T.C.

İSTANBUL ÜNİVERSİTESİ

SOSYAL BİLİMLER ENSTİTÜSÜ

KAMU HUKUKU ANABİLİM DALI

YÜKSEK LİSANS TEZİ

ULUSLARARASI HUKUKTA SİBER SUÇLA MÜCADELE

ABDULLAH ALDOORİ

2501171778

Tez Danışmanı

Prof.Dr. CÜNEYT YÜKSEL

İSTANBUL-2020

ÖZ

ULUSLARARASI HUKUKTA SİBER SUÇLA MÜCADELE

ABDULLAH ALDOORİ

Günümüzde yaşanan bilişim ve teknoloji evrimi hayatımıza birçok alanda faydalar sağlarken diğer yandan yeni suçluluk tipi olan siber suçun doğmasına neden olmuştur. Siber suç devletlerin arasındaki coğrafi ve siyasal sınırlarını ortadan kaldırmıştır. Bilişim teknolojisi aracılığıyla dünyanın herhangi bir yerinde uzaktan kolaylıkla suç işlenebilmektedir. Dolayısıyla siber suçlar sınır aşan suç olarak nitelendirilmektedir. Ulusal düzlemde yapılan düzenlemeler ve alınan tedbirler bu suçlara karşı yetersiz ve eksik kalmakta ve uluslararası toplumun barışına ve güvenliğine bir tehdit teşkil etmektedir. Bu nedenle siber suçlarla mücadelede devletler arasında işbirliğinin önemi ortadadır.

Siber suçu uluslararası hukuk kapsamında ele alan bu çalışma üç ana bölümden oluşmaktadır. Birinci bölümde siber suçun tarihsel gelişimi, kavramı, kendisine has özellikleri ve siber suçtan ayrı diğer kavramlar açıklanmıştır. İkinci bölümde siber suçlarla mücadelede uluslararası ve bölgesel düzeyde yapılan girişimleri ve düzenlemeleri inceleyerek değerlendirilmeye çalışılmıştır. Üçüncü bölümde ise ilk olarak siber suçlarla mücadelede siber suçun doğasından kaynaklanan sorunlar ardından hukuki zorluklar ortaya konmuştur. Özellikle uluslararası hukuk bazında zorlukların üzerinde durulmuştur. Son olarak Avrupa Konseyi Siber Suç Sözleşmesi'nin siber suçlarla mücadelede karşılaşılan zorlukların üstünden gelmek için getirdiği uluslararası işbirliği rejimi incelenmiştir.

Anahtar Kelimeler: Siber Suçlar, Sınır Aşan Suçlar, Uluslararası İşbirliği, Siber Suçlarla Mücadele, Yetki Zorluğu, Avrupa Konseyi Siber Suç Sözleşmesi.

ABSTRACT

FIGHTING AGAINST CYBERCRIME IN INTERNATIONAL LAW

ABDULLAH ALDOORİ

Nowadays information and technology evolution has brought benefits to our lives in many areas, on the other hand, it has led to the emergence of cybercrime, a new type of criminality. Cybercrime has eliminated the geographical and political boundaries between states. Crime can be easily committed remotely anywhere in the world through information technology. That is why cybercrime is considered as a transnational crime. Regulations and measures taken on the national level are inadequate against these crimes and pose a threat to the peace and security of the international community. Therefore, the importance of cooperation between states in the fight against cybercrime is obvious.

This study, which deals with cybercrime within the scope of international law, consists of three main chapters. In the first chapter, the historical development, concept, characteristics of cybercrime and other cyber threats separately from cyber crime are explained. In the second chapter, it sought to be evaluated by underscoring international and regional regulations to establish international cooperation in the fight against cybercrime. In the third chapter. In the third part, firstly, the challenges in fight against cybercrime arising from the nature of cybercrime and legal difficulties are presented. Specifically emphasis was placed on challenges at the level of international law. Finally, the international cooperation regime introduced by the Council of Europe Cyber Crime Convention to overcome the difficulties encountered in combating cybercrime was examined.

Keywords: Cybercrime, Transnational Crimes, International Cooperation, Combating Cybercrime, Jurisdiction Challenge, Council of Europe Convention on Cybercrime.

ÖNSÖZ

Siber suç sınır aşan bir suç olarak nitelendirmektedir. Bilişim teknolojisi aracılığıyla toprak sınırlarına dayanmadan ve herhangi bir sansüre maruz kalmadan dünyanın herhangi bir yerinde kolaylıkla suç işlenebilmektedir. Siber suç devletlerin arasındaki coğrafi ve siyasal sınırlarını ortadan kaldırmıştır. Belli bir ülkede bulunan kişi başka bir ülkede bulunan bilişim sistemleri aracılığıyla veya bunlara karşı işlenebilmektedir. Aynı zamanda suçun mağduru bambaşka bir ülkede olup etkisi diğer faklı bir ülkede olabilmektedir. Dolayısıyla uluslararası işbirliği olmasa olmaz bir durum meydana gelmektedir. Bu tür suçlar bütün devletleri ilgilendiren bir konudur. Bir devlet siber suçlarla mücadelede uluslararası işbirliğine katılmazsa siber suçlular için güvenli bir sığınak oluşturabilmekte ve bu suçlarla mücadele eden bütün devletleri olumsuz bir şekilde etkileyebilmektedir.

Yapılan çalışmaların çoğunda siber suç olgusu ulusal hukuk kapsamında ele alınmış olup uluslararası hukuk bağlamında işleyen çalışmaların sayısı azdır. Bu noktada bir boşluk olduğunu düşündüm ve bu boşluğu doldurmaya çalıştım.

Yüksek lisans tez konumun belirlenmesinde değerli görüşleriyle bana yardımcı olan saygıdeğer Hocam Yrd. Doç. Khalid Egab Hasun'a teşekkür etmeyi borç bilirim. Tez hazırlama sürecinde katkısı olan ve benden desteklerini esirgemeyen değerli danışman hocam Prof.Dr. Cüneyt Yüksel'e teşekkürlerimi sunarım. Ayrıca tez savunmasında kıymetli görüşlerinden yararlandığım Prof.Dr. İbrahim Kaya ve Prof.Dr. Naim Demiral'e teşekkür ederim. Tez yazmakta her zaman ve her konuda beni destekleyen ve hatalarımı düzelten can dostlarım Av. Eyüp Can ve Özge Ulu'ya ayrıca müteşekkirim.

ABDULLAH ALDOORİ

İSTANBUL, 2020

İÇİNDEKİLER

İKİNCİ BÖLÜM

ULUSLARARASI VE BÖLGESEL ORGANİZASYONLARIN SİBER SUÇLA MÜCADELEDEKİ ROLÜ

ÜÇÜNCÜ BÖLÜM

SİBER SUÇLA MÜCADELEDE KARŞILAŞILAN ZORLUKLAR VE ULUSLARARASI İŞBİRLİĞİ

TABLOLAR LİSTESİ

KISALTMALAR LİSTESİ

A.e. : Aynı eser

a.g.e. : Adı geçen eser

a.g.m. : Adı geçen makale

AB : Avrupa Birliği

ABD : Amerika Birleşik Devletleri

AMERIPOL: Police Community of the Americas

ASEANAPOL : Organisation for the Association of Southeast Asian Nations

AU : Afrika Birliği

b.a. : Eserin bütününe atıf

Bkz : Bakınız

BM : Birleşmiş Milletler

bs. : baskı

C. : Cilt

Çev. : Çeviren

DEÜHFD : Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi

DOS : Denial of Servic

Ed. : Editör

EJIL : European Journal of International Law

ENISA : European Union Agency for Network and Information Security

EUROPOL : Avrupa Polis Ofisi

G7 : Yediler Grubu

GCA: Global Cybersecurity Agenda

GSYİH: Gayri Safi Yurt İçi Hasıla

ICC : International Criminal Law

ICCP : Committee on Information, Communications and Computer Policy

IEEE: The Institute of Electrical and Electronics Engineers

INTERPOL : The International Criminal Police Organization

IP : İnternet Protokolü

ITU: International Telecommunication Union

İÜHFM: İstanbul Üniversitesi Hukuk Fakültesi Mecmuası

K.g. : Karşı görüş.

m. : Madde

No : Numara

OAS : Amerikan Devletleri Örgütü

OECD : Organisation for Economic Co-operation and Development

par. : Paragraf

PC-CY : Siber Alemde İşlenen Suçlar Uzmanları Komitesi

s. : Sayfa

S. : Sayı

TBBD : Türkiye Barolar Birliği Dergisi

TCK : Türk Ceza Kanunu

UNESCO : United Nations Educational, Scientific and Cultural Organization

UNODC : United Nations Office on Drugs and Crime

v.d. : Ve diğerleri

v.s. : Ve saire

Vol. : Volume

WSIS: The World Summit on the Information Society

y.y. : Basım yeri yok

GİRİŞ

Son yıllarda siber suçlar uluslararası güvenliğe ve ekonomiye yönelik oldukça ciddi bir tehdit haline gelmektedir. Dünya Ekonomik Forumu tarafından 2019 yılında hazırlanan küresel risklere ilişkin rapora göre dünyayı tehdit eden en önemli riskler sıralamasında veri hırsızlığı ve dolandırıcılığı dördüncü sırada yer alırken, siber tehditler beşinci sırada yer almaktadır. Güvenlik şirketi olan Kaspersky'ın yürüttüğü 1300 uzman tarafından 11 ülkede yapılan araştırma raporuna göre şirketleri ve organizasyonları tehdit eden siber saldırılar iki yıl içinde daha fazla artmakta olan en büyük üç riskin birincisidir. Bunun yanı sırada 2021 yılında dünya ekonomisinin siber suçlardan kaynaklanan kayıpların 6 trilyon dolara ulaşacağı tahmin edilmektedir[1]. Ayrıca 2018 yılında yapılan bir çalışmaya göre siber suçlardan elde edilen kazanç yıllık en az 1,5 trilyon dolardır[2]. Bu Rusya'nın GSYİH'sine eşdeğerdir. Siber suç, Guccifer 2.0 tarafından yönetilen bir devlet olursa dünyanın en yüksek 13. GSYİH'sine sahip olabilmektedir[3].

Günümüzde baş döndürücü bir hızla gelişen internet ve bilişim teknolojisi hayatımızın bütün alanlarına girmekte ve vazgeçilmez hale gelmektedir. Ticaret, eğitim, sosyal, haberleşme, alışveriş bilimsel araştırmalar, sanat, endüstri, iletişim ve her alanda birçok kolaylık ve avantaj sağlamaktadır. Yeni teknolojiler geleneksel postalar, telefon, televizyon gibi klasik iletişim araçlarının yerini almış ve dünyayı global bir köy hale getirmiştir. Bu sayede zaman ve mekan kavramlarını büyük bir değişikliğe uğratmaktadır. Her hangi bir kişi dünyanın herhangi yerine kolaylıkla ulaşabilmektedir.

---

[1] Andrii Borko, v.d., "Fighting Against Cybercrime: Problems and Prospects in Ukraine and the World", **Journal of Legal, Ethical and Regulatory Issues,** Vol. 22, No.2, 2019, s. 1.

[2] Mike Mcguire, **Into The Web of Profit An In-Depth Study of Cybercrime, Criminals and Money**, California, Bromium, Inc., 2018, s. 15.

[3] Patrick Nohe, "Cybercrime Pays: New Study Finds Cybercriminal Revenues Hit $1.5 Trilyon Annually", (Çevrimiçi), https://www.thesslstore.com/blog/cybercrime-pays-new-study-finds-cybercriminal-revenues-hit-1-5-trillion-annually/, Erişim Tarihi: 10.11.2019.

Ancak her yeni çıkan teknoloji olduğu gibi, bilişim teknolojileri bir yandan kolaylıklar sağlarken diğer yandan yeni olumsuzluklar ve sorunlar ortaya çıkarmaktadır. Bu teknolojiler her alanı etkilediği gibi özellikle hukuk alanını uluslararası hukuku da büyük bir şekilde etkilemektedir. Yeni teknolojilerin kötü niyetli kişiler tarafından hukuka aykırı eylemlerde bulunmak için kullanımına müsaade edilmiştir. Devletlerin ulusal güvenliğine, bireylerin hayatına ve malvarlığına karşı işlenen yeni suçluluk tipi olan siber suçların doğmasına veya geleneksel suçların yeni araçlarla işlenmesine sebep olmuştur.

Bilişim teknolojisinin yaratığı yeni ortam olan siber uzay herhangi bir sınır tanımamaktadır. Hızlı artan siber suçlar internet veya diğer bilişim teknolojisi aracılığıyla işlendiğinden devletlerin arasındaki coğrafi ve siyasal sınırlarını ortadan kaldırmaktadır. Siber suç işleyebilmek için diğer ülkelerle fiziksel bağlantının olmasına gerek kalmamıştır. Siber suçlular, ulusal sınırları aşarak dünyanın herhangi bir yerinden uzaktan kolaylıkla suç işleyebilmektedirler. Bu durumda bir devlette işlenen siber suçun mağduru veya etkisi bambaşka bir ülkede de olabildiği gibi aynı ülkede işlenip hizmet sağlayıcı başka ülkede olabilmektedir. Mutfağında kahve içen bir Rus tarafından evinden çıkmadan ABD'de veya Çin'de bulunan herhangi bir kişiye veya aktöre ait bilişim sistemine veya bunun içeriğine karşı suç işlenebilmektedir. Dolayısıyla siber suç sınır aşan bir suç olarak değerlendirilmektedir.

Siber suç küresel niteliği itibarıyla uluslararası toplumun barış ve güvenliğini tehdit etmektedir. Ulusal düzeyde yapılan düzenlemeler ve alınan tedbirler siber suçlara karşı yetersiz ve eksik kalmakta ve uluslararası topluma bir endişe kaynağı oluşturmaktadır. Devletlerin bu suçlarla etkin bir mücadele vermek için birlikte eyleme geçmeleri gerekmektedir. Global suçlar global mücadele gerektirmektedir. Dolaysıyla bu noktada uluslararası işbirliği kaçınılmazdır.

Siber suçlarla ilgili birçok çalışma yapılmaktadır. Ancak yapılan çalışmaların çoğunda bu olgu ulusal hukuk kapsamında ele alınmış olup uluslararası hukuk bağlamında işleyen çalışmaların sayısı oldukça azdır. Siber suçlar bütün devletleri ilgilendiren bir konudur. Bir devlet siber suçlarla mücadelede uluslararası işbirliğine

katılmazsa siber suçlular için güvenli bir sığınak oluşturabilmekte ve bu suçlarla mücadele eden bütün devletleri olumsuz bir şekilde etkileyebilmektedir. Siber suçlar uluslararası hukukun en önemli gündemlerinden biri haline gelmiştir. Dolayısıyla uluslararası hukukta ele alınması büyük önem arz etmektedir. Bu çalışmanın önemi bu noktadan kaynaklanmaktadır.

Bu çalışmada sınır aşan siber suçla nasıl mücadele edilebilir sorusuna cevap verilmeye çalışılmaktadır. Bu bağlamda araştırmanın amacı siber suçun uluslararası hukuktaki yerini ve önemini yansıtmak, siber suçlarla mücadelede uluslararası işbirliğine yönelik girişimleri ortaya koymak, uluslararası bazda siber suçlarla mücadelede zorlukları tespit etmek ve bu zorlulukların üstesinden nasıl gelinebileceği konusunda çözümler bulmaya çalışmaktır. Bu nedenle bu çalışma hem teorik hem de uygulama bakımından oldukça önem taşımaktadır.

Bu kapsamda çalışma üç ana bölümden oluşmaktadır. Birinci bölümde siber suçun mahiyesinin anlaşılması için ilk olarak tarihsel gelişimine, siber suçun hem terimi hem de tanımı konusunda hukuk literatüründeki tartışmalara, farklı görüşlere ve uluslararası girişimlere yer verilecektir. Siber suçları klasik suçlardan ayrı kılan ve kendine özgü özelliklerinin, yapılan çeşitli sınıflandırmalarının ve türlerinin, siber terör, siber savaş, siber saldırı gibi siber suça benzeyen diğer kavramların üzerinde durulacaktır.

İkinci bölümde siber suçlarla mücadelede uluslararası ve bölgesel düzeyde yapılan düzenlemelerin ve çalışmaların üzerinde durulacaktır. Bu kapsamda ilk olarak Birleşmiş Milletler, Yediler Grubu (G7), Ekonomik Kalkınma ve İşbirliği Örgütü (OECD), Uluslararası Telekomünikasyon Birliği ve İnterpol tarafından siber suçlara ilişkin yapılan çalışmalar incelenecektir. Ardından bölgesel bazda olan Avrupa Konseyi, Avrupa Birliği, Arap bölgesindeki organizasyonları, İngiliz Milletler Topluluğu, Afrika Birliği ve Amerikan Devletler Örgütü tarafından yapılan antlaşmalar ve çalışmalar irdelenecektir.

Çalışmanın üçüncü bölümünde ise öncelikle siber suçlarla mücadelede zorluluklar ortaya konacaktır. Bu kapsamda siber suçlarla mücadelede, siber suçun

doğasından kaynaklanan sorunlar ardından, hukuki anlamda ulusal düzeyde ve uluslararası düzeyde zorluklar bulunmaktadır. Uluslararası bazda zorluklar, yetki zorluğu ve uluslararası işbirliğine ilişkin zorluklardır. Siber suçlarla mücadelede uluslararası işbirliğiyle ilgili zorluluklar ise devletlerin hukuk sistemlerinin farklılığı, uluslararası sözleşmelerin eksikliği ve prosedürlerin hantal ve uzun olmasıdır. Ardından siber suç konusunda şu ana kadar yapılan en kapsamlı metin olan ve büyük önem taşıyan Avrupa Konseyi siber Suç Sözleşmesi'nin uluslararası işbirliğine ilişkin hükümleri incelenecektir.

BİRİNCİ BÖLÜM

SİBER SUÇUN GENEL ÇERÇEVESİ

1.1.Siber Suçun Gelişimi

Siber suçların tarihi gelişimine yer verilmesi önem arz etmektedir. Bu gelişim, siber suçun işlenme şekline, siber suç olgusu ile ilgili hukuki çalışmalara ve bu suçlarla mücadele eden düzenlemelere yansımaktadır. Bu başlık altında siber suçun bilgisayarla paralel olarak ortaya çıkışı, tarihsel gelişimi, ardından siber suçlar uluslararası boyutu ve siber suçlar hakkındaki bazı istatistiklerin üzerinde durulacaktır.

1.1.1.Siber Suçun Ortaya Çıkışı

Bilgi toplumunu temsil eden ve siber suçun temel aracı olan bilgisayarların ortaya çıkışı yıllar öncesine dayanmaktadır. Bugün kullanılan bilgisayarlar çok gelişmiş teknoloji nedeniyle geçmişteki bilgisayarlardan oldukça farklıdır. Bilgisayarların ilk ortaya çıktığı zamanlar kullanıcıların daha sınırlı olduğu ve genellikle bilimsel araştırmalar amaçlı kullanımı yapıldığı bilinmektedir. Ayrıca bilgisayarların kapalı yerlerde bulunması hafızasındaki bilgilere ulaşmayı zorlaştırmıştır. Bu nedenlerden dolayı bilgisayarlar ilk icat edildiğinde belirli bir süre için güvenli kalmış olup suç işlenme endişesiyle karşılaşılmamıştır[4]. Daha sonra taşınması ve kullanımı daha kolay ve yaygın hale gelen kişisel bilgisayarlar, günümüz dünyasında faydalarının yanında belirli başlı bazı sorunlara da sebep olmuştur[5].

1966 yılına dek siber suç olgusundan bahsedilmemiştir. Günümüzde hızlı bir şekilde gelişen bilgisayarın getirdiği olumsuz sonuçlarla birlikte siber suçları da vücut bularak ortaya çıkmış ve zaman ilerledikçe çoğalan bu suçların yeni çeşitleri belirmeye

[4] Debra Littlejohn Shinder, Ed Tittel, **Scene of The Cybercrime Computer Forensics Handbook**, Massachusetts, Syngress Publishing, 2002, s. 50.
[5] Yüksel Ersoy, "Genel Hukuki Koruma Çerçevesinde Bilişim Suçları", **Ankara Üniversitesi Siyasal Bilimler Dergisi**, C. XLIX, S. 3, 1994, s. 152.

başlamıştır. Bu nedenle siber suçların, bilgisayarın yaygın bir şekilde kullanılmaya başlamasıyla birlikte ortaya çıktığını söylemek mümkündür[6]. Bilgisayar ve internet kullanımının bütün kişilere açık olması, bunlar aracılığıyla işlenen suçların ortaya çıkmasına neden olmuştur. Bu suçlara klasik ceza hukuk kuraları uygulanması sonucunda ise birçok hukuki sorun meydana gelmiştir. Dolayısıyla bu suçların ceza kanunlarında düzenlenmesine ihtiyaç duyulmuştur[7].

1.1.2.Siber Suçun Tarihsel Gelişimi

Siber suçlar tarihsel olarak 20. yüzyılın altmışlı yıllarına dayanmaktadır. Bu dönem içerisinde bilgisayarlar yeni yeni kullanılmaya başlanmıştır. İlk kez olarak büyük kurumlar ve şirketler tarafından bilgisayarlar kullanılmıştır. Dolayısıyla bilgisayarlar aracılığıyla işlenen suçlar yavaş yavaş gündeme gelmeye başlamış, gazetelerde yer almış ve bilimsel makalelere de konu olmuştur. Özellikle siber suçlara ilişkin internet veya telefonun ücretli hizmetlerinin ücretsiz bir şekilde kullanılması [8], yetkisiz bilgisayar kullanımı, bilgisayar korsanlığı ve bilgisayar manipülasyonu gibi konular tartışılmıştır. Ancak bu bilgiler gazete haberlerine dayandığı için siber suç olgusunun gerçekten mevcut olup olamadığı etraflı bir şekilde ele alınmıştır[9].

Bu dönemde bilgisayarların odalar büyüklüğünde yerlere ihtiyaç duyması ve internete bağlı olmaması suç işlemeyi oldukça zorlaştırmıştır. Ayrıca bilgisayarlar sadece profesörler, araştırmacılar ve bazı öğrenciler tarafından kullanılmıştır. Dolayısıyla bu dönemde işlenen suçlar basit ve sayıca az olmuştur[10]. Söz konusu siber

[6] Bazı yazarlar, bu konuya başka bir bakış açısıyla bakmaktadırlar. Onlara göre siber suçlar, iyi niyetli bilgisayar korsanları (The White Hats) ve kötü niyetli bilgisayar korsanların (The black hats) ortaya çıkmasıyla başlamıştır. İyi niyetli bilgisayar korsanları Şirketler, hükümetler ve finansal kuruluşların menfaatleri için çalışmaktadırlar. bkz: Berandette H. Schell, Clemens Martin, **Cybercrime A Reference Handbook**, California, ABC-CLIO, 2004, s. 4-9.

[7] Murat Volkan Dülger, **Bilişim Suçları ve İnternet İletişim Hukuku**, 7. bs., Ankara, Seçkin Yayınları, 2018, s. 51.

[8] Rüya Şamlı, "Türk ve Dünya Hukukunda Bilişim Suçları", Akademik Bilişim'10 - XII. Akademik Bilişim Konferansı Bildirileri 10 - 12 Şubat 2010 Muğla Üniversitesi, s. 97.

[9] Ulrich Sieber, **Legel Aspects of Computer - Related Crime in The Information Society (Comcrime Study),** European Commissio, y.y., 1998, s. 18.

[10] Chuck Easttom, Jeffrey Taylor, **Computer Crime, Investigation and the Law**, Boston, Cengage Learning, 2011, s. 33.

suçlar sadece bu bilgisayarlarla doğrudan bağlantı kurabilen çalışanlar tarafından işlenmiştir. Konuyla alakalı kişiler kendi maddi menfaatleri için bilgisayarı haksız amaçları için kullanmışlardır. O nedenle bu zaman zarfında en çok işlenen siber suçlar mali suçlardır[11]. Bundan ziyade bilgisayar sistemlerine ve depolanan verilere fiziksel hasar verilmesi şeklinde de gündeme gelmiştir[12].

Bunun yanında bankacılık sektörünün gelişmesiyle beraber kişisel veriler işlenmeye ve kullanılmaya başlanmış olup sonucunda bilgisayar manipülasyonu ve casusluk suçları gibi veri gizliliğine aykırı olan birçok problem ve tehdit doğmuştur[13]. Örneğin, işlenen ilk siber suç ABD'de 1966 yılında kaydedilmiştir. Amerikan gazetesinde "bilgisayar uzmanı banka hesabında tahrif yapmakla suçlanıyor" başlıklı makale yayınlanmıştır[14]. Söz konusu bu olayda fail, Minneapolis City Bank'ta bulunan bilgisayarların programlanması ve onarımı kısmında çalışırken bankanın bilgisayarında manipülasyon yaparak kendi hesabına 1352 dolar çekmiştir[15].

