Asia-Pacific Security Challenges Managing Black Swans and Persistent Threats (1.Baskı). Springer Press. DOI: 10.1007/978-3-319-61728-2

Malisevic, N. (2022). Microsoft's Presentation at the Panel Titled: A Concerted Effort. [Poster Sunumu]. Third intersessional consultation of the Ad Hoc Committee on Cybercrime, Amerika Birleşik Devletleri, New york https://www.unodc.org/documents/Cybercrime/AdHocCommittee/Third_intersessional_consultation/Presentations/Panel_4_Microsoft.pdf adresinden 10 Temmuz 2023 tarihinde erişildi.

National Institute of Standards and Technology. (2023). NIST Glossary. https://www.nist.gov/itl/smallbusinesscyber/cybersecurity-basics/glossary#C adresinden 10 Ağustos 2023 tarihinde erişildi.

OECD. (2008). Policy Guidance on Online Identity Theft. https://www.oecd.org/sti/consumer/40879136.pdf adresinden 12 Temmuz 2023 tarihinde erişildi.

Singapore Police Force. (2023). Siber Suçun Sınıflandırılması ve Tanımı. https://www.police.gov.sg/Advisories/Crime/Cybercrime#:~:text=In%20Singapore%2C%20cybercrime%20is%20categorised,%2C%20website%20defacement-

s%2C%20ransomware%20etc adresinden 22 Ağustos 2023 tarihinde erişildi.

Smith, R. G., Grabosky, P., ve Urbas, G. (2004). Cyber Criminal on Trial. Cambridge University Press. https://www.researchgate.net/publication/233023456_Cyber_Criminals_on_Trial adresinden 2 Haziran 2023 tarihinde erişildi.

Suçluların İadesine Dair Avrupa Sözleşmesine Ek İkinci Protokol. https://inhak.adalet.gov.tr/Resimler/Dokuman/2712020132606098_tur.pdf adresinden 10 Ağustos 2023 tarihinde erişildi.

The Crown Prosecution Service. (2022). Cybercrime Definition. https://www.cps.gov.uk/crime-info/cyber-online-crime#:~:text=drugs%20and%20firearms.-,Cybercrime,or%20simply%20to%20disrupt%20businesses adresinden 12 Haziran 2023 tarihinde erişildi.

The CyberPeace Institute. (2023). Submission to the Fifth Session. https://www.unodc.org/documents/Cybercrime/AdHocCommittee/5th_session/Documents/Multi-stakeholders/CYBERP1.PDF adresinden 24 Temmuz 2023 tarihinde erişildi.

Thomas, D. ve Loader, B. (Ed.). (2000). Cybercrime: Law Enforcement, Security and Surveillance in the Information Age (1. Baskı). Routledge Press.

Türk Ceza Kanunu. Kanun Numarası: 5237. Kabul Tarihi: 26.09.2004. RG 12.10.2004/25611.

Türk Dil Kurumu. (2023). Türk Dil Kurumu Sözlüğü. https://sozluk.gov.tr/ adresinden 2 Eylül 2023 tarihinde erişildi.

Ulaştırma ve Altyapı Bakanlığı. (2020). 2020-2023 Ulusal Siber Güvenlik Strateji ve Eylem Planı. https://hgm.uab.gov.tr/uploads/pages/strateji-eylem-planlari/ulusal-siber-guvenlik-stratejisi-ve-eylem-plani-2020-2023.pdf dresinden 24 Temmuz 2023 tarihinde erişildi.

United Kingdom International Chamber Of Commercee. (2022). Submission To The Third Sessions. https://www.unodc.org/documents/Cybercrime/AdHocCommittee/Third_session/Documents/Submissions/ICC_UK_1.pdf adresinden 21 Temmuz 2023 tarihinde erişildi.

United Nations General Assembly. (2019). General Assembly Resolution 74/247. https://documnts-dds-ny.un.org/doc/UNDOC/GEN/N19/440/28/PDF/

N1944028.pdf?OpenElement eadresinden 4 Haziran 2023 tarihinde erişildi.

United Nations General Assembly. (2021). General Assembly Resolution 75/282. https://documents-dds-ny.un.org/doc/UNDOC/GEN/N21/133/51/PDF/N2113351.pdf?OpenElement adresinden 4 Haziran 2023 tarihinde erişildi.