1970'li yıllarda devamlı bir şekilde geliştirilen bilgisayarın daha küçük ve ucuz olmasıyla birlikte kullanımı da paralel olarak artmıştır. Özellikle idari ve ticari işlemler bilgisayarlar aracılığıyla yapılmaya başlanmıştır. Dolaysıyla bu dönemde bilgisayar sistemlerine karşı işlenen suçların yeni şekilleri olarak bilgisayar verilerinin manipülasyonu, bilgisayar aracılığıyla sahtecilik ve yasa dışı bilgisayar sistemi kullanımı gibi suçlar ortaya çıkmıştır[16]. Özellikle bilgisayarla ilgili dolandırıcılık milyonlarca dolar değerinde kayıplara sebep olmuştur[17]. Bu suçlara örnek vermek gerekirse Almanya'daki bir şirkette iki çalışan şirketin bilgisayarına sahte fatura

---

[11] Susan W. Brenner, **Cybercrime: Criminal Threats from Cyberspace**, California ABC-CLIO, 2010, s. 11.
[12] Marco Gercke, **Understanding Cybercrime: Phenomena, Challenges and Legal Response,** Geneva, International Telecommunication Union Publication, 2014. s. 13.
[13] Ebru Altunok, Ali Fatih Vural, "Bilişim Suçları", **Denetişim**, S.8, 2011, s. 76.
[14] Emin Doğan Aydın, **Bilişim Suçları ve Hukukuna Giriş**, Ankara, Doruk Yayınları, 1992, s. 13.
[15] Berrin Akbulut, **Bilişim Alanında Suçlar**, 2.bs, Ankara, Adalet Yayınevi, 2017, s. 51.
[16] Gerald L. Kovacich, William C. Boni, **High-Technology-Crime Investigator's Handbook: Working in the Global Information Environment**, Oxford, Elsevier, s. 55.
[17] Gercke, **a.g.e.**, s. 13.

işleyerek kendi hesaplarına 295,000 mark miktarında para aktarmıştır. Suçun ortaya çıkmasını engelleyebilmek için ise şirket yönetenlerinin imzası taklit edilmiştir[18].

Bu dönemde araştırmacıların siber suç olgusu ile ilgili ampirik çalışmalar yaptığına şahit olunmuştur. Söz konusu bu çalışmalar sınırlı sayıda suçlara uygulanmasına rağmen, keşfedilmemiş veya ihbar edilmemiş suçları da öngörmüştür[19]. Üstelik bu yıllarda siber suç olgusuna ilişkin birçok kitap yazılmıştır. Örneğin, 1974 yılında "Computer Crime" adlı kitap, Gerald Macknight, 1978 yılında "Computer Crime" adlı kitap Donn B. Parker ve 1979 yılında "Computer Fraud and Countrmeasures" adlı kitap Leonard I. Kurauss tarafından yazılmıştır.

Mevcut ceza kanunlarının siber suçlara uygulanmasının hukuki zorluklara neden olması devletlerin siber suçlarla ilgili yasalar ortaya çıkarmasına öncü olmuştur. 1973 yılında İsveç, Veri Korunması Kanunu'nu çıkarmasıyla bilgisayarlara ilişin bazı fiilleri yasaklayan ilk devlet olmuştur, ardından birçok devlet te bu konuda kanunlar çıkarmıştır. 1974'te ABD, 1977'te Almanya, 1978 yılında ise Fransa, Danimarka, Avustralya ve Norveç bu suçlarla ilgili yasa çıkarmıştır[20].

Siber suçların niceliği ve niteliği 1980'li yıllarda değişmiştir. Kişisel bilgisayarların üretilmesi ve herkese kullanıma açık olmasıyla birlikte program korsanlığı, elektronik para sistemi manipülasyonu ve iletişim sistemlerinin kötü kullanımı gibi kavramlar ortaya çıkmıştır. Ayrıca birçok virüs ve elektronik kurt yaygınlaşmıştır. Aynı zamanda bu suçların hukuk tarafından korunan her menfaate karşı işlenebileceği ortaya çıkmıştır[21]. Dolayısıyla siber suç olgusuna ilişkin tehlikenin gelecekte daha fazla artacağı ve bunun kontrol altında tutulması gerektiği kanaatine varılmıştır. Bu dönemde siber suçların çoğu bilgisayar sistemlerine karşı işlenmiştir.

[18] Akbulut, **a.g.e.**, s. 51.
[19] Bkz: Marc D. Goodman ,Susan W. Brenner, "The Emerging Consensus on Criminal Conduct in Cyberspace", **International Journal of Law and Information Technology**, Vol. 10, No. 2, 2002, s. 163.
[20] Sieber, **a.g.e.**, s. 19.
[21] Akbulut, **a.g.e.**, s. 52.

Örneğin, 1988 yılında ABD'de bir öğrenci tarafından üretilen internet kurdu aracılığıyla internet ağlarına bağlı nerdeyse 6,000 bilgisayar çevrimdışı bırakılmıştır[22].

Zira bu dönemde siber suçlara ilişkin kanunu olmayan bazı devletler yasalar çıkarmaya başlamıştır. Örneğin İngiltere'de 1981 yılında çıkan siber suçlarla ilgili kanununda sahtecilik tanımı ve veri depolamanın çeşitli araçları ele alınmıştır. Ayrıca Kanada 1985 yılında ceza kanununda değişiklik yaparak siber suçlar için maddeler eklemiştir. Fransa ise ceza kanunları geliştirmiş ve 1988 yılında siber suçlar ve verilen cezalara ilgili bir kanun çıkarmıştır.[23] Nitekim Arap ülkeleri de bu dönemde siber suçlarla ilgilenmeye başlamıştır. Örneğin, 1986 yılında Sudi Arabistan'ın içişleri bakanlığındaki ulusal bilgi merkezi tarafından "bilgisayarda bilgi güvenliği" başlıklı bir konferans düzenlenmiştir[24]. Aynı zamanda bu olguya ilişkin birçok Arapça kitap yazılmıştır.

1990'lı yıllarına gelindiğinde siber suçlar alanında oldukça büyük bir gelişme olmuş ve siber suç kavramı ve kapsamı değişmiştir. Uluslararası internet ağlarının (WWW) yaygınlaşmasıyla birlikte dünyanın her yerine ulaşma kolaylığı sağlanmış ve bu ağların kullanıcılarının sayısı hızlı bir şekilde artmıştır. Bu nedenle siber suçlar bu dönemde büyük artış göstermiştir. Üstelik bilgilerin uluslararası bazda hızlı alışverişiyle ilgili endişeler ortaya çıkışmıştır. Daha önceleri çocuk pornografisi, kitap ve kasetleri fiziksel yollarla dağıtılırken, bu yıllar web siteleri bu yıllarda web siteleri ve İnternet hizmetleri aracılığıyla çevrimiçi paylaşılmaya başlanmıştır. Böylece siber suçlar yerel düzeydeyken, internet ve diğer ağların ortaya çıkmasıyla birlikte sınır aşan bir suça dönüşmüştür[25]. Örneğin, Rusya'da 1994 yılında hacker Vladimir Levin'in yönettiği bir çete, elektronik para sistemiyle çalışan Citibank'ın sistemine girip Rusya,

---

[22] Kısa bir süre içerisinde The New York Times gazetesi tarafından hacker olan Robert Morris'ın bu suçu işlemiş olduğu tespit edilmiştir. Ayrıca Morris, 1986 yılında çıkan Bilgisayarla ilgili Dolandırıcılık ve Kötü Kullanım Kanunu'na aykırı davrandığından dolayı suçlanmıştır. Dolaysıyla Moris üç yıl hapis ve 10,000 dolar adli para cezasına çaptırılmıştır. Bill Gates, **The Road Ahead**, USA, Viking, 1995, s. 96-97.

[23] Yusuf Hasan Yusuf, **El Ceraim el Duveliye li İnternet**, Kahire, El merkez el Kavumi li el İsdarat el Kanuniye, 2011, s. 80.

[24] Faiz Bin Abdullah Elşehri,"EL Tahdiyat el Emniye el Musahibe li Vesail el İtisal el Cedide", **El mecele el Arabiye li Dirasat ve el Tedrib**, C.XX, S. 39, 2003, s. 172.

[25] Gercke, **a.g.e.**, s. 13.

Almanya, Finlandiya, Hollanda, İsrail ve ABD'deki hesaplarına 10 milyon dolar miktarında para transfer etmiştir[26]. Diğer bir örnek 1994 yılında, İngiltere'de "Data Stream" Veri Akışı kullanıcı adını kullanan 16 yaşındaki bir çocuk, dünyanın en büyük kurumlarından olan Griffith Hava Kuvvetleri Üssü, NASA ve Kore Atom Araştırma Enstitüsü çeşitli kritik sistemlere erişmiştir[27].

Bu dönemde siber suçlara ilişkin bir düzenlemeye ihtiyaç duyan Türkiye, ilk olarak 1991 yılında 765 sayılı TCK'ye "bilgileri otomatik işleme tabi tutan sistem" ifadesi eklenmesiyle bu suçları ele almıştır. Halen yürüklükte olan TCK'de bu tür suçlar "Bilişim Alanında İşlenen Suçlar" başlıklı olan bölüm 10. Bölümünde dört maddeyle düzenlenmiştir[28].

2000'li yıllarda ise siber suçlar artıp gelişmeye devam etmiştir. Ancak bu sefer inanılmaz bir hızla yayılan virüs ve solucan şeklinde baş göstermiştir. Bu dönemde bilgisayar sistemlerine karşı virüsler kullanılmaya başlanmıştır. 2000 yıllında "Mellisa", "love Bug" ve "killer Resume" olan virüsler ciddi büyüklükteki maddi kayıplara neden olmuştur[29].

Günümüzde internet ve bilişim teknolojisi geliştikçe siber suçların yeni yöntemler, güncel araçlar ve şekillerle karşımıza çıkmaktadır. Pek çok devlet bu suçlarla mücadele edebilmek adına birçok tedbir almış ve bununla ilgili kanunlar çıkarmıştır. Ancak siber suçların küresel niteliği dolayısıyla devletler ve uluslararası organizasyonlar uluslararası düzeyde çözümler aramaya başlamıştır.

1.1.3. Siber Suçun Uluslararası Boyutu

Gün geçtikçe gelişen teknoloji, her alanı etkilediği gibi uluslararası hukuku da etkilemiştir. Bilgisayar ve internetin özellikle dünya çapında ağların herkese

[26] Hedieh Nasheri, **Economic Espionage and Industrial Spying**, Cambridge, Cambridge University Press, 2005, s. 39.
[27] Chuck, Taylor, **a.g.e.,** s. 46.
[28] Hüseyin Akarslan, **Bilişim Suçları**, 2.bs., Ankara, Seçkin Hukuk, 2015, s. 43.
[29] Joseph Migga Kizza, **Computer Network Security**, Boston, Springer, 2005, s. 141.

açılmasıyla kullanıcı sayıları hayli artmış ve siber suç olgusunun yeni, tehlikeli boyutu ortaya çıkmıştır. Dolayısıyla bu noktada her bilgisayar kullanıcısı ceza mahkemelerinde olası suçlu veya mağdur olarak bulunabilmektedir.

Bunun yanı sıra internet ağları, devletlerin coğrafi ve siyasal sınırlarını kaldırmış olup siber suçlarla mücadele etmeye çalışanlara ve kolluk kuvvetlerine yeni bir yük yüklemiştir. Diğer bir deyişle siber suç işleyebilmek için diğer ülkelerle fiziksel bağlantının olmasına gerek kalmamıştır. Artık suçlular, ulusal sınırları aşarak dünyanın herhangi bir yerinde uzaktan kolaylıkla suç işleyebilmektedirler[30]. Bu durumda bir devlette işlenen siber suçun mağduru veya etkisi bambaşka bir ülkede olabildiği gibi aynı ülkede işlenip hizmet sağlayıcı başka ülkede olabilmektedir.[31] Ayrıca bazı insanlar fiziksel alanlarında statü ve sahip oldukları pozisyonu suç işlemezken, siber uzayının sunduğu kolaylıklarla örneğin kimlik esnekliği, anonimlik ve kimliğin gizlenmesi özellikle ciddi caydırıcı faktörlerin eksikliğinden dolayı siber uzayda suç işleyebilmektedirler[32]. Dolayısıyla siber suçlar sınır aşan bir suç olarak nitelendirilmektedir.

Siber suçlar genellikle yabancılık unsurunu taşıdığı[33] ve uluslararası toplumunun barış ve güvenliğini tehdit ettiğinden dolayı uluslararası hukukun konusunu teşkil etmektedir[34]. Siber suçlarla mücadelede ulusal düzeyde yapılan çalışmaların ve alınan tedbirlerin yeterli olamamasından dolayı uluslararası düzeyde de çalışmalar yapmak gerekmektedir[35]. Bu suçlarla mücadelede devletler arası işbirliği sağlamak maksadıyla bölgesel ve uluslararası düzeyde birçok çalışma yapılmıştır. Örneğin, Birleşmiş Milletler 'in siber suçlara ilişin kararları, bölgesel düzeyde ise 2001

---

[30] Ed Gabrys, "The International Dimensions of Cyber-Crime Part 1.", **Information Systems Security,** Vol.11, No. 4, 2002, s. 22-23.

[31] Bilal Şen, Mahmut Çengiz,"Bir Sınıraşan Suç Türü Olarak Bilişim Suçları", **Sınıraşan Organize Suçlar, Kavramlar, Yöntemler, Eğilimler**, Ed, Oğuzhan Ömer Demir, Bahadır Küçükuysal, 3.bs., Ankara, Adalet Yayınevi, 2013, s. 69.

[32] Steven Malby v.d., **Comprehensive Study on Cybercrime**, New York, United Nations Office on Drugs and Crime, 2013, s. 8.

[33] Murat Volkan Dülger, **Suç Gelirlerinin Aklanmasına ilişkin Suçlar ve Yaptırımlar**, Ankara, Seçkin Yayıncılık, 2011, s. 284.

[34] Neil Boister "Transnational Criminal Law?", **EJIL**, Vol. 14, No. 5, 2003, s. 954.

[35] Merve Erdem , Gürkan Özoczk, "Sınıraşan Bir Suç Olarak Siber Suçlarla Mücadelede Uluslararası İşbirliği", , **19. Akademik Bilişim Konferansı Bildiri Kitabı**, Aksaray Üniversitesi, 2017, s. 2.

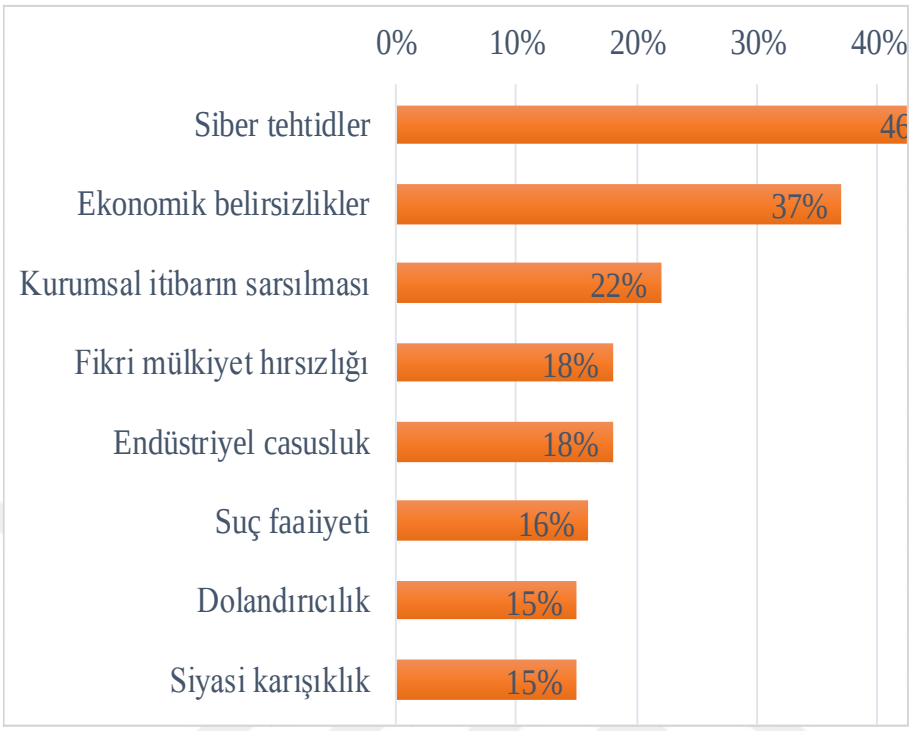
yılında yapılan en önemli olan çalışma Avrupa Konseyi Siber Suç Sözleşmesi ve daha sonra da 2010 yılında Bilişim Suçlarına İlişkin Arap Sözleşmesi'dir. Söz konusu çalışmalar ve sözleşmeler bu çalışmanın ikinci bölümünde yer alacaktır.

1.1.4 Siber Suç Hakkında İstatistikler

Son yıllarda siber suçlar sorunu oldukça önemli bir konu haline gelmiştir. 2005-2012 yılları arasında siber suçlar, klasik suçlara oranla %600 oranında artmıştır[36]. Sayısı ve karmaşıklığı artan siber suçları çözümlemek çok fazla zaman aldığı için bu durum maliyetleri olumsuz etkilemektedir. Kamu ve özel sektörlere yapılan siber atakların ortalama güvenlik ihlalleri %11'lık bir artış göstermiştir. 2017 yılında ortalama güvenlik ihlali 130 iken 2018 yılında 145'e çıkmıştır. Bunun yanında siber suçların şirketlere toplam maliyeti %12 artmıştır. 2017 yılında bu rakam 11.7 milyar dolarken 2018 yılında 13.0 milyar dolara çıkmıştır. Ayrıca bu rakamın gelecek beş yılda (2019-2023) 5.2 trilyon dolara çıkacağı tahmin edilmiştir[37].

Son İki Yılda Dünyada Gelişen En Önemli Riskler Sıralaması. Tablo (1)

[36] Steven Malby, v.d., **a.g.e.**, s. 7.
[37] The Cost of Cybercrime, (Çevrimiçi), https://accntu.re/30PiK9a, Erişim Tarihi: 19.07.2019, s. 2. Bu araştırmaya 11 ülkede yürütülen 351 şirket katılmıştır.



Siber suçların sayısının ve maliyetinin artmasının yanında tehlikesi de artmıştır. Dünya Ekonomik Forumu'nun 2019 küresel riskler raporunda veri hırsızlığı ve dolandırıcılığı dördüncü sırada yer almış olup, siber tehditler ise beşinci sırada yer almıştır[38]. Dahası birçok şirket ve organizasyon siber saldırıları finansal açıdan en çok risk taşıyan faktörler arasına koymuştur. Kaspersky'ın[39] yürüttüğü 1300 uzman tarafından 11 ülkede yapılan araştırma raporuna göre örgütleri tehdit eden siber saldırılar gelişmekte olan en büyük üç riskin birinci sırasında yer almaktadır. Yukarda yer alan tabloda görüldüğü gibi küresel olarak gelişen risklerin ilk üçü sırasıyla şunlardır; siber tehditler, resesyon gibi ekonomik belirsizlikler, markanın zarar görmesi veya kurumsal itibarın sarsılmasıdır. Raporun diğer bulgularına göre organizasyonların % 91'i finansal kazanç elde etmek için gerçekleştirilen siber

[38]World Economic Forum, The Global Risks Report 2019 14th Edition, (Çevrimiçi), http://www3.weforum.org/docs/WEF_Global_Risks_Report_2019.pdf, Erişim Tarihi: 21.11.2019, s. 11-12.

[39] Kaspersky veya Kaspersky Lab, Rusya Merkezli olan güvenlik şirketi, Dünyanın en önemli anti virüs yazılımı, bilgisayar ve internet güvenliği üzerine çözümler üretmektedir.

saldırılara maruz kalırken, %53'ü siber tehditlerden kaçınmak amacıyla sosyal ağ sitelerini yasaklamıştır[40].

En Çok Kazandıran Siber Suçların Beş Çeşidi. Tablo (2)

Suç	Yıllık gelir
Yasa dışı çevrimiçi marketler	860 milyar dolar
Ticari sır, IP hırsızlığı	500 milyar dolar
Veri ticareti	160 milyar dolar
Suç Yazılımları, (Hizmet Olarak Siber Suçlar)	1.6 milyar dolar
Ransomware (Fidye)	1 milyar dolar

Diğer yandan siber suçlardan elde edilen maddi kazanç epey artmıştır. Yeni bir suç ekonomisi olarak siber suçlar her yıl en az 1,5 trilyon dolar gelir yaratmaktadır. Zira muhafazakâr bir tahmine dayan verilere göre en yüksek kazanç elde eden siber suçların 5 çeşidi yukardaki şekildeki gibi belirlenmiştir[41].

Aslında siber suçların topluma verdiği zararları neredeyse tüm alanlarda gözlemlemek mümkündür. Siber zaralar beş kategoriye ayrılmıştır. Bunların ilki olan fiziksel ya da dijital zarar hasar görme, tahrip, hırsızlık, bedensel yararlanma veya istismar gibi zararları içerirken, ekonomik zarar ise operasyonların sekteye uğraması, satışların durdurulması, müşteri kaybı, karın düşmesi, finansal hırsızlık vb. zararlar içermektedir. Aynı zamanda psikolojik olarak karışıklık, rahatsızlık, kötü hissetme, depresyon, suçlu hissetme, hayal kırklığı vb. olumsuzluklara neden olurken itibarın zarar görmesindeyse olumsuz kamu algısı, şirkete olan güven sarsılması, müşterilerle ilişiklerin bozulması, yeni iş fırsatlarında azılma gibi olumsuzluklara da neden olmaktadır. Son olarak ise sosyal ve toplumsal, kamu algısındaki olumsuz

[40] Ready... or not? Balancing future opportunities with future risks, A Global Survey into Attitudes and Opinions on IT Security (Çevrimiçi), https://bit.ly/2Z5oF9M, Erişim Tarihi: 21.07.2019, s. 5-7.
[41] Mcguire, **a.g.e.**, s. 15.

değişiklikler, günlük yaşam faaliyetlerinde bozulma, millet üzerinde olumsuz etki, maneviyatın düşmesi gibi zararları kapsamaktadır[42].

Bu istatistiklere rağmen siber suçların gerçek işlenme sayısı ve etkilerini ölçmek mümkün değildir. Mağdur siber suça maruz kaldığını ve nasıl ihbar edeceğini bilmemesi nedeniyle veya çekindiğinden dolayı siber suçu ihbar etmez. Ayrıca bazı şirketler itibarları zedelenecek korkusuyla siber suça maruz kaldığını itiraf edemez[43]. Ancak bahsedilen rakamların her ne kadar gerçeği yansıttığı düşünülse de siber suçların etkisi ve devlet ekonomilerine verdiği zarar daha yüksek olabilmektedir. Özellikle siber suçlardan elde edilen kazancın artmasıyla birlikte siber suçların işlenme oranının ve etkilerinin katlanarak arttığı düşünülmektedir.

1.2.Siber Suç Kavramı

Siber suçlarla mücadele edebilmek için öncelikle yapılması gereken ilk adım siber suçu tanımlamaktır. Siber suçun yeni ve sürekli gelişen bir kavram olması nedeniyle tanımlanmasına bir çerçeve çizmek oldukça güçtür[44]. Zira siber suçun tanımı herhangi bir ulusal ya da uluslararası mevzuatlarda bulunmamaktadır. Dolayısıyla bu suçlar "çizgisiz çerçeveli suçlar" [45] olarak adlandırılmıştır. Siber suç terimi de sorun haline gelmiştir. Hukukçular, yazarlar, öğreticiler ve uygulamacılar tarafından birçok tanım yapılmıştır. Ancak herhangi birinde uzlaşmaya varılmamıştır. Bu kısamda siber suç terimi, tanımı ardından uluslararası mevzuatlarda siber suçun tanımı ele alınacaktır.

---

[42] Ioannis Agrafiotis, v.d.,"A Taxonomy of Cyber-harms: Defining The Impacts of Cyber-attacks and Understanding How They Propagate" **Journal of Cybersecurity**, Vol. 4, No. 1, 2018, s. 9-10.
[43] Kovacich, Boni, **a.g.e.**, s. 55.
[44] Siber suçun tanımı yapma sürecini zorlaştıran altı faktör bulunmaktadır. Bunlar: siber suçlar kavramının tarihçesi, atipik doğası, siber uzayın genişliği, küresel doğası, siber suç üzerine kriminolojik araştırmaların azlığı ve suçun çok değişken doğasıdır. bkz: Brian K. Payne, "Defining Cybercrime", **The Palgrave Handbook of International Cybercrime and Cyberdeviance**, Ed., Thomas J. Holt, Adam M. Bossler, Palgrave Macmillan, Switzerland, 2020, s. 5-13.
[45] Mustafa Karabal, Bekir Peker, Ali Sarvan, "Bilişim Suçları ve Türk Polis Teşkilatı", **Çağın Polisi Dergisi**, S.6, 2001, s. 2.

1.2.1.Siber Suç Terim Sorunu

Siber suçu tanımlamak için kullanılan terimlerin çeşitliği araştırmalarının karşılaştığı ilk sorundur. Bu konuda gerek ulusal ve uluslararası mevzuatlarda gerekse hukuk literatüründe ortak terimlerin kullanıldığı görülmemektedir. O nedenle öğretide Siber suçu ifade edebilmek için dünya çapında birçok terim kullanılmaktadır. Bu terimler dijital "digital", sanal "vitrtual",yüksek teknoloji "high-tech",bilgisayar bağlantılı "computer-related", internetle ilgili "Internet related", bilişimle ilgili "telecommunications-related", bilgisayar destekli "computer-assisted", çevrimiçi "on-line" suçlar gibi terimlerdir[46].

Bilgisayarın ilk ortaya çıktığı ülke olan Amerika Birleşik Devletleri ve doktrininde bu tür suçlara ilişkin yeni bir tip suçlar olarak ilk adlandırma yapan ülke olmuştur. Bu anlamda bilgisayar ile ilgili suçlar "computer related crimes", bilgisayar aracılığıyla işlenen suçlar "computer assisted crimes", bilgisayara karşı suçlar "computer agaist crimes" gibi terimler kullanılmış olup günümüzde bilgisayar suçu "computer crime" Amerikan öğretisinde kullanılan en yaygın terimlerdir[47].

Aynı şekilde Amerikan doktrinde olduğu gibi İngilizce konuşulan Avustralya ve İngiltere doktrininde de konuyla ilgili görüş birliği bulunmamaktadır. Bazı yazarlar tarafından "computer crime" terimi tercih edilmekte olup diğer yazarlar ise "e-crime" ifadesini tercih etmektedir[48]. Zira Avrupa ülkelerinde de aynı sorun yaşanmakta olup "elektronik suçlar" "bilgisayar kullanımıyla işlenen suçlar" "bilişim suçluluğu" "verileri otomatik işleme tabi tutan sistemlere karşı işlenen suçlar" gibi birçok terim ortaya atılmaktadır[49].

---

[46] Russell G. Smith, Peter Grabosky, Gregor Urbas**, Cyber Criminal on Trial**, Cambridge, Cambridge University Press, 2004, s. 21; Fausto Pocar, "New Challenges for International Rules Against Cyber-Crime", **European Journal on Criminal Policy and Research**, Vol. 10, No.1, 2004, s. 33.

[47] Caner Yenidünya, Olgun Değirmenci, **Mukayeseli Hukukta ve Türk Hukukunda Bilişim Suçları,** İstanbul, Legal Yayıncılık, 2003, s. 30.

[48] Commander Barbara, "Etter The Challenge of the Forensic İnvestigation of Computer Crime", (Çevrimiçi), http://www.austlii.edu.au/au/journals/AUFPPlatypus/2001/19.pdf, Erişim Tarihi: 07.10.2019.

[49] Bkz: Akbulut, **a.g.e.** s. 55-59; Dülger, **a.g.e.**, s. 72-73.

Arap öğretisinde yine bu suçun terim sorunu hakkında uzlaşmaya varılmamıştır. Siber suç anlamında bilgi suçu, elektronik suçlar, bilgisayarla bağlantılı suçlar, bilgisayar suçları, yüksek teknoloji suçları, örümcek ağı suçları gibi kavramlar kullanılmaktadır[50]. Ancak bu suçlara ilişkin Arap Sözleşmesi tarafından "bilgi teknolojileri suçları" kavramı kullanılmıştır.

Türk doktrinine gelince farklı farklı terimler kullanılmakta olup bu konu oldukça karmaşık hale gelmektedir. İnternet suçu[51], sanal suç [52], bilgisayar veya bilgisayar ağları ilgili suç[53], bilgisayar suçu[54], bilgisayar veri veya sistemlerine karşı işlenen suçlar[55], bilgisayarla işlenen suçlar veya bilişim suçları[56], siber suç[57], bilişim alanında işlenen suç[58] gibi bir sürü terim kullanılmaktadır. Kronolojik olarak ortaya yeni atılmış terimlerin, kendilerinden önceki terimlerden daha açıklayıcı olduğu görülmektedir. Dolayısıyla kullanılan terimler konulara bakış açısını etkilemekte olup konuya olan yaklaşımı da belirlemektedir[59].

Ancak doktrinde bu terimler çoğu çeşitli yönlerden eleştirilmiştir. Bilgisayar suçu teriminde mesela bilgisayar araç olarak kullanıldığı için bilgisayar suçu denilmemelidir. Diğer anlatımla suçlar işlenmesinde kullanılan araca göre adlandırılmamalıdır. Zira yaralanma suçu bıçak ile işlenmesi halinde "bıçak suçu"

---

[50] Osama Ahmet Elmenaase, Jelal Muhamet Elzubi, **Ceraim Tekeniyet Nuzum el-Melumat el-Elektroniye**, Umman, Dar el Sekafe li Neşir ve Tevzii, 2010, s. 62-63.

[51] Veli Özer Özbek, "İnternet Kullanımında Ortaya Çıkabilecek Bazı Ceza Hukuku Sorunları", **DEÜHFD,** C.IV, S.1., 2002, s.106-107; Mehmet Niyazi Tınılır, **İnternet Suçları ve Bireysel Mahremiyet,** Ankara, Liberte Yayınları, 2002, s. 1; Feridum Yenisy, "İnternet Suçlarının Yeni İşleniş Biçimleri", **Uluslararası İnternet Hukuku Sempozyumu 21-22 Mayıs 2001, İzmir,** Dokuz Eylül Üniversitesi Yayını, 2002, s. 447.

[52] Yılmaz Yazıcıoğlu," Bilgisayar Ağlarıyla İlgili Suçlar Konusunda Türk Ceza Kanunu 2000 Tasarısı" **Uluslararası İnternet hukuku sempozyumu 21-22 mayıs 2001, İzmir,** Dokuz Eylül Üniversitesi Yayını, 2002, s.452.

[53] Hasan Dursun ," Bilgisayarla İlgili Suçlar", **Yargıtay Dergisi**, C.XXIV, S.3, 1998, s. 334.

[54] Bkz: Erol Çitin, İsmail Malkoç, **Uygulamada Sahtekarlık Suçları, Bilgisayar Suçları, Tebligat Suçları ve İlgili Mevzuat**, Ankara, Adalet Yayınevi, 1995, b.a; Yılmaz Yazıcıoğlu, **Bilgisayar Suçları Kriminolojik, Sosyolojik ve Hukuki Boyutları İle**, İstanbul, ALFA, 1997, b.a.

[55] Kayhan İçsel, "Avrupa Konseyi Siber Suç Sözleşmesi Bağlamında Avrupa Siber Suç Politikasının Ana İlkeler", **İÜHFM**, C.LIX, S.1-2, 2001. s. 3.

[56] Dülger**, a.g.e**., Yenidünya, Değirmenci**, a.g.e.**, s.31; Akbulut, **a.g.e.**, s. 58-59.

[57] Recep Benzer, "Siber Suçlar ve Teorik Yaklaşımlar", **Güncel Tehdit : Siber Suçlar**, Ed. Hüseyin Çakır , Mehmet Serkan Kılıç, İstanbul, Seçkin Yayınları, 2014, s. 21.

[58] TCK'da kullanılmış olup yazarların çoğu bu terimi kullanmaktadır.

[59] Yazıcıoğlu, **a.g.e.**, s. 130.

olarak adlandırılmamaktadır. Dolayısıyla bilgisayar suçunun kapsamlı bir ifade olduğu düşünülmemektedir[60].

Sadece ağları esas alan İnternet suçu terimi de eleştiriye maruz kalmaktadır. İnternet siber suçların işlenmesine zemin hazırlayan günümüzde en yaygın ağ olsa da Extrenet v.s. gibi birçok bilgisayar ağı bulunmaktadır. Nitekim bu ağlarla veya herhangi bir ağ kullanmadan da siber suç işlenebilmektedir[61]. Bu nedenle siber suçun işlediği ortama göre çeşitli şekillerde adlandırılmasının doğru bir yaklaşım olduğu kabul edilmemektedir. Kasten öldürme suçunda olduğu gibi suçun bina içinde işlenmesi halinde bina suçu denilmemektedir[62].

Bilgisayara karşı işlenen suçlar, bilgisayar ile işlenen suçlarında da uygun terimler olmadığı düşünülmektedir. Bu terimler siber suçların bir yanını ele almış olup yeni ortaya çıkan suçun tüm çeşitli boyutlarını kapsamamıştır. Dolaysıyla bu terim yetersiz ve eksik kalmaktadır[63].

Bilişim suçları terimi siber suçları ifade edebilmek bilgisayar suçu teriminden daha uygun görülmektedir. Günümüzde bir sürü cihazın bilgisayarın yerine suç işlemek için kullanılabildiğinden ve buna bilgisayar suçu denmesi uygun görülmemektedir[64]. Dolayısıyla bilişim suçları teriminin Türk doktrinde en çok kullanılan terim olduğunu söylemek mümkündür. Aynı zamanda 2000 yılından bu yana gerek düzenlemelerde gerekse uygulamalarda bu terim tercih edilmiştir[65].

Siber suç terimine gelince öncellikle belirtilmesi gereken "siber" kelimesinin İngilizcede olan "cyber" kelimesinden gelmiş olduğu ve sanal gerçeklik veya

[60] Dursun, **a.g.m.**, s .339.
[61] Akbulut, **a.g.e.**, s. 59.
[62] Yenidünya, Değirmenci, **a.g.e.**, s. 31.
[63] Dülger, **a.g.e.**, s.74.
[64] Mesih Gözüşirin, "5237 Sayılı Türk Ceza Kanununda Bilişim Suçları ve Bilişim Suçları İle Mücadeleye İlişkin Model Önerisi", **Kara Harp Okulu Savunma Bilimleri Enstitüsü**, **Yayımlanmamış Yüksek Lisans Tezi**, Ankara, 2011, s. 27.
[65] Dülger, **a.g.e.**, s. 75.

bilgisayar ağları anlamında kullanıldığıdır. Yunanca'da gemiyi yönlendiren pilot anlamına gelen "Sibernetik" kelimesinden türetilmiştir[66].

Söz konusu siber suçlar, günümüzde bilişim suçlarını ve internet suçlarını ifade etmek için kullanılmaktadır. Ancak siber suçların büyük kısmı internette işlendiğinden dolayı siber suçun ve internet suçun aynı anlama geldiği düşünülmektedir. Tüm internet suçları siber suç olarak sayılabilir ancak her siber suç internet suçu olarak sayılmaz. Siber suç kelimesinin ilerde ortaya çıkacak olan yeni suç türlerini kapsayacağı düşünülmektedir[67]. Ayrıca siber suç doktrinde ve edebiyatta en çok kabul gören terim olup ağa bağlı olan bilgisayarlara ve sistemlere vurgu yapmaktadır. Nitekim bu terim uluslararası alanda en çok tanınan ve kullanılan terimdir. Avrupa Konseyi [68] ve Birleşmiş Milletler tarafından da tercih edilmektedir[69] . Dolayısıyla bu çalışmada genel anlamıyla siber suç teriminin kullanılması tercih edilmiştir.

1.2.2. Siber Suçun Tanımı

Siber suçların hukuki sorun olarak ortaya çıkmasıyla beraber yapılan ilk tanımlarda bilgisayarla ilgili her türlü fiil veya hareketler siber suç olarak nitelendirmiştir. Ancak zamanla siber suçlara ilişkin yasaların ve yargı kararların sonucunda meydana gelen suçla korunan hukuki değer unsurundan hareket ederek tüm fiiller siber suç olarak kabul edilmemiştir. Zira siber suç tanım sorunu çözülmemiştir. Dolayısıyla öğretide yazarlar ve hukukçular tarafından çeşitli esaslara göre birçok tanım yapılmıştır[70].

Akbulut'a göre siber suç çeşitli yedi kritere göre tanımlanabilir. Bunlar :

---

[66] Yavuz Erdoğan, **Avrupa Konseyi Siber Suçlar Sözleşmesi'nde Yer Alan Koruma Tedbirleri ve Bu tedbirlerin Türk Hukukundaki Yeri**, İstanbul, Legal Yayıncılık, 2018, s. 49.
[67] Sacit Yılmaz, **Türk Ceza Hukuku Sisteminde Siber Suçlar**, Ankara, Adalet Yayınevi, 2016, s. 5.
[68] Avrupa Konseyi bu Suçlarla ilgili Sözleşmesini çeviren, "siber suç" terimini kullandığı görülmektedir. Emine Eylem Aksoy, "Siber Suçluluğa Dair Sözleşme", **Prof. Dr. Kemal Oğuzman'a Armağan**, 2002, s. 869-896.
[69] Murat Volkan Dülger, "Karşılaştırtmalı Hukuk Bağlamında Birleşik krallık İngiltere Hukukunda Bilişim Suçları Mevzuatı ve Uygulaması", **Türkiye Adalet Akademisi Dergisi**, S. 31, 2017, s. 147.
[70] Dülger, **a.g.e.**, s. 76.

-Siber suçun bilgisayarın ya da sistemlerin amaç veya aracı olmasına göre tanım.

-Siber suçları malvarlığı ihlalleriyle sınırlayan tanım.

-Bilgisayar sistemleriyle ilgili her türlü suçları kıstas edinen tanım.

-Bilgisayar sistemlerinin araçlarının kullanımına göre tanım.

-Suçun failini kıstas edinen tanım.

-Veri ağlarını kıstas edinen tanım.

-Tanım yapılmayan siber suçları sınıflandırılması[71].

Karagülmez'e göre siber suçları üç kategoriye ayırıp tanımlanmaktadır. Bunların ilki bilgisayarın fiziğine zarar veren eylemler (bilgisayara verilen somut hasar), ikincisi bilgisayar sistemlerine karşı işlenen fiiller, üçüncü ise internet ağlarında işlenen diğer ifadeyle internet ortamında işlenen eylemlerdir[72].

Dülger ise konuya başka bir bakış açısıyla yaklaşmaktadır. Ona göre siber suç sayılan suçlar üç kategoride toplanmaktadır. Bunların ilki bilişim sistemlerine veya içeriğine (güvenliğine, verilerine, yazılmalarına ve bütünlüğüne) karşı işlenen suçlardır. Örneğin bilişim sistemine girme, sistemi engelleme, bozma, verileri yok etme veya değiştirme suçlarıdır. İkincisi işlenmesinde bilişim sistemleri kullanımının nitelikli unsuru olan suçlar, sözgelimi, bilişim sistemlerini kullanmak suretiyle hırsızlık veya dolandırıcılık suçları. Üçüncüsü ise işlenmesinde bilişim sistemleri sadece araç olarak kullanıldığı suçlardır. Örneğin, haberleşmenin engellenmesi, hakaret ve haberleşmenin gizliliğini ihlal etme suçlarıdır[73].

Dolayısıyla siber suçlar için dar ve geniş olmak üzere iki çeşit tanım yapmıştır. Siber suçların dar olan tanımı, bilişim sistemlerine, verilerine, gizliliğine, bütünlüğüne

[71] Akbulut, **a.g.e.,** s. 59-69.
[72] Ali Karagülmez, **Bilişim Suçları ve Soruşturma-Kovuşturma Evreleri,** 5.bs, Ankara, Seçkin, 2014, s. 71.
[73] Dülger, **a.g.e.,** s.77.

ya da sistemlerin veya verilerin fonksiyonuna karşı işlenen suçlardır. Geniş tanımı ise bilişim sistemleri ya da verileri aracılığıyla, bilişim sistemlerine veya verilerine karşı işlenen her çeşit suçlardır[74].

Farklı bir değerlendirme yapan Wall'a göre gelişen bilişim teknolojisi sonucunda şekillerle suçların ortaya çıktığı görülmektedir. Yani siber suç kazanç elde edilebilmek için yasal olmayan yollardan bilgiye erişmek ve manipülasyona başvurmaktır[75]. Öte yandan Brenner, siber suçu klasik suçtan farklı olarak siber ortamda bilgisayar sistemleriyle gerçekleştirilen suçlar şeklinde tanımlamıştır[76].

siber suçu teknik bakış açısıyla tanımlayan yazarlara göre, siber suçlar bilgisayar ve teknolojisine hakim olan fail tarafından verilerin yetkisiz bir şekilde işlenmesini düşünmektedir[77].

Tüm bu farklı tanımların genel ortak noktası siber suçun bilişim sistemleri aracılığıyla veyahut bilişim sistemlerine karşı işlenmesidir, başka bir ifadeyle siber suçun işlenmesinde bilişim sistemleri bir unsur olarak görülmektedir. Siber suçu işleyen fail daima bilişim sistemleri veya içeriğini hedef almaktadır. Öte yandan bilgisayara fiziki zarar verilmesi halinde siber suçu değil başka suçları (mala zara verme veya hırsızlık suçu) teşkil etmektedir[78].

Belirtilmesi gerekir ki siber suça ilişkin yapılan tanımlar bu çalışmada verilen tanımlarla sanrılı değildir. Hukuk literatüründe farklı açılardan değerlendirilmiş olan birçok tanım bulunmaktadır. Siber suçlar klasik suçlardan farklı olarak özel mücadele gerektirmektedir. Bu suçlara yönelik farklı politika ve stratejilerin uygulanması zorunluluğu sebebiyle siber suçun hukuki olarak tanımı oldukça önem arz etmektedir. Ancak bazı yazarlar tarafından siber suçun soruşturması ve kavuşturması konusunda

---

[74] Dülger, **a.g.e.,** s.77- 78.
[75] David S. Wall, **Cybercrime: The Transformation of Crime in the Information Age**, Cambridge, Polity Press, 2007, s. 10.
[76] Brenner, **a.g.e.**, s. 9.
[77] Elliot Turrini, Sumit Ghosh, "A Pragmatic, Experiential Definition of Computer Crimes" **Cybercrimes: A Multidisciplinary Analysis**, Ed. Elliot Turrini, Sumit Ghosh, Berlin, Springer, 2010, s. 9.
[78] Dülger, **a.g.e.**, s.77.

örneğin kimlik bilgisi çalma suçu ister gerçek alemde ister sanal alemde olsun her iki halde suç sayılmasından dolayı siber suçun tanımı yapmak gerek olmadığı belirlenmektedir[79].

Siber suçun tanımının genel bir tanım olması gerekmektedir. Yani hızlı gelişen teknolojinin ortaya çıkarabileceği yeni eylemleri kapsayacak şekilde "sınırlı olamayan ve ucu açık" bir tanım yapmak doğru bir yaklaşım olacaktır[80]. Yukarda üzerinde durulan tanıların ortak noktası siber suçun bilgisayar, internet veya diğer bilişim teknolojileri aracığıyla yada bunlara karşı işlenmesidir. Diğer yandan klasik suçların internet ya da bilişim sistemleri üzerinde işlenmesi siber suç olarak değerlendirilmemelidir[81]. Ayrıca siber suçun tanımı yapmaktan daha çok bu kavram altında hangi suçların düzenleneceği konusu daha çok önem taşımaktadır. Dolayısıyla siber suç kavramının kapsadığı suçların belirtilmesi ve tanımlanması daha faydalı olacaktır[82]. Oysa siber suçların ne olduğu konusunda görüş birliği olduğunu söylemek mümkündür. Bu anlamda siber suçların üç grupta ele alınmıştır. Bunların ilki bilgisayar veya teknolojilerine karşı işlenen suçlar. İkincisi bilgisayar ve teknolojisi aracılığıyla işlenen suçlar. Üçüncüsü ise siber suçların işlenmesinde bilgisayar ve teknolojisinin önemli rol oynadığı suçlar[83].

1.2.3.Siber Suçu Tanımlamaya Çalışan Uluslararası Girişimler

Siber suçun tanımı ve buna uygulanacak cezaları belirleme hususu, siber suçlarla ilgili olan uluslararası örgütler ve anlaşmalarda en önemli sorunu teşkil etmiştir. Dolayısıyla uluslararası bazda siber suçlarla erken ilgilenilmeye başlanmıştır.

---

[79] Kristin Finklea, Catherine A. Theohary, "Cybercrime: Conceptual Issues for Congress and U.S. Law Enforcement", (Çevrimiçi), https://fas.org/sgp/crs/misc/R42547.pdf, Erişim Tarihi: 25.08.2019; k.g. bkz: Hasan Sınar, **İnternet ve Ceza Hukuku**, İstanbul, Beta Basım, 2001, s. 73-76.
[80] Dülger, **a.g.e.**, s. 77; Akbulut, **a.g.e.**, s. 58-59.
[81] Dülger, **a.g.e.**, s. 77; Akbulut, **a.g.e.**, s. 70.
[82] Nusret Onur Akpek, Siber Suçlar Sözleşmesinin Getirdikleri ve İç Hukuk Açısından Konuya Yaklaşım, **İstanbul Bilgi Üniversitesi, Sosyal Bilimler Enstitüsü, Yayınlanmamış Yüksek Lisans Tezi**, İstanbul, 2015, s. 6.
[83] Smith, Grabosky, Urbas, **a.g.e.**, s. 7.

Bu başlık altında siber suçların tanımında uluslararası örgütlerin çalışmaları ardından uluslararası anlaşmalarda siber suçların tanımı üzerinde durulacaktır.

1.2.3.1.Uluslararası Örgütlerin Siber Suç Tanımı

2000 yılında Viyana'da gerçekleştirilen Birleşmiş Milletler'de Suçların Önlenmesi ve Suçlulara Muamele 10. Kongresi'nde siber suça ilişkin dar ve geniş olmak üzere iki tanım yapılmıştır. Dar anlamında bilgisayar suçu, meşru olmayan elektronik işlemlerle yönlendirilen bilgisayarın sistemlerinin güvenliğini veyahut verilerini hedef alan eylemlerdir. Geniş anlamda tanımı ise bilgisayar ile ilgili suçlar, bilgisayarın ağları ya da sistemleriyle veya bunlarla ilişkin olarak işlenen yasadışı eylemlerdir. Bu kapsama yasadışı bilgileri elde etme gibi suçlar olmak üzere bu bilgileri bilgisayar ağları ya da sistemleriyle sunmak ve dağıtmak da girmektedir[84].

Teknolojinin doğurmuş olduğu olumsuz etkilerle ilgilenen Ekonomik Kalkınma ve İşbirliği Örgütü (OECD) siber suçu, "otomatik işleme tabi tutulan verilere karşı veya verileri nakil etme işlemlerinde yasaya, ahlaki değerlere aykırı veya yetkisiz bir şekilde gerçekleştirilen her türlü eylemler" olarak tanımlamıştır[85].

İnterpol'e göre siber suçun evrensel bir tanımı bulunmamaktadır, Ancak kolluk kuvvetleri internetle ilgili suçları ikiye ayırmaktadır. Bunların ilki olan ileri siber suçları (Yüksek teknoloji suçları) bilgisayarlara ve yazılımlarına karşı gelişmiş araçlar kullanılarak işlenmektedir. Diğeri ise siber uzayda işlenen suçlardır. Bilişim teknolojilerinin getirmiş olduğu yeni araçlar klasik suçların işlenmesinde kullanılmaya

[84] Shinder, **a.g.e.**, s. 17; Telwant Singh Addl.Distt, Sessiens Judge .Delhi, "Cyber Law and Information Technology", s. 2, https://www.slideshare.net/talwant/cyber-law-information-technology, Erişim Tarihi: 18.10.2019.

[85] Haluk Çolak, "Siber Terörizmin Önlenmesinde Kurumsal Yapılanma ve Uluslararası Adli Yardımlaşma", **Türk Hukuk Araştırmaları Dergisi**, C.I, S.1, 2016, s. 4; Mehmet Emin Arslan, "Siber Güvenlik ve Siber Saldırı Türleri", (Çevrimiçi), https://cutt.ly/WeEY9LE, Erişim Tarihi: 03.11.2019. s. 2.

başlanmıştır. Örneğin çocuklara karşı, malvarlığına karşı işlenen suçlar veya terör suçlarıdır[86].

Europol'a göre ise yüksek teknoloji suçu bilginin ve telekomünikasyon teknolojisinin bir insana, mülkiyete, organizasyonlara veya bilgisayar ağ sistemlerine karşı suç işlemek ya da suçu sürdürmek için kullanılmasından oluşmaktadır. Siber suç ve alt kategorileri internetteki herhangi bir ağın ya da sistemin suç oluşturan kullanımı olup sistem ve ağlara karşı saldırıları, yeni teknolojiyi kullanarak var olan suçların kötüye kullanılmasını veya internetin gelişmesi ile birlikte yeni suçların ortaya çıkmasını kapsamaktadır[87].