United Nations General Assembly. (2022). General Assembly Resolution 76/552. https://www.unodc.org/documents/Cybercrime/AdHocCommittee/GA_decision_76-552.pdf adresinden 12 Haziran 2023 tarihinde erişildi.

United Nations Office on Drugs and Crime. (2021a). Organizational session of the Ad Hoc Committee. https://www.unodc.org/unodc/en/cybercrime/ad_hoc_committee/Organizational_session adresinden 3 Haziran 2023 tarihinde erişildi.

United Nations Office on Drugs and Crime. (2021b). The Draft Prepared By The Russian Federation Regarding The Contract. https://www.unodc.org/documents/Cybercrime/AdHocCommittee/Comments/RF_28_July_2021_-_E.pdf adresinden 3 Haziran 2023 tarihinde erişildi.

United Nations Office on Drugs and Crime. (2022a). Road map and mode of work for the Ad Hoc Committee". https://www.unodc.org/documents/Cybercrime/AdHocCommittee/Website/AHC_Road_map.pdf adresinden 6 Haziran 2023 tarihinde erişildi.

United Nations Office on Drugs and Crime. (2022b). Compilation of draft provisions submitted by Member State. https://www.unodc.org/documents/Cybercrime/AdHocCommittee/Second_session/Documents/CRP11.pdf adresinden 2 Haziran 2023 tarihinde erişildi.

United Nations Office on Drugs and Crime. (2022c). Comments and proposals of the Islamic Republic of Iran. https://www.unodc.org/documents/Cybercrime/AdHocCommittee/Second_session/Islamic_Republic_of_Iran_contribution.pdf adresinden 10 Haziran 2023 tarihinde erişildi.

United Nations Office on Drugs and Crime. (2022d). Report of First Session of the Ad Hoc Committee of the United States of America. https://www.unodc.org/documents/Cybercrime/AdHocCommittee/First_session/Comments/USA_National_Statement_-_Cybercrime_AHC.pdf adresinden 10 Haziran 2023 tarihinde erişildi.

United Nations Office on Drugs and Crime. (2022e). Contribution from The Russian Federation. https://www.unodc.org/documents/Cybercrime/AdHoc-Committee/Second_session/Russia_Contribution_E.pdf adresinden 16 Haziran 2023 tarihinde erişildi.

United Nations Office on Drugs and Crime. (2022f). Compilation of proposals and contributions submitted by Member States. https://documents-dds-ny.un.org/doc/UNDOC/GEN/V22/023/23/PDF/V2202323.pdf?OpenElement adresinden 5 Haziran 2023 tarihinde erişildi.

United Nations Office on Drugs and Crime. (2023a). Draft Text Of The Convention. https://documents-dds-ny.un.org/doc/UNDOC/GEN/V23/039/51/PDF/V2303951.pdf?OpenElement adresinden 4 Eylül 2023 tarihinde erişildi.

United Nations Office on Drugs and Crime. (2023b). Fifth session of the Ad Hoc Committee. https://www.unodc.org/unodc/en/cybercrime/ad_hoc_committee/ahc_fifth_session/main adresinden 4 Haziran 2023 tarihinde erişildi.

United Nations Office on Drugs and Crime. (2023c). Draft Text Of The Convention. https://www.unodc.org/documents/Cybercrime/AdHocCommittee/6th_Session/Pre-session-docs/A_AC_291_22_Advance_Copy.pdf adresinden 3 Eylül 2023 tarihinde erişildi.

United Nations Office on Drugs and Crime. (2023d). Consolidated Negotiating Document On The General Provisions. https://www.unodc.org/documents/Cybercrime/AdHocCommittee/4th_Session/Documents/CND_21.01.2023_-_Copy.pdf adresinden 11 Ağustos 2023 tarihinde erişildi.

US Department Justice Office. (2023). Office Of Justice Programs. https://www.ojp.gov/ adresinden 10 Ağustos 2023 tarihinde erişildi.

Usta, A. C. ve Benzer R. (2018). Avrupa Siber Suçlar Sözleşmesi ve Türkiye'nin Dahil Olma Süreci. Uluslararası Bilgi Güvenliği Mühendisliği Dergisi, 4(2), 35-42. DOI:10.18640/ubgmd.512829.