1.2.3.2. Uluslararası ve Bölgesel Düzenlemelerde Siber Suç Tanımı

Uluslararası ve bölgesel mevzuatların çoğunda siber suç tanımına rastlanmazken birkaç tanesinde bu tanımı görmek mümkündür. Örneğin Stanford Üniversitesi[88] tarafından 2000 yılında sunulan Siber Suç ve Terörizmden Korumanın Geliştirilmesine Yönelik Uluslararası Sözleşmesi (Draft International Convention To Enhance Protection from Cyber Crime and Terrorism) taslağında siber suç tanımı yapılmıştır. İşbu sözleşmenin tanımlar ve terimlere tahsis edilen 1.maddesine göre bilgisayar suçu, bilgisayardaki kontrol ve iletişim sistemleri ile ilgili, bu sözleşmede cezalandırılan bir suç olarak düzenlenen her türlü fildir[89].

Avrupa Konseyi Siber Suç Sözleşmesi, Bilgi Teknolojisi Suçlarıyla ilgili Arap Sözleşmesi ve Kişisel Verilerin Korunması ve Siber Güvenliğe ilişkin Afrika Birliği Sözleşmesi gibi siber suçları ele alan uluslararası metinlerde, bu suçlara ilişkin her

---

[86] Leo S. F. Lin, John Nomikos, "Cybercrime in East and Southeast Asia: The Case of Taiwan", **Asia-Pacific Security Challenges Managing Black Swans and Persistent Threats**, Ed. Anthony J. Masys, Leo S. F. Lin, Switzerland, Springer, 2018, s. 68.

[87] Pocar, **a.g.m.**, s. 32.

[88] Stanford Üniversitesi uluslararası bazda suçlarla mücadelede önemli bir rol oynayan kurumlardan birisidir. Bu sözleşme taslağı 1999 yılında hazırlamıştır.

[89] Bkz: Draft International Convention To Enhance Protection from Cyber Crime and Terrorism, (Çevrimiçi), https://media.hoover.org/sites/default/files/documents/0817999825_249.pdf, Erişim Tarihi: 08.10.2019.

hangi bir tanım görülmemektedir. Keza Bilgisayar Bilgileri Suçlarla Mücadeleye Yönelik İngiliz Milletler Topluluğu Sözleşmesi siber suç kullanmak yerine "bilgisayar bilgileri suçu" ve "bilgisayar bilgilerini hedef alan kriminolog fiil" ifadelerini kullanmıştır.

Görüldüğü gibi siber suçlar için uluslararası ve ulusal bazda ne terim konusunda ne de tanım konusunda bir uzlaşmaya varılamamıştır. Bu da devletler arasında işbirliğini zorlaştırıp siber suçlara yönelik mücadelede bir zorluk yaratmaktadır. Uluslararası ve ulusal mevzuatlarında siber suç tanımı yapmak yerine siber suçu teşkil eden fiillerin dikkatli bir şekilde tek tek "kazuisitk"[90] olarak belirlenmesi ve tanımlanması en tercih edilen yaklaşımdır. Doktrinde Avrupa Konseyi Siber Suç Sözleşmesi'nin bu yaklaşımı tercih ediş nedeni, taraf devletlerin arasında ortaya çıkacak terim ve tanım farklığının üstünden gelinebilmesidir, aynı zamanda sözleşmeye mümkün olduğunca daha çok katılım sağlamayı amaçlamasıdır. Zira sözleşmede başlıca birtakım suçların belirlenmesi, taraf devletlerin başka suçlar eklemesine engel olmamaktadır[91]. Dolayısıyla "Siber suç" kelimesini hukuki bir terim olarak kabul etmemekte yarar vardır. Yeri gelmişken belirtilmesi gerekir ki bu yaklaşım 2004 Birleşmiş Milletler Yolsuzlukla Mücadeleye İlişkin Sözleşmesi tarafından benimsemiştir. BM bu sözleşmede yolsuzluğun tanımını yapmamıştır. Ancak yolsuzluğu oluşturan hareketleri belirleme yükümlülüğünü devletlere bırakmıştır[92].

1.3. Siber Suçun Özellikleri

Bilgisayarın ve teknolojilerin ortaya çıkmasıyla birlikte suç kavramında değişiklikler olmuştur. Siber suçun klasik suçlardan ayıran ve kendine has olmasını sağlayan özellik sanal ortamda işlenmesidir. Başka bir ifadeyle klasik suçlarda maddi unsuru teşkil eden hareketlerin gerçekleştirilmesiyle işlenmektedir. Siber suçlarda ise

[90] Levent Kurt, **Açıklamalı -İctihatlı Tüm Yönleriyle Bilişim Suçları ve Türk Ceza Kanunundaki Uygulama,** Ankara, Seçkin Yayıncılık , 2005, s. 60.
[91] Erdoğan, **a.g.e**., s. 52.
[92] Malby, v.d., **a.g.e.**, s. 12.

genelde bir klavyeye basmakla veya bir dokunuşla işlenmektedir. Üstelik siber suçların sosyal ve ekonomik etkileri klasik suçlara göre daha fazla, hatta kimi durumlarda bu etkilerin tahmin edilmesi bile mümkün olmamaktadır[93]. Siber suçların klasik suçlardan ayıran ve kendine özgü en önemli özellikleri sınır aşan olması, kolaylıkla işlenmesi ve beyaz yakalıdır.

1.3.1. Sınır Aşan Suç

Siber suçların en önemli özeliği devletlerin arasındaki fiziksel sınırları ortadan kaldırmasıdır. Diğer bir ifadeyle siber suçlar dünyanın herhangi bir yerinden klasik coğrafik sınırlara bakılmaksızın herhangi bir riske maruz kalmadan işlenebilmektedir. Eskiden suçların çoğu yerel ve bölgesel sınırlar içerisinde gerçekleştirilirken, sınır aşan suçların büyük bir kısmı ancak suç örgütleri tarafından organize suç olarak işlenmekteydi[94]. Fakat son yıllarda bilgisayar ve bilişim teknolojisinin gelişmesi suçları devletlerin fiziksel sınırların ötesine taşımıştır. Söz konusu bu suçlar ağlara bağlı sistemler üzerinden veya bu sistemler aracılığıyla gerçekleştirilmektedir[95]. Günümüzde genellikle en yaygın ağ sistemi uluslararası niteliğine sahip olan internet üzerinden işlenmektedir.[96]

Wall tarafından "new wine, no bottles" ,"şişesi olmayan şarap" ya da "yeni şarap şişe yok"[97] şeklinde ifade edilen sınır tanımayan siber suçların denetlenmesi oldukça güçtür. Bunu Yazıcıoğlu üç nedenle açıklamaktadır. Bunların ilki siber suçların dijital bir ortamda işlenmesi dolayısıyla suçların incelenmesinin özel teknik uzmanlıklar gerektirmesidir. İkinci neden evrensel bilgisayar ağlarının kullanıcılara ülke sınırları dışına erişim imkanı tanımasıdır. Üçüncü neden ise siber suçluların

---

[93] Dülger, **a.g.e.**, s. 103.
[94] Karagülmez, **a.g.e.**, s. 78.
[95] Ankur Jain, "Cyber Crime: Nature, Elements and Types", **National Journal of Cyber Security Law**, Vol.2, No.2, 2019, s. 2.
[96] Dülger, **a.g.e.**, 189.
[97] David S. Wall, "Policing Cybercrimes: Situating The Public Police in Networks of Security Within Cyberspace", s. 5. (Çevrimiçi), https://cyberdialogue.ca/wp-content/uploads/2011/03/David-Wall-Policing-CyberCrimes.pdf, Erişim Tarihi: 17.10.2019.

kendilerine göre suç işlemek en müsait için ortamı seçme olanağına sahip olmalarıdır[98].

Öte yandan siber suç görünmez bir suçtur. Bundan maksat geleneksel suçlar duygularla hissedilebilir. Örneğin, saldırı suçu gerçekleştiği zaman mağdur bunu hissedebilir veya hırsızlık suçu gerçekleştiğinde bu durum duyulabilir. Ancak siber suç işlendiğinde genellikle görülmez, duyulmaz ve hissedilmez. Yani mağdur, siber suçu ancak işlendikten sonra bilir[99].

1.3.2. Kolaylıkla İşlenebilen Suç

Siber suçun diğer bir önemli özelliği oldukça kolay işlenebilir olmasıdır. Yeni teknolojilerin yaratığı dijital ortamlar suç işlemek için çok müsaittir. Bunun nedeni bu tür suçlar şiddet içeren hareketleri gerektirmemekte olup bir tuşa veya klavyeye basarak birkaç milisaniyeler içinde işlenebilmektedir[100]. Diğer yandan siber suçların işlenmesinde kullanılan araçların teknik bakımdan çok gelişmiş olması ve internete genellikle anonim bir şekilde girilmesi dolayısıyla bu suçlar işlendikten sonra arkada herhangi bir iz de bulunmamaktadır. O nedenle "sofistike"[101] olan bu suçların soruşturulması klasik suçlara göre daha güçtür[102].

Nitekim yetkili makamlar tarafından kaydedilmeyen siber suçların sayısı kaydedilen suçlardan daha fazladır. Bu suçların mağdurları özellikle bu konuda bilgisi olmayanlar kimseler olduğu için toplumdan dışlanacaklarını veya aşağılanacaklarını düşünmektedirler ve bu sebeple de suçu ihbar etmekten çekinmektedirler. Suçun mağduru şirketler olması durumunda ise kimseye duyurulmadan gizli bir şekilde

[98] Yılmaz Yazıcıoğlu, "Konuşma AB Uyum Komisyonu Çalışması Türk Mevzuatında Bilişim Suçları", s.3. (Çevrimiçi), http://docplayer.biz.tr/8186275-Konusma-ab-uyum-komisyonu-calismasi-turk-mevzuatinda-bilisim-suclari.html, Erişim Tarihi: 17.10.2019.
[99] Payne, **a.g.m.**, s. 8.
[100] Kurt, **a.g.e.**, s. 57.
[101] Dülger, **a.g.e.**, s. 189.
[102] Gercke, **a.g.e.**, s. 142.

çözülmeye gayret gösterilmektedir. Bu nedenle siber suçun faillerine en çok yardım eden bu suçun mağdurlarıdır[103].

1.3.3.Beyaz Yakalı Suç

Siber suçlar, beyaz yakalı suçlar olarak nitelendirilmişlerdir. Söz konusu bu suçlar çoğu kültürlü, eğitimli, sosyal hayatında başarılı, toplumda değer, saygı ve en önemlisi bilgisayar bilgisine sahip olan kişiler tarafından çıkar elde edebilmek için işlenmektedir. Buna ek olarak, bu nitelikli "birinci nesil"[104] suçluların işledikleri suçlardan meydana gelen zararlar, geleneksel suçlarla mukayese edilemeyecek kadar büyüktür[105].

ABD'de ve Almanya'da yapılan araştırmalara göre bu suçların faillerinin genelde yaşları 24-33 arasında olup düzenli, sağlıklı, yüksek seviyede bilgisayar ve teknoloji bilgisine sahip ve çoğu erkeklerden oluşmaktadır. Bu kişiler işyerinde işverenler tarafından kıymetlerini ve değerlerini yeteri kadar anlaşılmamış olduğu görüşündedirler. Ayrıca yeterli destek ve ilgi görmedikleri ve onlara karşı haksızlık yapıldığını düşündükleri için verileri değiştirmekte veya hileler aracılığıyla siber suç işlemektedirler. Bunun amacı onlara göre menfaat dengesini tekrar düzenlenmektir. Onlar bu suçları kamu kuramlarına veya şirketlere karşı işledikleri için bu durumda kimsenin mağdur olmadığına inanmakta ve dolayısıyla da kimseye zarar vermediklerini düşünmektedirler. Yani suçluluk hissini duymamaktadırlar[106].

---

[103] Kurt, **a.g.e.**, s. 58.
[104] Birinci nesil suçlular şu şekilde tanımlanmaktadır: Bilgisayarların ilk ortaya çıktığı zamandan itibaren yaygınlaşmasına kadar devam eden sürede bilişim bilgileriyle yasaya aykırı davranışlar işleyen faillerdir. Bkz: Yazıcıoğlu**, a.g.e.**, s. 105.
[105] Dülger**, a.g.e.**, s. 129.
[106] Kurt, **a.g.e.**, s.59-60.

1.4.Siber Suçun Sınıflandırması ve Türleri

Siber suçları sınıflandırma konusunda yine tanım ve terimde olduğu gibi standart bir sınıflandırma bulunmamaktadır[107]. Bunun temel nedeni bilgisayar ve teknolojilerin hızlı gelişmesinin sonucunda siber suçların yeni şekillerinin ortaya çıkmasının devam etmesidir. Ayrıca siber suçların sınıflandırması yapılırken suçun işlenme şekli, hukuki düzenlemeler, uluslararası metinler gibi kriterler dikkate alınmaktadır[108]. Dolayısıyla bu konuya ilişkin hem öğretide[109] ele alınan kaynaklarda hem de uluslararası metinlerde ve hatta örgütlerin yaptığı çalışmalarda çeşitli sınıflandırmalar görülmektedir. Bu başlıkta siber suçların Birleşmiş Miletler, Avrupa Konseyi Siber Suç Sözleşmesi, Ekonomik Kalkınma ve İşbirliği Örgütü (OECD), McConnel International, ve son olarak Bilgi Teknolojisi Suçlarına İlişkin Arap Sözleşmesi tarafından sınıflandırılmasına değinilecektir.

1.4.1.Birleşmiş Milletler Sınıflandırması

İtalya'da Birleşmiş Milletler tarafından düzenlenen "Symposium on The Occasion of The United Nations Convention Against Transnational Organized Crime" sempozyumunda 14 Aralık 2000 tarihinde yapılan "The Challenge of Borderless CyberCrime" başlıklı panelde üye devletlerin siber suçlara ilişkin birçok eylemi cezalandırması önerilmiştir. Bunlar:

-Bilişim sistemlere izinsiz giriş.

-Bilgisayar veya bilişim sistemlerinin yasal olmayan bir şekilde kullanımının engellenmesi.

---

[107] Sarah Gordon, Richard Ford, "On the Definition and Classification of Cybercrime", **Journal in Computer Virology**, Vol. 1, No. 2, 2006, s. 14-15.
[108] Akarslan, **a.g.e.**, s. 41.
[109]Bkz: Serdar Havuz, "Avrupa Konseyi Siber Suçlar Sözleşmesi kapsamında Türkiye Güvenliği", **Harap Akademileri Komutanlığı Stratejik Araştırmalar Enstitülüsü, Yayımlanmamış Yüksek lisans Tezi,** İstanbul 2007, s. 37-41; Yazıcıoğlu, **a.g.e.**, s. 143-150.

-Bilişim sistemlerin içerdiği verilerin yok edilmesi veya değiştirilmesi.

-Program veya veri gibi soyut birçok değerin ele geçirilmesi.

-Bilişim sistemleri aracılığıyla sahtekârlık eylemleridir[110].

Ancak BM bünyesinde 2013 yılında Uyuşturucu ve Suç Ofisi tarafından hazırlanan çalışma'da (Comprehensive Study on Cybercrime) siber suçlar: bilgisayar verilerinin veya sistemlerinin gizliliğine, bütünlüğüne ve kullanılabilirliğine aykırı eylemler, kişisel kazanç ya da finansal veya zarar vermek için bilgisayarla ilgili eylemler ve bilgisayar içeriğiyle ilgili eylemler olmak üzere üç kapsamlı kategoriye ayrılmıştır. Birinci kategoride bilgisayar sistemlerine veya bilgisayar verilerine yasa dışı bir şekilde erişme, verileri elde etme, bilgisayar verilerine yasa dışı müdahale, bilgisayar, bilişim sistemlerini kötüye kullanmak için araçlar üretme, dağıtma veya ilgili araçlara sahip olma ve verilerin korumasına ilişkin hukuk kurallarına aykırı eylemler yer almaktadır. İkinci kategori bilgisayar sistemleriyle ilişkili dolandırıcılık, hırsızlık, kimlik hırsızlığı, telif hakları veya ticari marka suçları, spam gönderme veya gönderimini kontrol etme ve çocuk istismarı suçlarını içermektedir. Son kategoride ise bilgisayar sistemi üzerinden nefret söylemi, çocuk pornografisi üretimi, dağıtımı veya bulundurulması, terör suçlarını destekleme suçları sayılmaktadır[111].

1.4.2. Avrupa Konseyi Siber Suç Sözleşmesindeki Sınıflandırma

Avrupa Konseyi Siber Suç Sözleşmesi'nde siber suçlar; bilgisayar veri sistemlerinin erişilebilirliğine, gizliliğine ve bütünlüğüne karşı işlenen suçlar, bilgisayarla ilişkili suçlar, içerikle ilgili suçlar ve telif hakları ve bununla ilişkili hakların ihlâline ilişkin suçlar olmak üzere dört ana kategori altında sınıflandırılmıştır. Bunların ilk kategorisi olan bilgisayar veri sistemlerinin erişilebilirliğine, gizliliğine ve bütünlüğüne karşı işlenen suçlar; yasadışı erişim, yasadışı araya girme, verilere

[110]Olgun Değirmenci, "Bilişim Suçları", **Marmara Üniversitesi Sosyal Bilimler Enstitüsü**, **Yayımlanmamış Yüksek Lisans Tezi**, 2002, s. 120.
[111] Malby, v.d., **a.g.e.**, s. 116.

müdahale, sistemlere müdahale ve sistemlerin kötüye kullanımını kapsamaktadır. İkinci kategori olan bilgisayarla ilişkili suçlar; bilgisayar bağlantılı dolandırıcılık ve bilgisayar bağlantılı sahtekârlıklardır. Üçüncü grup olan içerikle ilgili suçlar; çocuk pornografisine ilişkin suçlar, bilgisayar sistemleri aracılığıyla ırkçılık ve yabancı düşmanlığı (Ek protokolde) suçlarını içermektedir. Son grup ise telif haklarının ve bunula ilgili hakların ihlallerine ilişkin suçlardır[112].

1.4.3. Ekonomik Kalkınma ve İşbirliği Örgütü'nün (OECD) Sınıflandırılması

1986 yılında Kalkınma ve İşbirliği Örgütü tarafından hazırlanan "Computer Related CrimeCriminal Threats from Cyberspace: Analysis of Legal Policy" başlıklı raporda kanunda düzenlenmesi gereken bir takım fiiller siber suç olarak sayılmıştır. Söz konusu fiiller şunlardır: Bilgisayar aracılığıyla dolandırıcılık, bilgisayar aracılığıyla sahtekârlık, bilgisayar verilerinde veya sistemlerinde değişiklik yapılması, bilgisayar programlarının hak ihlaline uğratılarak dağıtılması, değiştirilmesi ve kopyalanması, bilgisayar ve sistemlerine yetkisiz giriş veya bu sistemlerin yetkisiz kullanılmasıdır[113].

1.4.4. McConnel International Sınıflandırması

Amerikan global politika ve teknoloji yönetimi danışmanlık şirketi olan McConnel International tarafından yapılan sınıflandırma öğretide en çok kabul gören

[112] Cahit Aliusta, Recep Benzer, "Avrupa Siber Suçlar Sözleşmesi ve Türkiye'nin Dahil Olma Süreci", **Uluslararası Bilgi Güvenliği Mühendisliği Dergisi**, C.IV, No.2, 2018, s. 38; Murat Volkan Dülger, "Avrupa Konseyi ve Avrupa Birliği Düzenlemelerinde Çocuk Pornografisinin İnternet Aracılığıyla Yayılmasına Karşı Yapılan Düzenlemeler", **İstanbul Barosu Dergisi**, S. 4, 2004, s. 1487.
[113] Umut Eker, "Türk Ceza Hukukunda Bilişim Suçları- Eski TCK Bağlamında Hukukumuzda Yer Alan İlk Düzencemeler ve 5237 Sayılı Yeni Türk Ceza Kanunu'nun İlgili Hükümlerinin Yorumu", **TBBD**, S. 62, 2006, s. 109.

sınıflandırmadır[114]. Bu sınıflandırmaya göre siber suçlar; verilere karşı suçlar, ağ suçları, yetkisiz giriş suçları ve bilgisayarla ilişkili suçlar olmak üzere dört ana kategori altında ele alınmıştır. İlki olan veri suçları; veriler müdahalesi, değiştirilmesi ve veri hırsızlığıdır. İkinci kategori ağ suçları; ağın engellenmesi ve sabotajı suçlarını içermektedir. Üçüncü kategori yetkisiz giriş suçları; yetkisiz erişim ve virüs yayılmasıdır. Son kategori bilgisayarla ilişkili suçlar ise; bilgisayar aracılığıyla sahtekârlık ve dolandırıldık suçlarını içermektedir[115].

1.4.5. Bilgi Teknolojisi Suçlarına İlişkin 2010 Arap Sözleşmesi Tasnifi

Arap Ligi tarafından 2010 yılında imzalanan Bilgi Teknolojisi Suçlarına İlişkin Arap Sözleşmesi'nin 5.-18. maddelerinde üye devletlerin siber suç olarak düzenlemesi gereken eylemler belirlenmiştir. Söz konusu suç eylemleri: yetkisiz erişim, verilere yetkisiz müdahale, verilere zarar verme, bilgi teknolojilerinin kötüye kullanılması, bilişim sistemleri aracılığıyla sahtecilik ve dolandırıcılık, pornografi suçu ve ayrıca çocuk pornografisi suçları daha ağır cezaya tabi tutulmuş, özel hayata ilişkin siber suçlar, bilgi teknolojileri aracılığıyla terör suçları, bilgi teknolojileri aracılığıyla örtülü suçlar, telif hakları ve bunla ilgili hakların ihlal edilmesi ve elektronik ödeme yöntemlerin yasa dışı kullanılmasıdır[116].

1.5.Siber Suça Benzeyen Diğer Kavramlar

Teknolojinin ve bilişim sistemlerinin yarattığı siber ortam sayesinde devletlerin arasındaki coğrafi sınırlar ortadan kaldırılmıştır. Bunun sonucunda

---

[114] Uğur Özüdoğru, "Siber Suçlar ve Mücadele Yöntemleri : Dünya Uygulamaları ve Türkiye İçin Çözüm Önerileri" **Bilgi Teknolojileri ve İletişim Kurumu, Yayımlanmamış Bilişim Uzmanlığı Tezi,** 2011, s. 21.

[115]McConnell International, "Cyber Crime . . . and Punishment?", (Çeveimiçi), http://www.iwar.org.uk/law/resources/cybercrime/mcconnell/CyberCrime.pdf,Erişim, Erişim Tarihi 15.10.2019.

[116] Ahmet Hemi, Zühera Keisi, "Suar Creaim Tekneiyet el Melumat Wifke li İtifakiye el Arabiye li Senet 2014", **Mecelet el Ulum el Siyasiye ve el Knuniye**, C.X, S.1, 2019, s. 781-788; İmam Hesenin Ata Alla, **Ceraim Tekeniyet el Malumat fi el Teştiaat ve el Sukuk el Arabiye**, Riyad, Dar Camiat Naif li Neşir, 2017, s. 137.

bilişimle ilgili bilgiye sahip olan herkes tarafından dünyanın herhangi bir yerinde bilgisayar sistemlerine ulaşılıp suç veya saldırı geçekleştirilebilmektedir. O nedenle devletler önemli ve kritik kurumlarda kullandıkları lokal bilişim sistemlerini dış ağlardan ayırmaya çalışmaktadırlar[117]. Fakat bunun her zaman mümkün olmaması siber tehditler için kritik bir ortam yaratılmasına neden olmaktadır[118].

Devletler güvenliklerine karşı geçekleştirilebilecek tehditleri klasik anlamda dış ve iç saldırı olmak üzere ikiye ayrılmaktadır. İç tehditler suç ve terör, savaş ise dış tehdit olarak nitelendirilmiştir[119]. Genellikle suçlar iç hukuka, savaş suçlar uluslararası silahlı çatışmalar hukukuna tabidir[120]. Ancak bu sınıflandırma siber alanda yapılan tehditler için geçerli değildir. Bunun nedeni siber saldırıların herhangi bir coğrafi sınırı tanımamasıdır. Bu başlık altında siber alanda diğer siber tehditler olan siber terörizm, siber savaş ve siber saldırı üzerinde durulacaktır.

1.5.1.Siber Terörizm

11 Eylül 2001 olaylarından sonra terörizmin etkileri ve boyutları açısından yeni bir dönem başlamıştır. Bundan önce terör faaliyetlerinde geleneksel patlayıcı maddeler kullanılmakta olup ölen kişilerin, tahrip edilen kurumların veya binaların sayısı yüzler civarında olmuştur. Ancak anılan tarihten sonra terör nedeniyle gerçekleştirilmiş eylemlerden dolayı meydana gelen zararlarının niceliği ve niteliği oldukça büyüktür. Neticede kıyamet terörizmi veya süper terörizm kavramı ortaya çıkmıştır. Bu kavram içerisinde terör eylemlerinin eşzamanlı saldırı olanağı, saldırılarda kullanılan yüksek teknoloji yöntemleri, askeri ve ekonomik kurumların hedef alınması (Pentagon ve Dünya Ticaret Merkezi), sivil uçakların kaçırılıp kitle imha silahlarına dönüştürülmesi

---

[117] Halihazırda Rusya kendini muhtemel siber saldırılardan korumak için has yerel ağ yaratmaya çalışmaktadır.https://edition.cnn.com/2019/05/01/europe/vladimir-putinindependent-russian--internet-intl/index.html, Erişim Tarihi: 25.10.2019.

[118] Haydar Çakmak, Cenker Korhan Demir, "Siber Dünyadaki Tehditler ve Kavramlar", "**Suç, Terör ve Savaş Üçgeninde Siber Dünya**", Ed. Haydar Çakmak, Taner Altunok, Ankara, Barı Platin Kitabevi, Platin Yayınevi, 2009, s. 29.

[119] **A.m.**, s. 24.

[120] Alexandra Perloff-Giles, "Transnational Cyber Offenses: Overcoming Jurisdictional Challenges", **The Yale Journal of International Law**, Vol. 43, No. 1, 2018, s. 200.

ve biyolojik, kimyasal, nükleer vb. silahlarla saldırı gerçekleştirilmesinden bahsedilmeye başlanmıştır[121].

Son yıllarda siber terörizm bilimsel bir olgu haline gelmiştir. Teknolojinin sağladığı imkânlardan büyük ölçüde yararlanan teröristler, bilgisayar sistemleri ve ağlarını kullanarak kamu ve özel sektörlerine karşı eylemler gerçekleştirmeye kolaylıkla devam etmektedirler[122]. Temel amacı bazı siyasi hedefleri gerçekleştirmek olan kişiler, ellerine geçen bilişim sistemleri veya ağları aracılığıyla terör eylemlerinde bulunmaktadırlar. Bu nedenle siber terörizmin felsefesi ve ideolojisinde bir değişiklikten bahsedilemez. Ancak siber terörün metotlarında ve kullandığı araçlarda oldukça önemli bir değişiklik söz konusu olmuştur[123]. Yani klasik terör yeni teknoloji araçlarını kullanarak yeni bir şekilde[124] başka bir ifadeyle "yeni yüzü"[125] ile karşımıza çıkmaktadır.

Siber terörizmin tanımı konusuna gelince siber terör, terörizm ve teknolojinin birleşmesi sonucunda ortaya çıkan bir kavramdır. Tüm milletler için tehlike kaynağı oluşturan siber terörizmin dünyada herkes tarafından kabul edilen bir tanımı bulunmamaktadır [126]. Ayrıca klasik terörün bile hala dünya çapında kabul gören bir

---

[121] Murat Saraçlı, "Uluslararası Hukukta Terörizm", **Gazi Üniversitesi Hukuk Fakültesi Dergisi,** C. XI, S.1-2, 2007, s. 1055-1056.

[122]Scott J. Shackelford, "Toward Cyberpeace: Managing Cyberattacks through Polycentric Governance", **American University Law Review**, Vol. 62, No. 5, 2013, s. 1301.

[123] Kyung-shick Choi, Claire Seungeun Lee, Robert Cadigan, "Spreading Propaganda in Cyberspace: Comparing Cyber-Resource Usage of Al Qaeda and ISIS", **International Journal of Cybersecurity Intelligence and Cybercrime**, Vol. 1, No. 1, 2018, s. 22.

[124]Mehmet Özcan "Siber Terörizm ve Ulusal Güvenliğe Tehdit Boyutu", (Çevrimiçi), https://docplayer.biz.tr/29878985-Siber-terorizm-ve-ulusal-guvenlige-tehdit-olusturma-boyutu.html, Erişim Tarihi: 24.10.2019, s. 7.

[125] Bkz: Bekir Peker,"Bilişim Suçları ve Bilişim Güvenliğinin Ulusal ve Uluslararası Boyutu" **Selçuk Üniversitesi Sosyal Bilimler Enstitüsü, Yayımlanmamış Yüksek Lisans Tezi**, Konya, 2010, s. 41.

[126] Bkz: Ünal Acar, Ömer Urhal, **Devlet Güvenliği İstihbarat ve Terörizm,** Ankara, Adalet Yayınevi, 2007, s.217; İbrahim Kaya, **Terörle Mücadele ve Uluslararası Hukuk,** Ankara, USAK Yayını, 2005, s. 9.

tanımı yapılmamıştır[127]. Dolaysıyla siber terörizm tanımının olmaması normal bir durum olarak görülmektedir[128].

Terör kelimesi yıldırma, tehdit, panik veya korkutma anlamında kullanılmaktadır. Siber terörizm, genellikle bilişim sistemleri ve ağları aracılığıyla devletlerin kritik altyapılarına ve tesislerine (Devlet işlemleri, ulaşım, enerji v.s.) zarar vermek, bunların işlerini aksatmak veya kullanımını engellemek amacıyla gerçekleştirilen saldırılardır[129]. Siber terörizm ırkçı, sosyal, dini veya siyasi hedeflere ulaşmak için bir devletin vatandaşlarını korkutmak, yıldırmak veya onlara zarar vermek, şiddet kullanmak gibi eylemlerle gerçekleştirilmektir. Başka bir anlatımla, herhangi bölgede yaşayan belirli bir topluma baskı uygulayarak, korkutmak veya yıldırmak yöntemiyle siyasal amaçlarına ulaşmaya çalışmaktır. Yani terörist, belli amaçlara (genellikle siyasi amaçlar) ulaşmak için kullanılan bir araçtır[130].

Siber terörle ilgili öğretide ve bazı uluslararası örgütlerin yaptığı çalışmalarda birçok tanım bulunmaktadır[131]. Siber terörizm, devletin ulusal güvenliğine veya kamu menfaatlerine karşı eylemlerde bulunmak amacıyla kişisel veya siyasal olarak teşvik edilmiş insanların bilişim sistemleri aracılığıyla gerçekleştirdiği her türlü eylemler bütünüdür. Kısa bir tanım yapmak gerekirse klasik anlamda terörizmin bilişim sistemleri ve ağları aracılığıyla gerçekleştirilmesidir[132], ya da bilgisayar yoluyla

---

[127] Her devlet kendi iç ve dış politikasına veya siyasi hedeflerine göre farklı terörizm tanımı yapmaktadır. Dolayısıyla bir gurup veya bir kişi bir devlet tarafından terör olarak değerlendirilebilirken başka bir devlet tarafından özgürlük savaşçı olarak değerlendirilebilmektedir. bkz; Ercan Çitlioğlu, **Gri Tehdit Terörizm,** Ankara, Destek Yayınları, 2008, s. 17.

[128] Muharrem Gürkaynak, Adem Ali İrem, "Reel Dünyada Sanal Açmaz: Siber Alanda Uluslararası İlişkiler", **Süleyman Demirel Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi,** C.XVI, S.2, 2011, s. 266.

[129] Gabriel Weimann, "Cyberterrorism: The Sum of All Fears?", **Studies in Conflict & Terrorism**, Vol. 28, No. 2, s. 130.

[130] Oğuz Kara, Üzeyir Aydın, Ahmet Oğuz, "Ağ Ekonomisin Karanlık Yüzü: Siber Terör", (Çevrimiçi), http://kisi.deu.edu.tr/oguz.kara/Ag%20Ekonomisinin%20karanlik%20yuzu%20siber%20teror.pdf, s.2. Erişim Tarihi: 25.10.2019.

[131] Çolak, **a.g.m.**, s. 6

[132] Mesut Hakkı Çaşın, **Uluslararası Terörizm**, Ankara, Nobel Yayın Dağıtım, 2008, s. 449.

milletin korkmasına veya devletin siyasi ve ekonomik çıkarlarının büyük zarara uğratılmasına neden olacak tüm eylemlerdir[133].

Teröristlerin faaliyetlerinde interneti ve bilişim sistemlerini kullanmayı tercih etmelerinin birkaç nedeni bulunmaktadır. Bunlardan en önemlisi bilişim sistemleri üzerinden yapılan eylemlerin maliyetinin, fiziksel eylemlere göre daha düşük olmasıdır. Kısaca herhangi bir bilgisayar olağanüstü zararlara neden olabilmektedir[134]. Bunu yanı sıra, siber eylemde bulunan kişinin arkada iz bırakmaması nedeniyle takip edilmesi oldukça zordur. Aynı zamanda fail klasik eylemlerde olduğu gibi herhangi bir havalimanı kontrolünden ya da arama noktasından geçmediği için anonim kalmaktadır[135]. Son olarak, siber terörün birden fazla hedefi olabilmektedir. Örneğin, hem kamu hem de özel sektörün çeşitli kuruluşlarının internet sitelerini veya çağrı merkezlerini hizmet dışı edebilmektedir[136]. Özetle anonimlik, hızlılık, yerden bağımsızlık, maliyet düşüklüğü ve evrensellik faktörleri siber terör eylemlerini kolaylaştırmaktadır[137].

Siber terörü geleneksel terör eylemlerinden farklı kılan birçok yönü bulunmaktadır. İlk akla gelen farklılık klasik terörün, siber teröre göre daha tehlikeli olmasıdır. Teröristler geleneksel anlamda eylemleri gerçekleştirirken gerekli bazı durumlarda hayatlarını ortaya koymak zorunda olup, ayrıca polis tarafından yakalanma ihtimali de bulunmaktadır. Siber terörizmde ise terörist oturduğu yerde sigarasını veya kahvesini içerken dünyanın herhangi bir yerinde, çok güvenli bir ortamda, herhangi bir riske maruz kalmadan terör eylemlerini yapabilmektedir[138].

---

[133]Dorothy D. Denning, "Is The Cyber Terror Next?", Çimrimiçi, http://essays.ssrc.org/sept11/essays/denning.htm, Erişim Tarihi, 25.10.2019.
[134] Irving Lachow ,Courtney Richardson "Terrosit Use of the Internet: The Real Story", **Joint Force Quarterly National Defense University**, Vol.45, No.2,, 2007, s. 101-103.
[135] Çakmak, Demir, **a.g.e.**, s. 38.
[136] Gürkaynak, İrem, **a.g.m.**, s. 276.
[137] Phillip W. Brunst, "Terrorism and the Internet: New Threats Posed by Cyberterrorism and Terrorist Use of the Internet", **A War on Terror? The European Stance on a New Threat, Changing Laws and Human Rights Implications,** Ed. Marianne Wade, Almir Maljevic, Berlin, Springer, 2010, s. 52-54.
[138] Çaşın, **a.g.e**., s. 451.

İkinci farklılık, terörün temel amacından kaynaklanmaktadır. Klasik terörün esas amacı topluma veya hükümete bir konu hakkında siyasi, sosyal, dini bir mesaj iletken aracı insanlara zarar vermek veya şiddet uygulamaktır. Örneğin, IRA örgütünün yaptığı gibi, bu örgüt, ortaya çıkacak zararı minimum seviyede tutmak için yapacağı eylemleri kısa bir süre önce bildirmektedir. Siber terörizmde ise sanal alanda yapılan siber eylemler araç olarak değil, amaç olarak görülebilmektedir. Örneğin, terörist bilişim sistemleri sayesinde devlet kurumlarının, bankaların, şirketlerin bilgi iletişim sistemlerine saldırı yapıp oldukça büyük zararlara neden olabilmektedir[139].

Üçüncü olarak siber terör uluslararası niteliğe sahiptir. Klasik terör eylemleri geniş kitleye ulaşabilmesine rağmen yerlidir. Yani devletin bir tesisinin, binasının hedef alınması halinde sadece o binadaki insanlar hayatını kaybeder. Fakat siber terörün etki alanı bilgisayar ve bilişim sistemleridir. Bu sistemleri yönlendiren fareyle siber terörün etki alanı akıl almaz oranda genişletilebilir ve fare tıklamasıyla bir ülkenin birçok binası veya birçok ülkede bulunan binalar aynı anda yıkılabilir[140].

Dördüncü farklılık ise normal terörün bedensel güç gerektirmesi nedeniyle bu eylemleri ancak belli bir yaş üstündeki insanların yapabilmesidir. Siber terörizm tam tersine çocuk veya büyük fark etmeksizin herkes tarafından gerçekleştirilebilir. Ayrıca siber terör, silah veya bombalara ihtiyaç duymaz ve siber faaliyetleri gerçekleştirmek için sadece bilgisayarın kullanımı yeterli olmaktadır[141].

Son olarak normal terör eylemlerinde kişi kiralamak bu eylemleri gerçekleştirenler için büyük bir risk faktörü oluşturduğu için az tercih edilen bir yöntemdir. Diğer yandan siber terör eylemlerinde kullanılan kişilerin sürekli değişiklik gösterebilmesi ve bu kişilerin bilgisayar aracılığıyla izlenebilmesinin zorluğu nedeniyle buradaki risk faktörü yok denecek kadar azdır. Dolayısıyla siber eylemler

[139] Çaşın, **a.g.e**., s. 451- 452.
[140] Çaşın, **a.g.e**., s. 454.
[141] Çaşın, **a.g.e**., s. 454.

yapan kişi fiilen terör örgütü üyelerinden biri olmadığından, güvelik makamlarının siber eylemler hakkında bilgi alması oldukça güçtür[142].

1.5.2. Siber Savaş

İnsanlar geçmişte birbirine benzemeyen ve her birinin kendisine has özellikleri olan iki ortamda savaşmışlardır. Bunlar kara ve deniz ortamdır. Yıllar önce geliştirilen hava teknolojisi sonucunda üçüncü savaş alanı olan gökyüzü ortamı ortaya çıkmıştır. Daha sonra savaşın dördüncü alanı olan uzay kendini göstermiştir. Son yıllarda inanılmaz bir hızla gelişmeye devam eden teknolojinin yarattığı siber alan, askeri literatürde beşinci savaş ortamı olarak kabul edilmektedir[143].

Günümüzde devletlerin en önemli bilgileri siber alanda depolanıp işlenmektedir. Ayrıca ulusal savunma sistemlerinin bilişim sistemleri vasıtasıyla korunması, savaş halinde muhtemel bir siber saldırı tehdidine maruz kalmak anlamına gelmektedir. Bu nedenle devletler konvansiyonel savaşın taktikleri ve stratejileri yanı sıra yeni savaş ortamına uyum sağlamak amacıyla, ordularının siber alanda yeteneklerini ve taktiklerini geliştirmeye çalışmaktadırlar[144].

Siber savaşın, siber suç ve siber terörizm gibi dünyada herkes tarafından kabul edildiği bir tanım bulunmamaktadır[145]. Zaten uluslararası hukukta geleneksel savaş ve silahlı çatışma ayrımı konusunda objektif normlar bulunmadığı için devletler kendi menfaatleriyle orantılı olarak tamınlar yapmıştır[146]. Dolayısıyla siber savaşın birkaç tanımı mevcuttur. Siber savaş, bir ülkenin ulusal bir amaca ulaşmak veya devam eden gerçek savaşa destek vermek maksadıyla bilişim sistemlerini kullanarak, diğer

---

[142] Çaşın, **a.g.e.**, s. 454-455.
[143] Mehmet Yayla, "Hukuki Bir Terim Olarak Siber Savaş", **TBBD**, Y.25 S.104, 2013, s. 183; Hasan Çifci, **Her Yönüyle Siber Savaş**, Ankara, TÜBİTAK Popüler Bilim Kitapları, 2013, s. 7.
[144] Yayla, **a.g.m.**, s. 183.
[145] Erdi Şafak, "Uluslararası Hukukta Değişen Güvenlik Algısı ve Saldırı Suçu Bağlamında Siber Saldırılar", **Selçuk Üniversitesi Hukuk Fakültesi Dergisi**, C.XXVIII, S. 1, 2020, s. 131; Shackelford , **a.g.m.**, s. 1297.
[146] Hatice Kübra Ecemiş Yılmaz, "Birleşmiş Milletler Antlaşması, Kuzey Atlantik Antlaşması ve Uluslararası Hukuk Açısından Siber Saldırının Tanımlanması Sorunu", **Journal of Social And Humanities Sciences Research,** Vol.6, No.38, 2019, s. 1647.

devletin sivil ve askeri herhangi bir kuruluşunun bilgi ve iletişim sistemlerini yok etmek, engellemek, devre dişi bırakmak veya kendi menfaatleri için herhangi bir şekilde kullanmak[147] olarak tanımlanabilmektedir[148]. Söz konusu eylemler Çin'de bilgi savaş (informationalized warfare) olarak bilinirken ABD'de askeri perspektif açıdan "bilgi operasyonları" kapsamında yer almaktadır[149].

Siber savaşın en yaygın tanımı ABD eski başkanı olan Bush'un siber güvenlik müşaviri olarak görev yapmış olan Clarke tarafından yapılmıştır. Ona göre siber savaş, bir ülke tarafından başka ülkenin bilişim sistemlerine ve ağlarına zarar vermek veya onların işlerini aksatmak maksadıyla yapılan tüm eylemleridir[150]. Diğer tanıma göre "Siber savaş, politikanın uzantısı olarak bir ulusun güvenliğine ciddi bir tehdit oluşturan ya da bir ulusun güvenliğine yönelik algılanan bir tehdide yanıt olarak yürütülen devlet veya devlet dışı aktörler tarafından siber uzayda gerçekleştirilen eylemlerdir[151].

Siber savaştan bahsedilirken bilgi savaşına değinmek gerekmektedir. siber savaş (cyber war) bilgi savaşı (information warfare) BM terimler sözlüğünde aynı anlamda kullanılmaktadır[152]. Ancak günümüzde söz konusu iki terim eş anlam olarak kullanımı kabul edilmemektedir[153]. Bilgi savaşı, siber savaş kavramı içeren daha geniş bir alandır. Yani siber savaş, bilgi savaşının alt bölümünü oluşturmaktadır[154]. Bilgi savaşı, şu şekilde tanımlanabilir: Düşmana karşı büyük avantaj, zafer, hedef elde etmek için bilgi kaynaklarını yok etmek, kullanmak veya tahrip etmektir. Bu anlamda bilgi savaşı kavramı gözetleme sistemleri, insan istihbaratı, casus uyduların

---

147 Gökhan Bayraktar, **Siber Savaş ve Ulusal Güvenlik Stratejisi**, İstanbul, Yeniyüzyıl Yayınları, 2015, s. 48.

148 Siber savaşın başka tanımları için bkz: Jana Shakarian, Paulo Shakarian, Andrew Ruef, **Introduction to Cyber-Warfare: A Multidisciplinary Approach,** USA, Elsevier, 2013, s.2; Solange Ghernaouti, **Cyber Power Crime, Conflict and security in Cyberspace**, Switzerland, EPFT press, 2013, s.165.

149 Shackelford, **a.g.m.**, s. 1297.

150 Çifci, **a.g.e.**, s. 5.

151 Paulo Shakarian, Jana Shakarian, Andrew Ruef, **Introduction to Cyber Warfare: A Multidisciplinary Approach,** Waltham, , Syngress, 2013, s. 2.

152 Yayla, **a.g.m.**, s. 185.

153 **A.m**. s. 186

154 Mustafa Sağsan," Bilgi Savaş: Siperlerden Klavyelere Taşınan Hareketin Anatomisi", **Avrasya Dosyası,** C.VIII, S. 2, 2002, s. 224-22; Yayla, **a.g.m.**, s. 186.

kullanılması, psikolojik operasyonların kullanılması ve dezenformasyon gibi eylemleri kapsamaktadır[155]. Daha açık bir tanıma göre bilgi savaş, düşmanın kuvvetlerini azaltmak, tahrip etmek amacıyla bilişim sistemlerin ya da verilerin aracılığıyla yapılan tüm eylemlerdir[156].

Teknolojinin gelişmiş olduğu devletler, siber alanın ulusal güveliğe tehdit kaynağı oluşturabileceğinin farkında olup bilişim sistemlerini korumak üzere siber alanla ilgilenecek kurumlar teşkil etmeye ve tedbirler almaya başlamıştır. Bu devletlerin en önemli aktörlerinin başında gelen ABD'de ilk önce siber savaşın kontrol edilmesi stratejik komutanlığa dönüştürülen uzay komutanlığına bırakılmıştır. Ancak daha sonra siber alanın oldukça önem taşıdığı kanaatine varan ABD ayrı bir siber komutanlık oluşturmuştur[157]. Söz konusu bu komutanlığın görevi, siber alanda devletin savunma sistemlerinin ve ağlarının güvenliğini korumak için eylemler yapmak, emir verilmesi halinde siber saldırılarda bulunmak, düşman siber saldırılarına karşı eylemler düzenlemek ve koordinatörlük yapmaktır[158].

Diğer yandan Çin, Kuzey Kore ve Rusya'da siber savunma sistemlerini geliştirme konusunda büyük yatırım yapan devletlerdir. Çin'nin Milli Özgürlük Ordusu siber alanın kara, deniz ve hava alanları kadar önem taşıdığını ve bu alanda ayrı bir ordu kurumak gerektiğini belirtmiştir. Ayrıca dünyanın en güçlü iki ülkesi olan ABD ve Rusya'yla siber ortamda mücadelede ve siber alandaki savaş için çalışmalar yapmak gerekmektedir. Rusya da oldukça önemli bir siber altyapıya sahip bir ülke olup birçok yazılım ve virüsler gelişmektedir. Kuzey Kore de olası siber savaş için siber önlemler almaktadır. Kuzey Kore'de en önemli "Unit 121" olarak adlandırılan kurum siber alandaki gerçekleştirilebilecek olan muhtemel saldırılara karşı savunma stratejileri geliştirmeye çalışmaktadır[159].

---

[155] Çakmak, Demir, **a.g.e.,** s. 45; Sait Yılmaz, **21. Yüzyılda Güvenlik ve İstihbarat**, İstanbul, Alfa Yayınları, 2006, s. 615.
[156] Yayla, **a.g.m.**, s. 186
[157] Richard A. Clarke, Robert K. Knake, **Siber Savaş, Ulusal Güvenliğine Yönelik Yeni Tehdit**, Çev. Murat Erduran, İstanbul, İstanbul Kültür Üniversitesi Yayınevi, 2010, s. 21.
[158] Yayla, **a.g.m.**, s. 187.
[159] Bkz: Major Arıe J. Schaap, "Cyber Warfare Operations: Development and Use under International Law", **Air Force Law Review,** Vol.64, 2009, s. 127-132-133.

İlk siber savaş Çin ve Tayvan arasında olmuştur. İki devlet arasında uyuşmazlık nedeniyle Çin, Tayvan'ın bilişim sistemlerine ve ekonomisine zarar vermek amacıyla siber saldırılar gerçekleştirmiştir[160]. Siber savaşa 2008 yılında Rusya ve Gürcistan arasında ortaya çıkan savaş başka önemli bir örnek olarak verilebilir. Söz konusu bu klasik savaş başlamadan önce iki devlet arası siber savaşı başlamış ve Rusya, Gürcistan'ın internet sitelere siber saldırılar yapmıştır. Bunun sonucunda kimi siteler engellenmiş ve kimi sitelerin içeriği değiştirilmiştir. Gürcistan devletini zayıf hale getirmek, saldırıların temel amacını teşkil etmiştir[161].

Son olarak, klasik savaşı desteklemek için yapılan siber eylemlerden bir de Irak'ta gerçekleştirilmiştir. 2003 yılında ABD'nin Savunma Bakanlığı olan Pentagon, Irak'ı işgal etmek için yaptığı planların yanı sıra, Irak subaylarının savaşa katılmadan teslim olmalarına teşvik eden bir mesaj hazırlamıştır. Bu mesajın Irak subaylarına ulaşmasını sağlayabilmek için, Irak Savunma Bakanlığına ait gizli ağlar uluslararası hukuka ve Irak egemenliğine aykırı bir şekilde kullanılarak iletilmiştir[162].

Bu açıklamalardan hareketle siber suç, siber terörizm ve siber savaş kavramlarının tamları üzerinde herhangi bir uzlaşma söz konusu olmamaktadır. Ancak bu kavramlar arasında hukuki niteliği açıdan çeşitli farklılıklar bulunduğunu belirtmek gerekir. Fail bakımından siber suç herkes tarafından işlenmekte, siber terör bir kişi örgütlü bir grup (devlet dışı aktör) tarafından işlenmekteyken siber savaş ancak bir devlet veya devlete bağlı bir aktör tarafından işlenmektedir[163]. Eylemin etkisi bakımından siber suç birey kişilere karşı, siber terör devletin altı yapılarına, topluma veya bireylere büyük zarar vermek gibi şekillerde gerçekleştirilebilirken siber savaş

---

[160] Yılmaz, **a.g.e.**, s. 95.
[161] Ocak, v.d., **a.g.e.**, s. 297
[162] Mesaj şu şekilde "Bu ABD Genelkurmayından size gönderilen bir mesajdır. Bildiğiniz üzere, yakın bir gelecekte Irak'ı işgal edeceğiz. Birkaç yıl önce yaptığımız gibi, sizi tamamen imha edecek bir güçle bunu gerçekleştireceğiz. Size veya askerlerinize zarar vermek istemiyoruz. Amacımız Saddam'ı ve iki oğlunu devirmek. Zarar görmek istemiyorsanız, tanklarınızı ve zırhlı araçlarınızı sıraya dizerek terk edin. Yürüyün, gidin, kendinizi kurtarın. Siz ve askerleriniz evlerinize dönün. Bağdat'ta gerekli rejim değişikliği yapıldıktan sonra siz ve başka Irak birlikleri yeniden göreve çağırılacaktır", Clarke, Knake, **a.g.e.**, s. 12.
[163] Murat Dogrul, Adil Aslan, Eyyup Celik, "Developing an International Cooperation on Cyber Defense and Deterrence against Cyber Terrorism", 2011 3rd International Conference on Cyber Conflict, **IEEE**, 2011, s. 31.

sadece devletlere karşı (devletler arasında) yapılmaktadır. Amaç bakımından siber suçlarda genellikle failler kazanç veya başka kişisel menfaat elde etmeyi amaçlamaktadır. Siber terörizm genellikle belli etnik, siyasi, sosyal veya ideoloji hedeflere ulaşmak için toplumları veya hükümetleri korkutmak veya zorlamak, siber savaş ise devlet siyasi amaçlar için siber eylemlerde bulunmakta veya klasik savaşla bağlantılı diğer düşman devlete karşı olarak kendini savunmaktır[164]. Hukuki statüsü bakımından siber suçlar, bunu düzenleyen ulusal hukuka, siber terör ulusal hukuka veya uluslararası hukuka tabi olabilmektedir. Siber savaş ise ancak uluslararası hukuka örneğin, Birleşmiş Milletler Anlaşması'na tabidir[165]. Bütün söz konusu bütün bu eylemlerin tek ortak noktası bilişim sistemlerinin aracılığıyla gerçekleştirilmesidir.

1.5.3. Siber Saldırı

Siber saldırı yine diğer kavramlar gibi doktrinde, ulusal ve uluslararası metinlerde tanımlanmış değildir. O nedenle öğretide birçok tanım bulunmaktadır. En önemli tanımlardan birini ABD Bilgisayar Bilimleri ve İletişim Kurulu Ulusal Araştırma Merkez'nin (Computer Science and Telecommunications Board of the National Research Council) bilişim uzmanı olan Lin şu şekilde yapmaktadır: siber saldırı muhtelif tarafından bilişim sistemlerini ve ağlarını ya da bu sistemlerdeki verileri, yazılımları kasten tahrip etmek, silmek, değiştirmek veya çalmak gibi tüm eylemleri kapsamaktadır[166]. Siber saldırı genel anlamıyla sistemde gizli olan verileri çalmak, değiştirmek, ortadan kaldırmak, kötü amaçlar için kullanmak veya ifşa etmek maksadıyla hedef alınan kişi, şirket veya devletin bilişim ağlarına veya sistemlerine karşı düzenlenen genellikle koordineli eylemlerdir[167]. Ancak siber saldırıların amacı sadece bilişim sistemleri veya sistemlerin içerdiği bilgilerle sınırlı olmamakla birlikte kontrol-komuta işlevselliğinin veyahut alt yapısının imha edilmesi veya tahrip

[164] **A.m.**
[165] Perloff-Giles, **a.g.e.**, s. 200.
[166] Herbert S. Lin, "Offensive Cyber Operations and the Use of Force", **Journal of National Security Law & Policy,** Vol.4, No.63, 2010, s. 63.
[167] Çakmak, Demir, **a.g.e.**, s. 29-30

edilmesi maksadıyla da gerçekleştirilebilmektedir[168]. Siber saldırılar, siber savaş kavramları kapsamında edilip edilemeyeceği konusu tartışmalıdır[169]. Siber saldırı kavramı tanılanırken siber suç, siber savaş ve siber terör kavramlardan ayrı tutulması gerekmektedir. Siber saldırının devletler arasında gerçekleştirilmesi söz konusu olduğunda savaş hukuku kavramları arasında yer alması gerekmektedir[170]. Aslında bu noktada dikkat edilmesi gereken husus söz konusu siber eylemin kimin tarafından ve hangi tarafa karşı işlendiğidir. Bu kriterlere göre siber suç, siber savaş veya siber terör olarak değerlendirilebilmektedir.

Klasik saldırı, klasik silahlarla gerçekleştirildiği gibi siber saldırı da siber silahlarla yapılmaktadır. Ancak siber alanda silah kavramı doğal olarak farklılık göstermektedir. Başka ifadeyle geleneksel saldırıda bomba, füze, top veya mermi gibi fiziksel silahlar kullanılırken siber saldırıda kullanılan çeşitli yazılımlar, bilgisayar veya bilişim sistemleri siber silahları teşkil etmektedir[171]. Ek olarak siber saldırının hedefi bilişim sistemindeki bulunan verileridir. Gerçekleştirilen siber saldırının sonucunda maddi zararlara meydana gelebilmektedir. Ancak siber saldırı temelde bilişim sistemine veya verilerine karşı işlemektedir[172].

Siber alanda gerçekleştirilen saldırılar; sözdizimsel saldırılar (syntactic attacks), anlamsal saldırılar (semantic attacks) ve karışık saldırılar (Blended Attacks) olmak üzere üç ana kategoriye ayrılabilir. İlk olarak sözdizimsel saldırılar, yazılım düzeyinde olup bilişim sistemlerinin işletimine veya işlevlerine yönelik gerçekleştirilmektedir. Son yıllarda yapılan siber saldırılardan olan Solucanlar,

[168] Şinasi Özgür Mumcu, "Siber Saldırıları ve Uluslararası Hukuk Hakkında Genel Bir Değerlendirme", **Galatasaray Üniversitesi Hukuk Fakültesi Dergisi**, S.1,2012, s. 212.
[169] Mehmet Yayla, "Siber Savaş ve Siber Ortamdaki Kötü Niyetli Hareketlerden Farkı", **Hacettepe Hukuk Fakültesi Dergisi**, C.IV, S.2, 2014, s. 192.
[170] Ecemiş Yılmaz, **a.g.m.**, s. 1642-1643.
[171] Yayla, "Siber Savaş ve Siber Ortamdaki Kötü Niyetli Hareketlerden Farkı", s. 187.
[172] Erdi, **a.g.m.**, s. 134.

(Worms), virüsler (viruses), Truva atı (Tro an Horses) ve DoS Saldrıları (Denial of Servic)[173], kötü amaçlı yazılımlar v.s. sözdizimsel saldırılardır[174].

İlk olarak, sözdizimsel saldırılarda virüs veya solucan şeklinde olan siber saldırılar inanılmaz bir hızla yayılıp oldukça büyük zararlara neden olabilmektedir. Örneğin bilgisayarda bulunan verileri ve şifreleri çalan Love Bug diye adlandırılan virüs 2002 yılında Hong Kong'da ortaya çıkmış[175] olup iki saat içinde dünya çapında yayınlayarak yirmiden fazla ülkede kırk beş milyon kullanıcıyı etkilemiş ve 2 ila 10 milyar dolar değerinde hasara neden olmuştur[176].

DoS saldırılara en önemli örneği 2000 yılında on beş yaşında olan bir çocuk tarafından Yahoo, Amazon ve CNN'ın web sitelerine gerçekleştirilen siber saldırılardır. Saldırı sonucunda bu siteler saatlerce kaplı tutulmuş olup 1.2 milyar dolarlık hasara sebep olmuştur. Diğer önemli örnek, 2007 Estonya devleti tarafından verilen "Kahraman Rus Askeri" adlı heykeli kaldırma kararı nedeniyle Rusya DoS saldırılarında bulunmuştur. Saldırlar sonucunda Kağıtsız olan Estonya devletinin bürokrasi ve ekonomisi son derece zarara görmüş ve devlet yapısı alt üstü hale gelmiştir. Buna karşı Estonya devleti ancak sistemlere kapatma önlemini almıştır[177].

Ayrıca, 2010 yılında İran'ın nükleer çalışmalarına zarar vermek maksadıyla tasarlanan "stuxnet" diye isimlendirilen bir yazılım şeklinde saldırı neticesinde İran'ın nükleer çalışmalarında beş yıl geri gittiği belirtilmiştir. Söz konusu siber saldırının ABD tarafından gerçekleştirildiği iddia edilmiştir[178].

---

[173] DOS saldırı hakkında detaylı bilgiler için bkz: Resul Das, Muhammet Zekeriya Gündüz, "Analysis of Cyber-attacks in IoT-based Critical Infrastructures", **International Journal of Information Security Science,** Vol.8, No.4, 2019, s. 123-125.

[174] Susan W. Brenner, Marc D. Goodman, "In Defense of Cyberterrorism: An Argument for Anticipating Cyber- Attacks", **University of Illionis Journal of Law, Technology and Policy**, No.1, 2002, s. 27-42.

[175] Goodman , Brenner, **a.g.m.**,s. 139-140.

[176] Brenner, Goodman, **a.g.m.**, s. 40-42; bkz: Ovidiu Mosıu, Ion Balaceanu, Eduard Mihai, "Cyber Terroism and the Eeffects of the Russian Attacks on Democratic States in Eas Europe", **Scientific Journal of Silesian University of Technology. Series Transport**, Vol. 106, No.11, 2020, s. 133.

[177] Yılmaz, **a.g.e.**, s. 95.

[178] Dülger, **a.g.e.**, s. 182.

İkinci olarak anlamsal saldırıların amacı sözdizimsel saldırılardan farklı olarak bilişim sistemlerine zarar vermek değil, bilişim sistemlerindeki verilerin doğruluğunu hedef almasıdır. Başka deyişle anlamsal saldırılar, bilişim sistemlerine zarar vermeden içindeki verilere müdahale edilerek değiştirilmesidir. Bu saldırılar özellikle resmi internet sitelerini veya kritik kuruluşların sistemlerini hedef almaktadır. Örneğin 2001 yılında Kaliforniya'da ikamet eden Rusya vatandaşı olan Dmitry Sklyarov, dijital telif haklarını ihlal etmekle suçlanıp yakalanmıştır. Daha sonra Yahoo! News tarafından Sklyarov'ın kavuşturulma işlemlerinin ertelenmesiyle ilgili bir haber yayınlanıştır. Ancak bir hacker tarafından Yahoo web sitesine anlamsal saldırı gerçekleştirilmiş olup haber değiştirilmiştir. Haber, yanlış bir şekilde Sklyarov'ın ölüm cezasına çaptırıldığını bildirmiştir[179].

Üçüncü olarak karışık saldırılar, anlamsal ve sözdizimsel saldırıların beraber yapılamayla gerçekleşmektedir. Yani bilişim sistemlerine veya içerisinde bulunan bilgilere zarar verilmesinin yanı sıra verilerin doğruluğuna müdahale edilip değiştirilmesidir. Örneğin işletim veya bilişim sistemlerine yanlış bilgiler verilerek zarar verilmesidir[180].

[179] Brenner, Goodman, **a.g.m.**, s. 32-33.
[180] Brenner, Goodman, **a.g.m.**, s. 40-41.

İKİNCİ BÖLÜM

ULUSLARARASI VE BÖLGESEL ORGANİZASYONLARIN SİBER SUÇLARLA MÜCADELEDEKİ ROLÜ

Devletler, bölgesel ve uluslararası organizasyonlar hızla değişen teknolojilerin yaratığı sorunlara ayak uydurmakta zorluk çekmektedirler. Yeni teknolojiler, suçluların tek bir yargı alanında etkin bir soruşturma ve kovuşturma yürütülmesi için gerekli bilgi ve kanıtların bulunmasını ve toplanmasını daha da zorlaştırmaktadır. Kolluk kuvvetlerinin bu tür suçlarla mücadele probleminin üstesinden gelebilmesi için yüksek derecede eğitimli ve kendilerini geliştirmiş olması gerekmektedir[181]. Bundan dolayı siber suçların önüne geçmek gerekliliğinin farkındalığına erken varan devletler ve ilgili örgütler, siber suçlarla mücadelede uluslararası ve bölgesel yönetmelikler geliştirerek maddi hukuk ve eğitim gibi alanlarda girişimlerini bir araya getirmektedir[182].

Bu bölümde siber suçlarla mücadele uluslararası girişimleri akabinde bölgesel girişimlerin üzerinde durulacaktır.

2.1.Uluslararası Organizasyonlar

2.1.1. Birleşmiş Milletler Örgütü

Uluslararası bağımsız bir organizasyon olan Birleşmiş Milletler Örgütü'ne üye devletlerin sayısı 193'e ulaşmıştır. Bu örgütün uluslararası ilişkiler alanında bir amacı vardır. Ancak siber suçlara ilişkin en önemli amacı bütün "devlet çalışmalarının koordinasyon merkezi" olmaktır. Nitekim BM'ye tüm üye devletleri uluslararası

[181] Lucie Angers, "Combating Cyber-Crime: National Legislation as a Pre-Requisite to International Cooperation", **Crime and Technology New Frontiers for Regulation, Law Enforcement and Research,** Ed. Ernesto U. Savona, Dordrecht, Springer Science, 2004, s. 41.
[182] Dülger, **a.g.e.**, s.189.

anlaşmayla bağlama yetkisine sahip olup ve hukukun yaklaşımına neredeyse küresel bir erişim sağlayabilmektedir[183]. Her ne kadar BM uluslararası meseleler için ideal bir platform olarak görünse de BM'nin siber suçlara ilişkin sorunu ele alıp almayacağı tartışmalara neden olan bir konudur. Siber tehdit meselelerine bir "Egemen mantık" ile yaklaşan Rusya ve Çin (ayrıca bazı Arap ülkeleri) gibi devletler BM aracılığıyla siber suçlarla ilgili küresel bir sözleşme görmek isterken AB, İngiltere ve ABD, BM'i (ve BM ajansı olarak ITU) internet ve siber güvenliğe öncülük edecek uygun bir örgüt olarak görmemektedirler. Bunun nedeni, hızla gelişen teknolojilerin karşısında BM'nin karar alma sürecinin yavaş olması ve hantal doğasıdır[184].

BM Uyuşturucu ve Suç Ofisi (UNODC), Uluslararası Telekomünikasyon Birliği (ITU), UNESCO ve BM Genel Kurulu siber suçlarla mücadelede devletlere katkıda bulunmaktadır. Bu örgütlerin amacı siber güvenlik ve siber suç konularında farkındalık yaratmak, üyelerini teşvik etmeye yönelik önerilerde bulunmak ve ulusal siber güvenlik yeteneklerini geliştirmek için uyum sağlamaktır[185].

Siber suç konusu 1985 yılında BM çalışmalarında yer almaya başlamıştır. İtalya'da yapılan Suçların Önlenmesi ve Suçluların Tretmanı Kongresi'nde siber suçların tipleri belirlenerek uluslararası toplumun siber suçlarla ilgili artan tehlikeye dikkat çekilmiştir[186].

BM'nin siber suçlarla mücadele girişimleri BM Genel Kurulu kararları ve BM Ekonomik ve Sosyal Konseyi çalışmaları olmak üzere aşağıda iki başlık altında ele alınacaktır.

---

[183] Stefan Fafinski, **Computer Misuse Response, Regulation and The Law**, Devon, Willan Publishing, 2009, s. 228.
[184] George Christou, **Cybersecurity in the European Union Resilience and Adaptability in Governance Policy,** London, Palgrave Macmillan, 2016, s. 46.
[185] **A.e.**
[186] Hasan Sınar, "Avrupa Konseyi Siber Suç Sözleşmesi Üzerine Bir Deneme", **Prof. Dr. Çetin Özek Armağanı**, İstanbul, Şan Ofset, 2004, s. 767.

2.1.1.1. Birleşmiş Milletler Genel Kurulu

BM Genel Kurulu tarafından siber suçlara ve teknolojinin kötü kullanımına ilişkin birçok karar alınmıştır. 1990 yılı 45/121 sayılı kararında devletler o yılın başlarında düzenlenen BM konferansında geliştirilen politikalara rehberlik etmeye davet edilmiştir. Söz konusu bu karar doğrultusunda, BM üyelerinin ceza yasalarının siber suçlarla mücadele konusunda yeterli olmasını sağlamak gerektiği vurgulanmıştır. Ayrıca bu kararda BM Genel Kurulu siber suçlarla mücadelede yapılması gereken kanunlar ve devletler arası işbirliğiyle ilgili el kitabı yayınlanmıştır[187].

2000 yılında BM Genel Kurulunun bilgi ve iletişim teknolojilerinin suç işleme amacıyla kullanımına dair çıkardığı kararda, siber suçları önlemek için 1997 yılında Yediler Grubu (G7) tarafından ortaya konulan on ilkeye benzeyen birçok tedbir belirtilmiştir.[188] Bu tedbirler şunlardır:

a. Devletler yasalarında ve uygulamalarında bilgi ve iletişim teknolojilerini kötü kullananlara güvenli sığınaklar oluşturmamaya dikkat etmelidir.

b. Bilgi ve iletişim teknolojilerinin suç işleme amacı ile kullanımına dair davaların soruşturması ve kavuşturması konusunda devletler arasında işbirliği ve koordinasyon sağlanması gerekmektedir.

c. Bilişim teknolojileri suçun aracı olarak kullanımıyla mücadelede karşılaşan sorunlara ilişkin bilgiler konusunda devletler arası karşılıklı yardımlaşma (beraberlik, dayanışma, işbirliği...) olması gerekmektedir.

ç. Kolluk kuvvetlerinin bilişim teknolojilerinin kötü kullanımıyla mücadele edebilecek şekilde eğitilmesi gerekmektedir.

d. Yasal sistemlerin verilerin gizliliğini ve sistemlerin bütünlüğünü koruması, yetkisiz bir şekilde kullananları ise cezai işleme tabi tutması gerekmektedir.

---

[187] Brenner, **a.g.e.**, s. 174; bkz: BM(A/RES/45/121).
[188] Jody R. Westby, **International Guide to Combating Cybercrime**, Chicago, American Bar Association, 2003, s. 110.

e. Hukuk sistemlerinin siber suçların kavuşturmasıyla ilgili elektronik verileri kaydetmesi ve onlara hızlı erişim sağlaması gerekmektedir.

f. Devletler arası karşılıklı yardım sistemlerinde siber suçların kavuşturulması ve delillerin toplanmasına dair işlemlerin uygun zamanda sağlanması gerekmektedir.

g. Bilişim teknolojilerinin suç işlemek maksadıyla kullanımını önleme gerekliliği konusunda insanlarda farkındalık yaratılması gerekmektedir.

ğ. Yasaların bilişim teknolojilerinin mümkün olduğu kadar kötü kullanımı önlenmesi ve suçluların tespit edilmesi konusunda yardımcı olacak şekilde tasarlanması gerekmektedir.

h. Bilişim teknolojilerinin suç işlemek maksadıyla kullanımının önlenmesi, bireylerin özgürlük ve özel hayatlarının dikkate alınarak çözümler geliştirilmesi, devletlerin bu tür suçlarla mücadele etmesi gerektirmektedir[189].

2002 yılında BM Genel Kurulu, bilişim teknolojilerinin suç işlemek için kullanımına dair başka bir karar almıştır. Kararda siber suçlarla mücadelede uluslararası yaklaşım olarak uluslararası işbirliğinin önemine vurgu yapılmıştır. Öte yandan BM ve Avrupa Konseyi başta olmak üzere uluslararası ve bölgesel organizasyonların bu konuda etkin bir rol oynaması gerektiğine dikkat çekilmiştir. Ayrıca devletler siber suçlarla mücadele etmek maksadıyla yasalar çıkarırken BM Suçun Önlenmesi ve Ceza Adaleti Kurultayının ve diğer uluslararası ve bölgesel örgütler tarafından yapılan çalışmaların göz önünde bulundurulması gerektiği belirtilmiştir[190].

Yine BM Genel Kurulu 2002 yılında küresel siber güvenlik kültürü oluşturmak amacıyla bir karar almıştır. Söz konusu bu kararda Küresel bir siber güvenlik kültürü oluşturmak için dokuz unsur belirtilmiştir[191]. Ayrıca üye devletlerin ve ilgili

[189] Bkz: BM(A/RES/55/63).
[190] BM (A/ERES/56/121).
[191]Unsurlar şunlardır: farkındalık, sorumluluk, güvenlik ihlallerine tepki verebilme, ahlak kuraları, demokrasi, risk değerlendirme, güvenlik tasarımı ve uygulaması, güvenlik yönetimi ve yeniden değerlendirmedir.

uluslararası organizasyonların siber güvelik kültürü oluşturması gerekliliği belirtilmiş olup karada belirtilen unsurlara dikkat etmeleri tavsiye edilmiştir[192].

2003 yılında BM Genel Kurulu küresel siber güvenlik kültürünün oluşturulması ve kritik bilişim altyapılarının korunmasına ilişkin başka bir karar daha almıştır. Bu kararda bilişim kritik altyapılarının koruması gerektiği dikkat çekilmiş olup devletler bilişim kritik altyapılarına dair riskleri azaltmak için kendi ulusal kanunlarına göre stratejiler geliştirmeye davet edilmiştir. Ayrıca üye devletlerin, uluslararası ve bölgesel kuruluşların siber güvenlik ve kritik bilişim altyapılarının korunması konusunda izlemesi gereken 11 koşul belirtmiştir[193].

2005 yılında BM Genel Kurulunun aldığı kararda siber suçlarla mücadelede devletlerin ve uluslararası kuruluşların birlikte hareket etmelerinin gerekliliği belirtilmiş ve bu konuda gelişmekte olan devletlerin desteklemesi teşvik edilmiştir.[194]

Genel kurulunun 2011 yılı kararında bilişim teknolojilerinin kullanımında güvenliğin bilgi toplumunun temel direkleri olduğu belirtilmiştir. Dolayısıyla üye devletleri bilişim altyapılarının koruması konusunda sarf ettikleri eforları yeniden değerlendirmeye davet etmiştir[195].

2016 yılında BM Genel Kurulu, Suçun Önlenmesi ve Ceza Adaleti programı ve teknik işbirliğiyle ilgili kararında üye devletlerin ve ilgili uluslararası kuruluşların BM

[192] BM (A/RES/57/239).
[193] Söz konusu koşullar şunlardır: 1. Siber uzaydan kaynaklanan tehditleri ve açıklılarıyla ilgili acil uyarı ağları oluşturulmalıdır, 2. Paydaşların bilgi altı yapılarıyla ilgili rollerine ilişkin farkındalığı artırılmalıdır, 3. Kritik bilgi altı yapılarının güvenliğini artırmak üzere bunları incelenip arasındaki bağlantıları belirlenmelidir, 4. Kamu veya özel paydaşların arasındaki bilgi altı yapılarıyla ilgili iletişimi sağlamak için sağlamak için ortaklıkları güçlendirilmelidir, 5. Kriz halleri için iletişim ağları kurulmalı ve acil durumlarda çalışıp çalışmayacağı test edilmelidir, 6. Bilgilerin erişimiyle ilgili politikaların kritik bilgi altı yapılarını korunma ihtiyacını dikkate alınmalıdır, 7. Kritik bilgi altyapılarının maruz kaldığı saldırıların takibi kolaylaştırılmalı ve söz konusu saldırılar hakkında elde edilen bilgiler diğer devletlerle paylaşılmalıdır, 8. Siber güvelikle ilgili olaylara müdahale kapasitelerini geliştirmek için eğitim verilmeli ve beklenmedik durumlarda test edilmelidir, 9. Kritik bilgi altyapılarına karşı gerçekleştirilen siber saldırıların soruşturulması ve kavuşturulması yapılabilmesi için hukuki düzenlemeler yapılmalı, görevliler yüksek düzeyde eğitime sahip olmalıdır, 10. Kritik bilgi altı yapılarını korumak üzere, çeşitli alanlarda uluslararası işbirliği sağlanmalıdır, 11. Ulusal ve uluslararası araştırma ve geliştirme çalışmaları teşvik edilmeli ve uluslararası normlara kabul edilen güvenlik teknolojisi uygulanması özendirlimelidir. bkz; BM(A/RES/58/199).
[194] BM (A/ RES/60/177).
[195] BM (A/RES/64/211).

Suçun Önlenmesi ve Ceza Adaleti programıyla birlikte uluslararası işbirliğinin prosedürlerini kolaylaştırmak amacıyla bölgesel ve ulusal stratejiler geliştirmeleri ve gereken başka tedbirleri almaları gerektiğini belirtmiştir. Nitekim ulusal sınır aşan suçlar ve çocuklara zarar vermek için yeni teknolojilerin kullanımı konusunda BM'nin ilgili kurumlarla koordine etmek gerekliliğine dikkat çekilmiştir[196].

Son olarak BM Genel Kurulu Dijital çağda gizlilik hakkına ilişkin çok sayıda karar almıştır. 2013 ve 2014 yıllarında alınan kararda teknoloji aracılığıyla ve özellikle devlet dışından yapılan bireylerin iletişim araçlarının takip edilmesi, engellenmesi, kişisel verilerinin müdahale edilmesi gibi insan haklarına karşı işlenen suçlarla mücadele edilmesi vurgulanmıştır. Zira üye devletleri bu hakları korumak için gereken tüm tedbirleri almaya, mevcut koruma araçları ve stratejilerini yeniden değerlendirmeye davet etmiştir[197].

2.1.1.2. Birleşmiş Milletler Ekonomik ve Sosyal Konseyi

Birleşmiş Milletler Antlaşmasının 62. maddesine göre BM Ekonomik ve Sosyal Konseyine uluslararası ekonomik, sosyal, kültürel ve bu alanları kapsayan konulara dair araştırıma yapma yetkisi verilmiştir. Bunun yanı sıra söz konusu Konsey, BM Genel Kurulu ve ilgili diğer kurumlara tavsiyede bulunabilmektedir. Zira yetki alanına giren meselelerde sözleşmeler tasarlayabilmekte ve konferanslar düzenleyebilmektedir[198].

Özellikle BM Ekonomik ve Sosyal Konseyi, Suçun Önlenmesi ve Ceza Adaleti Kurultayı'nı (United Nations Congress on Crime Prevention and Criminal Justice) beş yılda bir düzenlemesiyle birlikte siber suçlarla mücadelede önemli rol oynamaktadır. 2000 yılında Viyana'da yapılan Suçun Önlenmesi ve Ceza Adaleti 10. Kurultayı'nda siber suçlarla ilgili bir atölye çalışması yapılmıştır. Siber suçların türlüleri, siber

[196] BM (A/RES/71/209).
[197] Bkz: BM(A/RES/68/167); (A/RES/69/166); (A/RES/71/199).
[198] Donald A. Wells, **The United Nation: States vs International Laws**, New York, Algora Publishing 2005, s. 26.

suçlarda ulusal sınırlar dışında devletler arası kavuşturulması atölyenin ana unsurlarını teşkil etmiştir. Bunun sonucunda siber suçlarla mücadelede temel stratejiler ortaya konulmuştur. Söz konusu stratejiler şu şekilde sıralanmıştır:

a. Maddi mevzuatın yanında usul kanunu çıkarmak suretiyle siber suçları cezalandıran kanunlar oldukça önemlidir.

b. Kamu ve özel sektörlerinde katılımıyla uluslararası işbirliği gereklidir.

c. Siber suçlarla mücadelede kapasitenin geliştirmesi vurgulanmalıdır.[199]

2001 yılında BM Ekonomik ve Sosyal Konseyi'nin tavsiyesiyle BM Bilgi ve İletişim Görev Gücü (United Nations Information and Communication Technologies Task Force) bilgi ve teknoloji konusunda uluslararası destek sağlamak amacıyla kurulmuştur. Söz konusu kurum 2002'de, siber güvenliğin sorunları ve bununla ilgili çözüm, önerileri, standart ve uygulamalar içeren "Bilgi Güvenliği, Siber Tehditlerin ve Siber Güvenliğin Keşfedilmemiş Bölgelerinde Hayatta Kalabilme Kılavuzu" başlıklı bir kılavuz hazırlamıştır[200].

2010 yılında Brezilya'da BM Suç Önleme ve Ceza Adaleti 12. kongresi düzenlenmiştir. Siber suçlarla ilgili uluslararası sözleşme düzenlenmesi konusunun diğer konferanslara göre daha çok üzerinde durulmuştur. Zira siber suçlarla mücadelede hukuki standartların koordinasyonu ve gelişmekte olan ülkelerin bu konuda nasıl destek alabileceği kongresinin ana unsurlarını oluşturmuştur. Bunun neticesinde "Suç Önleme ve Ceza Adalet Sistemleri ve Gelişimi Değişen Bir Dünyada Küresel Zorluklar İçin Kapsamlı Stratejiler Hakkında Salvador Bildirisi" ortaya konulmuştur. Söz konusu bu bildiride BM tarafından siber suçlara ilişkin uluslararası standartlar konulması gerekliliği belirtilmiştir. Aynı zamanda Salvador Bildirisi'nin 42. maddesi uyarınca devletler arası uzmanlar kurulu kurulmuştur. Söz konusu Uzmanlar Kurulu, üye devletlere teknik yardım, eğitim, ulusal mevzuatın iyileştirilmesi, ulusal makamların kapasitelerinin arttırılması siber suçlarla ulusal ve

[199] Gercke, **a.g.e.**, s. 125.
[200] Mustafa Ünver, Cafer Canbay, Ayşe Gül Mirzaoğlu, **Uluslararası Kuruluşların Siber Güvenlik Faaliyetleri**, Ankara, Bilgi Teknolojileri ve İletişim Kurumu, 2011, s. 4-5.

uluslararası yöntemler geliştirmek konusunda üye devletlerin ilgili uluslarasın kuruluşlarla işbirliği yaparak çalışmalara başlamıştır[201].

2015 yılında Doha'da gerçekleştirilen BM Suç Önleme ve Ceza Adaleti 13. Kongresi'nin hazırlık toplantılarında üye devletler tarafından, siber suçlarla mücadelede kapsamlı tedbirler alınmak ve bu suçların olumsuzluklarıyla ilgili farkındalık yaratmak gerektiği belirtilmiştir. Aynı zamanda devletlerin ulusal düzeyde siber suçlarla ilgili politikalar ve stratejiler geliştirmesi bu suçlarla mücadelenin temelidir[202]. Söz konusu bu kongrenin sonucunda kabul edilen Doha Deklarasyonu'nda, güvenli bir siber alan sağlayabilmek maksadıyla yeni önlemler alınmasının internet üzerinde yapılan suç işleme faaliyetlerini önlemenin altı çizilmiştir. Nitekim siber alanda kimlik hırsızlığı ve çocuk istismarıyla ilgili kolluk kuvvetleri arasında ulusal ve uluslararası düzeyde işbirliğine özel bir ilgi gösterilmiştir[203].

Görüldüğü üzere BM öncülüğünde gerçekleştirilen girişimler uluslararası niteliğinden dolayı oldukça önemlidir. Ancak yukarda bahsedilen girişimler ister BM genel kurulunun kararları isterse BM Ekonomik ve Sosyal Konseyi'nin girişimleri tavsiye niteliği içermesinden ve üye devletleri bağlayıcı olamamasından kaynaklı olarak siber suçlarla mücadelede istenilen sonuç sağlanmamaktadır[204]. Dolayısıyla son yıllarda BM, üye devletlere hukuki yardım yerine teknik destek vermeye ve devletlerin teknik yetkilerini geliştirmeye yönelik tedbirler almaya başlamıştır[205].

---

[201] BM(A/RES/65/230);bkz: (A/CONF.213/18).
[202] (A/CONF.222/12)
[203] UNODC, Doha Declaration on Integrating Crime Prevention and Criminal Justice into the Wider United Nations Agenda to Address Social and Economic Challenges and to Promote the Rule of Law at the National and International Levels, and Public Participation, New York, 2015, (Çevrimiçi), https://www.unodc.org/documents/congress/Declaration/V1504151_English.pdf, Eeişim Tarihi: 15.12.2019. s.10.
[204] Roderic Broadhurst, "Developments in The Global Law Enforcement of Cyber-Crime", **Policing: an International Journal of Police Strategies and Management**, Vol. 29, No. 3, 2006, s. 417.
[205] Fafinski, **a.g.e.**, s. 231-232.

2.1.2. Yediler Grubu (G7)

G7[206] bünyesinde sınır aşan organize suçlarla mücadele girişimlerine, 1995 yılında düzenlenen Halifax Zirvesi'nde başlanmıştır. Genellikle ekonomik işbirliğiyle ilgili faaliyet gösteren G7, terörizm ve uyuşturucu suçları gibi ulusal güveliğe ilişkin sorunlarla ilgilenmiştir. G7 sınır aşan organize suçlarla ilgili sorulara çözüm üretmek için uzmanlardan oluşan çalışma ekibi Lyon Grubu'nu kurmuştur. Söz konusu uzmanlar grubu 1996 yılında yeni bir adım atarak siber suçlarla ilgili hususları ele almaya başlamıştır[207]. G7 siber suçlarla mücadelede girişimleri, G7 Lyon Grubu ve G7 Siber Suçlarla İlgili Diğer Girişimleri olmak üzere iki başlık altında ele alınacaktır.

2.1.2.1.G7 Lyon Grubu

1995 yılında G7 tarafından alt komisyon olarak kurulan "Lyon Grubu", 1996 yılında sınır aşan organize suçlarla mücadeleye ilişkin 40 tavsiye hazırlamıştır[208]. Buna göre devletleri, iç yasalarını yeni teknolojilerle ilgili suçları cezalandıracak şekilde, yeniden değerlendirmeye davet etmiştir. Ayrıca bu tavsiyeler uluslararası toplumlar tarafından referans kaynağı olarak kabul edilmiştir[209]. Nitekim 1997 yılında Lyon Grubu'nun tavsiyelerinin uygulanabilmesi için İleri Teknoloji Suçları Alt Grubu[210] başta olmak üzere 5 komisyon kurulmuştur. Lyon Grubu, siber suçlarla

---

[206] G7 (Group of Seven) dünya ekonomisinin %64'ü oluşturan yedi ülkedir. Söz konusu ülkeler şunlardır: ABD, Almanya, Birleşik Krallık, Fransa, İtalya, Japonya ve Kanada. Bu ülkeler, 1975 yılında küresel ekonominin en önemli sorunu olan petrol krizini tartışmak için bir araya gelerek bir birlik kurmuşlardır. Uluslararası olan bu forum, 1998 yılında Rusya'nın katılmasıyla birlikte "G8" olarak adlandırılmıştır. Ancak 2014 yılında Rusya'nın Kırım Yarımadasını ilhak etmesi dolayısıyla üyeliği askıya alınmıştır. O nedenle kuruluş yeniden G7 ismini almıştır. Bkz; https://www.aydinpost.com/ekonomi/g7-nedir-g7-ulkeleri-hangileridir-h749844.html.

[207] Ian Hosein, "Creating Conventions: Technology Policy and International Cooperation in Criminal Matters", **Governing Global Electronic Networks International Perspectives on Policy and Power,** Ed. William J. Drake, Ernest J. Wilson III, London, The MIT Press, 2008, s. 335.

[208] Fafinski, **a.g.e.**, s.231; Yılmaz, **a.g.e**., s.153; Lyon Grubu'nun tavsiyeleri için bkz: Amandine Scherrer, **G8 against Transnational Organized Crime,** England, Ashgate, Publishing Limited, 2009, s. 149-155.

[209] Scherrer, **a.g.e.**, s. 109-110.

[210] Alt Grupta G7 devletleri, siber suç araştırmacıları ve savcıları ile hukuk sistemleri, adli analiz ve uluslararası işbirliği anlaşmaları uzmanlarını içeren multidisipliner heyetler tarafından temsil edilmektedir. Söz konusu bu Alt Grup, sınır ötesi suçlar, bilgisayar ağları, güvenlik, yardım için

mücadelede devletler arasında bilgi paylaşımı konusunda etkin bir rol oynamıştır. [211] Söz konusu bu grup, G7'ye üye devletlerin siber suçları önlemesi, kavuşturması meselelerinde yeteneklerini ve kapasitelerini geliştirmek için gereken tüm tedbirleri almalarını gerektirmiştir[212].

Söz konusu İleri Teknoloji suçları Alt Grubu'nun siber suçlarla mücadelede attığı en önemli adım, 7/24 çalışan ileri teknoloji suçlarıyla ilgili uluslararası iletişim ağ noktasını (International 24/7 Point of Contact Network) kurmasıdır[213]. Bu mekanizma, devletleler arası siber suçlarla mücadelede birliği sağlamakta ve bilgi erişimini kolaylaştırmak, elektronik deliller içeren acil durumlarda yardım taleplerine yanıt vermek amacıyla 7/24 çalışmaktadır. Diğer yandan bu mekanizma sadece G7 devletlerine değil tüm devletlerin üyeliğine açık olup, Avrupa Birliği üyeleri başta olmak üzere devletleri bu iletişim ağına katılmaya teşvik etmektedir. Dolayısıyla grup üyelerin sayısı 2004 yılında kırka kadar ulaşmıştır[214]. Nitekim bu ağ, çok sayıda devlette siber tehditleri ve diğer suçları araştırmak için birçok durumda kullanılmış olup olumlu sonuçlar elde edilmiştir. Örneğin söz konusu ağ, ABD'de internet kayıtlarının korunması ve suçların tespitini kolaylaştırarak Birleşik Krallık'ta bir katilin mahkum edilmesine yardımcı olmuştur. Ayrıca ağ Amerika Birleşik Devletleri, Almanya ve Meksika'daki bankalara yapılan saldırılar da dahil olmak üzere hackleme saldırılarını önlemek için birkaç kez kullanılmıştır. Buna karşılık, 11 Eylül 2001

uluslararası talepleriyle ilgili ve mevzuat çalışmaları için klavuzlar dahil olmak üzere, çeşitli çalışmalar ve raporlar yayınlamamıştır. Ayrıca siber suçlarla mücadelede uluslararası işbirliği ve terörizmin iletişim takibi hakkında birçok konferans düzenlemiştir. Örnekler arasında, 2000 yılında Paris'te 2001 yılında Berlin ve Tokyo'da ve 2003 yılında Paris'te düzenlenen Sanayi atölyeleri yer almaktadır. bkz: Hosein, **a.g.m.**, s. 200.

[211] Delphine Nain, Neal Donaghy, Seymour Goodman, "The International Landscape of Cyber Security", **Information Security: Policy, Processes, and Practices**, Ed. Detmar W. Straub, Seymour Goodman, Richard Baskerville, New York, M.E. Sharpe, 2008, s. 200.

[212] Weiping Chang, v.d., "An International Perspective on Fighting Cybercrime", **International Conference on Intelligence and Security Informatics,** Ed. Hsinchun Chen, v.d., Berlin, Springer, 2003, s. 382.

[213] Christopher Painter, "Threats to the Net: Trends and Law Enforcement Responses", **Crime and Technology New Frontiers for Regulation, Law Enforcement and Research,** Ed. Ernesto U. Savona, Dordrecht, Springer**,** Springer, 2004, s. 76.

[214] Hosein, **a.g.m.**, s. 200.

terörist saldırılarıyla ilgili devam eden soruşturma bağlamında, belirli bir ülkede bir temas noktası bulunmaması ciddi bir suç soruşturulmasını engellemiştir[215].

Belirtilmesi gerekir ki, 1998 yılında Washington'da G8 üye devletlerinin Adalet ve İçişleri Bakanları tarafından yapılan toplantı sonucunda, siber suçları önlemek için İleri Teknoloji Alt Grubu tarafından hazırlanan 10 prensip ve eylem planı kabul edilmiştir[216]. Söz konusu tüm devletlerin benimsemesi gereken prensipler şunlardır.

a. Devletler bilgi teknolojilerini kötüye kullanan suçlular için güvenli bir sığınak olmamalıdır.

b. Suçun işlendiği yere bakılmaksızın, siber suçların soruşturulması ve kavuşturulması tüm devletler arasında koordine edilmelidir.

c. Siber suçlarla mücadele eden kolluk kuvvetlerine gereken eğitim verilmeli ve zaruri donanım sağlanmalıdır.

ç. Yasal sistemlerin verilerin gizliliğini, bütünlüğünü ve kullanılabilirliğini koruyup bunları yetkisiz bir şekilde kullananları cezalandırması gerekmektedir.

d. Siber suçların soruşturma sürecinin başarılı olmasına yardımcı olan yasal sistemlerin elektronik verilerin korunmasına ve hızlı erişimine izin vermesi gerekmektedir.

e. Devletler arası karşılıklı yardım sistemlerinde siber suçların kavuşturulması ve delillerin toplanması işlemlerinin seri bir şekilde yapılması gerekmektedir.

f. Verilerin bulunduğu sistemlere devletin izni gerekmeden kolluk kuvvetleri tarafından elektronik erişimi sağlanmalıdır.

g. Siber suçlarda kullanılmak üzere elektronik verileri almak ve doğrulamak için adli standartlar ,soruşturma ve kovuşturmalar geliştirilmelidir.

---

[215] Nain, Donaghy, Goodman, **a.g.m.**, s. 201.
[216] Scherrer, **a.g.e.,** s. 110.

ğ. Bilişim teknolojilerinin mümkün olduğu kadar teknolojinin kötü kullanımı önlenmesi ve suçluların tespit etme konusunda yardımcı olacak şekilde tasarlanması gerekmektedir.

h. Söz konusu bu girişimlerin tekrarlanmaması için diğer ilgili uluslararası forumların çalışmaları ile koordine edilmelidir[217].

2.1.2.2.G7'nin Siber Suça İlişkin Diğer Girişimleri

Siber suçlar konusu G7 tarafından düzenlenen konferanslarda da yer almıştır. 1997 yılında Denver Zirvesi'nde, "Devletlerin ulusal sınırları boyunca bilgisayar ve telekomünikasyon teknolojisini kötü kullananlar gibi yüksek teknoloji suçlularının soruşturulması ve cezalandırılması" ve "Siber suçların nerede işlenebileceğine bakılmaksızın, tüm devletlere bu suçlara karşı durabilmek için yasak ve teknik destek verilmesi" konularının G7'nin önceliklerinden biri olduğu belirtilmiştir. Ayrıca G7 devletlerinin dışişleri bakanlıkları raporunda siber suçlarla mücadelede yasal düzenlemeleri yeterli olmadığı kabul edilmiştir. Ona göre ilerleyen bilgisayar ve bilişim teknolojilerinin yeni zorluluklar getirmesiyle birlikte global ağların bu tür suçlarla mücadele için uygun zamanda yanıt vermesi gerekmektedir[218].

2000 yılında Paris'te düzenlenen ilk konferansta G7 ülkelerinin siber suçlulukla mücadele edebilecek şeffaf ve net bir rejim kurmaları gerektiğine dikkat edilmiştir. Zira konferansta iki atölye yapılmıştır. İlki siber suçluların yerleri ve kimliklerini tespit edilmesiyle ilgiliyken, ikincisi siber tehditlerin değerlendirilmesi ve önlenmesi üzerinde yapılmıştır. Diğer yandan 2001 yılında Tokyo konferansında, verilerin korunması ve bireylerin gizlilik haklarıyla ilgili atölyeler yapılmıştır[219].

---

[217] Hosein, **a.g.m.**, s. 236; Meeting of Justice and Interior Ministers of The Eight December 9-10, 1997, (Çevrimiçi), https://www.justice.gov/sites/default/files/ag/legacy/2004/06/08/97Communique.pdf, Erişim Tarihi: 20.12.2019. s.6.

[218]

[219] Hosein, **a.g.m.**, s. 239-141.

Washington 2004 yılında, düzenlenen G7 konferansında, adalet ve İçişleri Bakanları tarafından çıkarılan beyannamede internetin cezai kullanımlarına karşı mücadelede küresel kapasitelerin oluşturulmasına ihtiyaç duyulduğu belirtilmiş olup devletlerin siber suçlara ilişkin yasalarını geliştirmeleri gerektiği vurgulanmıştır. Ayrıca Avrupa Konseyi Siber Suç Sözleşmesi'nin içerdiği hukuki normların kabulüne yönelik adımlar atılmıştır[220].

Moskova'da 2006 yılında düzenlenen konferansta G7 üye devletlerinin siber güvenlik, siber suçlarla mücadele ve siber terörizm konuları ele alınmış ve bunlara karşı alınan tedbirlerin geliştirilmesinin altı çizilmiştir. Zira 2007 senesinde Almanya'da G7 tarafından gerçekleştirilen konferansta terör eylemlerini yapmak için internetin kullanması konusu üzerinde daha çok durulmuştur. 2009 yılında Roma'da siber suçları ele alan konferansta, çocuk pornografi içeren sitelerin engellenmesi ve bununla ilgili ortaya çıkan kara listenin uluslararası kuruluşlar tarafından göz önünde bulundurulması gerektiği kaydedilmiştir[221].

2011 Deauville Zirvesinde ise fikri mülkiyet hakları konusu ele alınmıştır. Söz konusu fikri mülkiyet haklarının koruması G7 için yeni bir konu olamamakla birlikte, son zamanlarda sadece siber alanda ele alınmıştır. Ancak 2011 zirvesinde ilk defa internet ve fikri mülkiyet hakları arasındaki ilişki üzerinde derin bir çalışma yapılmıştır. Özellikle telif hakları, ticari markalar, ticari sırlar ve patentlerle ilgili olarak, devletlerin fikri mülkiyetinin korunması için ulusal yasalar çıkarılması gerekliliği belirtilmiştir. Ayrıca 2011 Deauville Zirvesinden önce "e-G8" adlı Fransa Cumhurbaşkanlığı tarafından özel bir G8 internet konferansı geçekleştirilmiştir. Bu konferansta büyüyen internet ekonomisini tartışmak üzere teknoloji şirketleri, girişimciler, blogçular ve akademisyenleri çağırılmıştır. Bu konferansta çıkan en

[220] Gercke, **a.g.e.**, s. 124.
[221] Gercke, **a.g.e.**, s. 124.

önemli sonuçlardan biri şudur: "fikri mülkiyet hakları korunmadan, sağlıklı ve yaratıcı bir dijital ekonomi gerçekleştirilmez"[222].

2016 yılında Japonya'da düzenlenen G7 konferansında siber güveliğin önemine dikkat çekilmiş ve siber alanın kötüye kullanımına karşı durabilmek için devletler ve diğer uluslararası organizasyonlarla işbirliğini güçlendirmek üzere alınması gereken önlemler üzerinde durulmuştur. Ayrıca tüm devletlerin, 2015 yılanda BM Hükümet Uzmanları Grubu (Groups of Governmental Experts) tarafından hazırlanan uluslararası hukukun siber uzayda devlet davranışına uygulanabilirliği ve bilgi teknolojileri güvenliği ve kapasite geliştirme konusunda uluslararası işbirliği ve yardımlaşmayla ilgili raporda[223] yer alan tavsiyelere uymaları salık verilmiştir[224]. Diğer yandan yeterince emniyetli bir siber alan tedarik etmeye yönelik G7 üye devletlerin strateji ve politikalar geliştirmeleri gerektiği vurgulanmıştır. Zira gelişmekte olan ülkeler ve gelişmiş ülkeler arasında dijital boşluğu ortadan kaldırmak maksadıyla tedbir uygulamalarının gerekliliğine dikkat edilmiştir[225].

2.1.3. Ekonomik Kalkınma ve İşbirliği Örgütü (OECD)

Paris'te merkezi olan Ekonomik Kalkınma ve İşbirliği Örgütü, demokratik rejime ve piyasa ekonomisine sahip olan 36 üye devletten oluşmaktadır[226]. Söz konusu üye devletler, ekonomik ve sosyal politikaları geliştirmek amacıyla toplantı

[222]Abdi Aidid, v.d., 2011 Deauville G8 Summit Final Compliance Report, (Çevrimiçi), http://www.g7.utoronto.ca/evaluations/2011compliance-final/2011g8finalcompliance.pdf, Erişim Tarihi: 15.12.2019, s. 236-237.

[223] BM(A/70/174), Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, Çevimiçi, https://undocs.org/pdf?symbol=en/A/70/174, Erişim Tarihi: 15.12.2019.

[224] G7 Principles and Actions on Cyber, (Çevrimiçi), https://www.mofa.go.jp/files/000160279.pdf, Erişim Tarihi: 15.12.2019, s. 1.

[225] Chair's Report of the Meeting of the G7 Ise-Shima Cyber Group, (Çevrimiçi), https://ccdcoe.org/uploads/2018/11/G7-180423-IseShimaChairsReport.pdf. Erişim Tarihi: 15.12.2019.

[226] OECD, 1960 yılında imzalanan Paris Sözleşmesi uyarınca 1961 yılında kurulmuştur. İkinci Dünya Savaşında yıkılan Avrupa'nın Marshall Planı kapsamında yeniden inşa etmesini amaçlayan bu organizasyon 1948 yılında kurulan (OEEC) Avrupa Ekonomik İşbirliği Organizasyonu'nun uzantısıdır. bkz: https://disiliskiler.ktb.gov.tr/TR-22153/ekonomik-isbirligi-ve-kalkinma-orgutu-oecd.html.

düzenlemektedirler. Küreselleşmenin getirdiği sorunlara ve diğer ortak problemlere çözümeler bulmak için iç ve dış politikaları koordine etmektedirler[227].

OECD, siber suçlarla mücadelede ve siber güveliğin korunması konusunda önemli adımlar atmıştır. Örgüt, uluslararası alanda siber suçlara ceza hukuku uygulama sürecinin sorunlarına ilişkin kapsamlı bir çalışma başlatan ilk kuruluş olmuştur. 1983 yılında örgütte bir grup uzman tarafından, OECD'nin Avrupa devletlerinin siber suçlarla ilgili mevzuatlarını uyumlu hale getirmek maksadıyla girişimde bulunması tavsiye edilmiştir[228]. Siber suç sorunu 1983-1985 yıllar arasında yapılan incelemenin sonucunda 1986'da Bilgisayarla İlişkili Suç: Yasal Politikanın Analizi " Computer related Crime: Analysis of Legal Policy" başlıklı bir rapor hazırlanmıştır[229]. Raporda Avrupa devletlerinin yürürlükte olan kanunları ve reform tavsiyeleri bulunmaktadır. Ayrıca dünyadaki temel pozitif yasalar karşılaştırılmış olup ülkelerin ceza yasaları kapsamında cezaya tabi tutulması gereken siber suçlarla ilgili asgari eylemlere ilişkin bir liste önerilmiştir[230].

OECD, 1992 yılında örgüt, kamu ve özel sektöre yönlendirilen bilişim güvenliğiyle ilgili bir yönergeler kabul etmiştir. Söz konusu bu tavsiyede bilişim sistemlerinin güvenliği için asgari standartların uygulanıp kötü kullananlara cezai ve idari yaptırımlar uygulanması gerektiğine dikkat edilmiştir[231]. Ayrıca 1996 yılında OECD tarafından kurulan şifreleme uzmanlardan oluşan Committe on Information, Communications and Computer Policy (ICCP)[232], Bilişim ve Bilgisayar Politikası Komitesi'nin, ortaya koyduğu şifreleme teknolojisi, kolluk kuvvetleri ve gizlilik endişeleri ile ilgili üye devletlerin şifreleme politikalarını koordine edebilecekleri araçların değerlendirilmesinde çok sayıda yönergeler, 1997 yılında OECD tarafından

---

[227] Marc Goodman "International Dimensions of Cybercrime", **Cybercrimes: A Multidisciplinary Analysis**, Ed.,Sumit Ghosh, Elliot Turrini, Berlin, Springer, 2010, s. 326

[228] Ana I. Cerezo, Javier Lopez , Ahmed Patel, "International Cooperation to Fight Transnational Cybercrime", Second International Workshop on Digital Forensics and Incident Analysis, **IEEE**, 2007, s. 16.

[229] Goodman, **a.g.m.**, s. 326

[230] Nain, Donaghy, Goodman, **a.g.m.**, s.197.

[231] Sieber, **a.g.e.,** s.157.

[232] Bkz: OECE (ICCP), (Çevrimiçi), http://www.oecd.org/internet/ieconomy/37328586.pdf, Erişim Tarihi: 20.12.2019.

kabul edilmiştir[233]. Zira 2001 yılında meydana gelen terör saldırıları sonrasında OECD üye devletleri, siber terörizm, bilgisayar virüsleri, "hackleme" ve ilgili tehditlere karşı koymak için tasarlanmış bir dizi yönerge ortaya çıkarmıştır[234].

OECD, 2002 yılında bilgi sistemleri ve ağlarının güveliğiyle ilgili farkındalık yaratmak maksadıyla yeni yönergeler ortaya koymuştur[235]. 2003 yılında Norveç'te OECD örgütünün uluslararası bilişim sistemleri ve ağların güvenliği forumu düzenlenmiş olup siber suçlarla ilgili çalıştay da yapılmıştır. Ayrıca 2004 yılnda OECD bünyesinde kurulan "Yığın mesaj" olarak bilinen Spam'la ilgilenen grup, 2006 yılında bir rapor hazırlamış ve söz konusu bu mesajlarla mücadele için birçok mekanizma ortaya koymuştur. Diğer yandan kötü yazılımlarla ilgili birçok çalıştay düzenlenmiştir[236].

2008'de OECD, internet üzerinden kimlik hırsızlığıyla ilgili olan "OECD Policy Guidance on Online Identity Theft" raporu hazırlamıştır[237]. Üye devletlerin internet üzerinde kimlik hırsızlığına karşı stratejilerini geliştirmek, bu konuda eğitim vermek ve farkındalık yaratmak amacı olan bu rapor, siber uzayda kimlik hırsızlığıyla ilgili işlenen suçların yöntemlerini açıklamakta, devletlere ve özel sektöre birçok öneri sunmaktadır[238].

Son olarak esnek hukuk "Soft law" olarak bilinen OECD önerileri, çeşitli uluslararası meseleler hakkında devletlerin politikalarıyla ilgili bağlayıcı olmayan bir araçtır. Örneğin siber uzayın kötüye kullanılması, gizlilik, şifreleme teknolojisi, verilerin korunması, tüketicinin korunması ve siber güveliktir. Söz konusu önerileri amacı, belirli bir konu hakkında devletlerin politikalarını geliştirmektir[239].

---

[233] Websty, **a.g.e**., s. 109.
[234] Broadhurst, **a.g.m.,** s. 425.
[235] Bkz: OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security, https://www.oecd.org/internet/ieconomy/15582260.pdf, Erişim Tarihi: 20.12.2019.
[236] Stein Schjolberg, **The History of Cybercrime: 1976-2014**, Germany, Cybercrime Research Institute, 2014, s. 96-97.
[237]OECD, Policy Guidance on Online Identity Theft, (Çevrimiçi), https://www.oecd.org/sti/consumer/40879136.pdf, Erişim Tarihi: 20.12.2019.
[238] Schjolberg, **a.g.e.,** s.97.
[239] Westby, **a.g.e.,** s. 109.; Broadhurst, **a.g.m.**, s. 425.

2.1.4.Uluslararası Telekomünikasyon Birliği

BM'ye bağlı olan Uluslararası Telekomünikasyon Birliği (ITU)[240]siber güvenlik ve bilişim teknolojileriyle ilgili çalışmalar yapmakta olup üyelerin arasında kamu ve özel sektörler yer alabilmektedir. Cenevre merkezli olan ITU'e bağlı 193 üye devletin bulunmasının yanı sıra özel sektör üyelerinin sayısı 700'den fazladır[241]. ITU'nun faaliyetleri radyo iletişimi, standardizasyon ve geliştirme olmak üzere üç ana alana odaklanmaktadır. Zira ITU, radyo spektrumunun ortak global kullanımını koordine etmekle birlikte siber suçlar ve uluslararası telekomünikasyon standartlarının geliştirilmesinde de önemli rol oynamaktadır[242].

ITU,1998 yılında aldığı kararda Dünya Bilgi Toplumu Zirvesi (WSIS) düzenlemesi için öncü olmuştur. Söz konusu bu zirvenin 2001 yılında ITU konseyi tarafından iki aşamada gerçekleştirilmesine karar verilmiştir. İlki 2003 yılında Cenevre'de, ikincisi ise 2005'te Tunus'ta gerçekleştirilmiştir. Söz konu Dünya Bilgi Toplumu Zirvesi'nde siber suçlar konusu ele alınmış olup bilgi toplumunun en önemli unsuru olan siber güvenliğin korunması gerekliliği vurgulanmıştır[243]. Söz konusu WSIS'ın sonucunda Bilgi ve iletişim teknolojisinin kullanımında güvenlik oluşturmaya yönelik olan C5 planın uygulanması için ITU, kolaylaştırıcı tek aday olarak gösterilmiştir[244]. Ayrıca siber suçlarla mücadele ve siber uzayda güveliği

---

[240]1865 yılında Avrupa devletlerin arasında yapılan bilgi ve iletişim teknolojisiyle ilgili çeşitli sözleşmelerin sonucunda Uluslararası Telgraf Birliği kurulmuştur. ITU'nun yirmi Avrupa ülkesi tarafından kurulmasına rağmen kurulduğunda tüm devletlere ulaşmıştır. Zira üyelerinin birçoğunun sömürge mülkiyeti söz konusu olmuştur. Ayrıca ekonomik faaliyetlerini kolaylaştırmakta, ticareti desteklemekte ve uluslararası barış ve güvenliği korumakta önemli rol oynamıştır. Dolayısıyla uluslararası kalkınmayı desteklemiştir. Söz konusu en eski uluslararası kurum olan ITU sadece ilk uluslararası kurum olmamakta birlikte karar alma süreçlerine devlet dışı sektörleri dahil eden ilk kurumdur. bkz: Don Maclean, "Sovereign Right and the Dynamics of Power in the ITU: Lessons in the Quest for Inclusive Global Governance", **Governing Global Electronic Networks International Perspectives on Policy and Power,** Ed., William J. Drake, Ernest J. Wilson III, London, The MIT Press, 2008, s. 83-84; Rolf H. Weber, **Shaping Internet Governance: Regulatory Challenges**, Berlin, Springer, 2010, s. 41-42.

[241] Özüdoğru**, a.g.m.**, s.55.

[242] Rolf H. Weber, Ulrike I. Heinrich, **Anonymization,** London, Springer, 2012, s.53.

[243] Stein Schjolberg, Amanda B. Hubbard "Harmonizing National Legal Approaches on Cybercrime", International Telecommunication Union, WSIS Thematic Meeting on Cybersecurity, 2005, s. 6.

[244] Gercke, **a.g.e.**, **s**. 131.

koruma konusunda işbirliğinin sağlanması amacıyla ITU genel Sekreterliği, hükümetler, uluslararası organizasyonlar ve sivil toplum kuruluşlarıyla bir araya gelerek 2007 yılında ilgili Küresel Siber Güvenlik Gündemi'ni (Global Cybersecurity Agenda) ortaya çıkarmıştır. Buna göre siber uzayda işlenen suçların soruşturulması, ulusal yasalara bakılmaksızın uluslararası hukuk uyarınca olmalıdır[245].

Söz konusu Küresel Siber Güvenlik Gündeminde siber suçlarla mücadele kapsamında 7 hedef belirtilmiştir. Hedefler şunlardır:

a. Global olarak siber suçlarla ilgili uygulanabilir model yasalar koymak için stratejilerin belirlenmesi, aynı zamanda bu stratejiler uluslararası, bölgesel ve ulusal hukuki tedbirlere uyumlu hale getirilmesi,

b. Siber suçlarla mücadelede uygun ulusal ve bölgesel yapıların geliştirilmesi için genel bir politika modelinin ve ulusal stratejilerin oluşturulması,

c. Siber güvenlik, yazılım uygulamaları ve sistemleriyle ilgili küresel olarak kabul edilen minimum standartların konulması için Stratejiler geliştirilmesi,

ç. Mevcut tedbirlerin yanı sıra sınır ötesi koordinasyonu sağlamak maksadıyla siber suçlarla izleme, uyarı ve olay tepkilerini kapsayan küresel bir çerçevenin oluşturulması için stratejilerin geliştirilmesi,

d. Dijital kimlikle ilgili genel küresel bir sistem oluşturulması, coğrafi sınırlar dışarısında kalan bireyler için dijital kimlik sisteminin hayata geçirilmesi ve gerekli organizasyon yapılarının oluşturulması,

f. Bilişim alanda beşeri ve kurumsal kapasitenin geliştirilmesine kolaylaştırılacak küresel bir stratejinin belirtilmesi,

g. Yukarıda bahsedilen tüm hedefleri gerçekleştirmek ve uluslararası işbirliğini desteklemek üzere taraflarla birlikte küresel strateji oluşturulmasıdır[246].

[245] Weber, **a.g.e.,** s. 53.
[246] Gercke, **a.g.e.**, s. 131-132; Weber, **a.g.e.,** s. 54; Cerezo, Lopez , Patel**, a.g.m.**, s. 18.

GCA'nın yedi hedefi ile ilgili tedbirler ve stratejileri geliştirmek için, ITU Genel Sekreterliği, üye Devletler, endüstri ve bilimsel alandaki temsilcilerden oluşan üst düzey bir uzman grubu (High-Level Expert Group) oluşturmuştur.[247] Söz konusu grubun yayınladığı Küresel Stratejisi Raporu'nda siber suçlarla ilgili yasal önlemler, teknik ve prosedürel tedbirle, örgütsel yapılar, kapasite geliştirme ve uluslararası işbirliği hususların üzerinde durulurmuştur.[248]

Bilgi ve iletişim teknolojisini destekleme doğrultusunda ITU, 2008 yılında (ITU-EC-ACP Project) başlığı altında üç proje kabul etmiştir. Dünyanın hızla gelişen Afrika, Karayıp Denizi ve Büyük Okyanus (ACP) bölgelerindeki devletlerde bilişim teknolojileriyle ilgili uluslararası, bölgesel ve ulusal politikalar ve teknoloji konusunda beşeri kapasiteleri geliştirmeyi amaçlayan projelerin her biri için özel yaklaşımlar hazırlanmıştır. Söz gelimi projeler bağlamında hazırlanan model kanunlarda maddi hukuk olarak siber suç türleri, usul hukuku tedbirleri, yargı yetkisine ve devletler arasında işbirliğiyle ilgili hükümler yer verilmiştir[249]. Projeler şunlardır:

a. HIPCAR Projesi:[250] Karayıp Denizi bölgesindeki devletlerin rekabet gücünün artırılması için bilişim teknolojilisiyle ilgili politikaları ve Mevzuat ve Düzenleyici Prosedürlerin birbiriyle uyumlu hale getirilmesi hedeflenmiştir.

b. HIPSSA Project: Sahra Altı Afrika'da bulunan devletlerin bilişim teknolojisiyle ilgili politikalarının uyumlu hale getirilmesinin desteklenmesi için hazırlanmıştır.

[247] Bkz: ITU Global Cybersecurity Agenda (GCA), High-Level Experts Group (HLEG), (Çevrimiçi), https://www.itu.int/en/action/cybersecurity/Documents/gca-chairman-report.pdf, Erişim Tarihi: 21.12.2019.
[248] Gercke, **a.g.e.**, s. 132.
[249] Erdem, Özocak, **a.g.m.**, s. 164-165.
[250] Bkz: HIPCAR Harmonization of ICT Policies, Legislation and Regulatory Procedures in the Caribbean , (Çevrimiçi), http://caricom.org/documents/16583-universal_service_and_access_mpg.pdf, Erişim Tarihi: 20.12.2019.

c. ICB4PAC Projesi: yine Büyük Okyanus devletleri için bilişim teknolojisiyle ilgili politikalar geliştirmek ve bunula ilgili yasal çerçevelerini desteklemek için konulmuştur[251].

ITU hakkında belirtilmesi gereken son husus, siber suç konusunu ele alan siber güvenlikle ilgili çok sayıda karar almış olmasıdır. Bunlar örneğin, ITU'nun bilgi ve iletişim teknolojilerinin kullanımında güven sorunun ve güvenliğin geliştirilmesindeki rolünün güçlendirilmesiyle ilgili karar (Guadalajara, 2010, 150 numaralı) ve siber güvenlikle ilgili işbirliğini geliştirmeye yönelik mekanizmalarla ilgili olan karardır (Doha, 2006, 45 numaralı) [252].

2.1.5. İnterpol

BM'den sonra en büyük uluslararası kriminal polis teşkilatı olan Interpol, 1923 yılında suçlara karşı devletler arası polis işbirliğini gerçekleştirmek, desteklemek ve geliştirmek amacıyla kurulmuştur[253]. Buna göre Interpol ,"Daha güvenli bir dünya yaratabilmek için vardır… Suçla mücadelede uluslararası girişimleri en iyi şekilde geliştirmek için kolluk kuvvetlerinin gerek duyduğu benzersiz bir dizi hizmetleri sağlamaktır"[254]. Günümüzde Interpol'ün üye devletlerin sayısı 190'e kadar ulaşmıştır. Dolayısıyla siber suçu önleme ve suçluları tespit etme yeteneklerini güçlendirmek için dünyanın dört bir yanındaki kolluk kuvvetleriyle birlikte çalışma imkânı sağlayabilmektedir.

1990 yılından beri siber suçlarla mücadelede aktif bir rol oynayan Interpol,[255] siber saçlarla mücadeleyi en önemli önceliklerden biri haline getirtmiştir. Interpol, söz

---

[251] ITU-EC-ACP Project, Support for the Establishment of Harmonized Policies for the ICT Market in the (ACP) States,, (Çevrimiçi), https://www.itu.int/en/ITU-D/Projects/ITU-EC-ACP/Pages/default.aspx, Erişim Tarihi: 20.12.2019.

[252] Gercke, **a.g.e.**, s.132; daha fazla kararlar için bkz: Richard Hill, **The New International Telecommunication Regulations and the Internet A Commentary and Legislative History,** Berlin, Springer, 2014, s. 125-141.

[253] Yılımaz, **a.g.e.**, s. 163; Durmuş Tezcan, Mustafa Ruhan Erdem,R. Murat Önok, **Uluslararası Ceza Hukuku,** 4.bs, Ankara, Seçkin Yayıncılık, 2019, s. 188 .

[254] Goodman, **a.g.m.**, s. 332.

[255] Nain, Donaghy, Goodman, **a.g.m.**, s. 203.

konusu bu suçlarla ilgili faaliyetlerini üye ülkelerdeki Ulusal Merkezleri aracılığıyla koordine etmektedir[256]. Interpol'ün görevi, şüpheli kişiler, gruplar ve faaliyetleri hakkında bilgileri toplamak, depolamak, analiz etmek ve paylaşmaktır. Organizasyon ayrıca üye ülkelerde bulunan teröristlere, tehlikeli suçlulara ve silah tehditlerine karşı uyarı ve uyarıların dolaşımını koordine etmektedir[257].

Sınır aşan siber suçlarla mücadele kapsamında Interpol tarafından 2017 yılında bir strateji hazırlamıştır. Söz konusu bu strateji, üye devletlere karşı gerçekleştirilen siber saldırıların faillerini tespit etmeye yönelik beş etkenden oluşmaktadır. Buna göre[258]:

a. Siber tehditlerin tespit edilmesi, tehdidin değerlendirilmesi, analizi ve eğilimleri izleme yoluyla gerçekleştirilir.

b. Siber saldırın tespit edilmesini kolaylaştıracak temel dijital verilere erişimi sağlanmasıdır.

c. Siber saldırılarla ilgili dijital delillerin mahkeme tarafından kabul edilir hale getirilmesi için bu delillerin hukuki olarak toplanması ve korunmasıdır.

ç. Muhtemel siber faillerin yerini tespit etmek üzere dijital deliller ve fiziksel delilerle bağlantı kurarak bunlar arasındaki boşluğu doldurulmasıdır.

d. Yasaların uyumlaştırılması, uluslararası işbirliği ve koordinasyonun teşvik edilmesidir.

Son olarak Interpol tarafından siber suçlarla mücadele doğrultusunda yapılan operasyonlara örnek vermek gerekirse, 2015 yılında Interpol, (Tayland, Filipin, Kamboçya, Vietnam) devletlerin polisleriyle işbirliği yaparak, internet aracılığıyla hukuka aykırı olarak kumar ve dolandırıcılık suçu işleyen suç örgütlerine karşı bir

---

[256] Broadhurst, **a.g.m.**, s. 426.

[257] Rob van den Hoven van Genderen, "Cybercrime Investigation and the Protection of Personal data and Privacy", Economic Crime Division Directorate General of Human Rights and Legal Affairs, b.y., Strasbourg, 2008, s. 42.

[258] Interpol, Global Cybercrime Strategy , (Çevrimiçi), https://www.interpol.int/content/download/5586/file/Summary_CYBER_Strategy_2017_01_EN%20LR.pdf?inLanguage=eng-GB, Erişim Tarihi: 25.12.2019.

operasyon gerçekleştirmiştir. Bunun sunucunda 48 kişi tutuklanmış olup 10 milyon dolar değerinde para haczedilmiştir. Ayrıca söz konusu bu suç örgütünün 200 milyon dolar miktarında para kazandığı tahmin edilmiştir[259].

2.2. Bölgesel Organizasyonlar

2.2.1. Avrupa'nın Siber Suçlarla Mücadele Girişimleri

2.2.1.1. Avrupa Konseyi

Avrupa Konseyi, 1949 yılında Avrupa ülkeleri arasında güvenliği kurumak ve işbirliği sağlamak maksadıyla kurulan bir organizasyon olup üyeliğinde Türkiye ve Rusya dahil olmak üzere 47 üye[260] ve ABD, Kanada, Japonya ve Meksika gözlemci olarak bulunmaktadır.[261] Keza Avrupa'nın ortak sorunlarına (örneğin, insan hakları, sosyal güvenlik, çevre, bölgesel politikalar v.s.) çözüm üretmektedir. Avrupa hukuk düzeni ve ortak standartlar kurmayı amaçlayan Avrupa Konseyi, genellikle bu konularda devletlerin ulusal yasalarını uyumlu hale getirmek için sözleşmeler ve protokoller düzenlemektedir[262].

Siber suç sözleşmesine gelmeden önce Avrupa Konseyi'ndeki siber suçlarla ilgili gelişmelere yer vermekte yarar vardır. 1970 yıllarında banka sektörlerinde kişisel verileri otomatik olarak işlenmeye başlanmıştır. Dolayısıyla Avrupa konseyi, bireylerin özel hayatını korumaya ilişkin çalışmalar doğrultusunda, Almanya, Fransa, Danimarka, Avusturalya ve Norveç devletlerinin ulusal yasaları dahil eden iki tavsiye kararı kabul etmiştir. Daha sonra da iletişim sistemlerinin ortaya çıkardığı problemlerden biri olan özel verilere yasa dışı bir şekilde erişebilmesi ve müdahale edilmesine Avrupa ülkelerinin ulusal kanunları aciz kalmıştır. Bundan ötürü Avrupa

[259] Yılmaz, **a.g.e.**, s. 163-164.
[260] Marc Goodman, **a.g.m.**, s. 330.
[261] Fafinski, **a.g.e.**, s. 208.
[262] Akarslan, **a.g.e**., s. 152; Özüdoğru, **a.g.m.**, s. 64-65.

Konseyi'ne üye devletler tarafından 1981 yılında 108 sayılı "Kişisel verilerin Otomatik İşleme Tabi Tutulması karşısında bireylerin korunması" sözleşmesi imzalanmıştır[263].

Avrupa Konseyi'nin siber suçlarla ilgili çalışmaları 1980'lı yıllarda başlamış olup bu suçlarla ilgili çalışmaları yürütmek amacıyla konsey tarafından uzmanlar komitesi kurulmuştur. Söz konusu siber suçlara ilişkin çalışmanın amacı üye devletlere ceza kanunlarında cezalandırılması gereken siber eylemleri belirtmek, özgürlük ve güvenlik arasında ortaya çıkan uyuşmazlığın üstünden gelineceği yöntemleri açıklamaktır[264].

Kurulan Uzmanlar Komitesi, Ekonomik Kalkınma ve İşbirliği Örgütü (OECD) tarafından 1986 yılında yayınlanan(Bilgisayarla İlgili Suç: Hukuk Politikası Analizi) başlıklı raporu referans alarak raporda yer alan eylemleri üye devletlerin ceza yasalarında cezalandırılması gerektiği belirtilmiştir. Ayrıca söz konusu raporda belirtmeyen siber suçlarla ilgili ilkeleri de vurgulanmıştır[265].

Siber suçlarla ilgili çalışmalara devam eden Uzmanlar Komitesi, 1989 yılında tavsiye kararı almıştır. Söz konusu R (89) 9 numaralı tavsiye kararında sınır aşan niteliğe sahip olan siber suçlarla mücadele etmek için hızlı tepki verilmesine, üye devletlerin yasalarının koordinasyonuna ve uluslararası işbirliğinin önemine dikkat edilmiştir. Ayrıca üye devletlerin ulusal yasalarında siber suçlarla ilgili cezaya tabi tutulması gereken eylemlere ilişkin iki liste hazırlanmıştır. İlki Uluslararası mutabakat tarafınca cezaya tabi tutulması gereken siber suçlara ilişkin asgari listesi, diğeri ise uluslararası uzlaşma sağlanması güç olan suçlarla ilgili seçmeli bir listedir[266].

1991 yılında siber suçlarla ilgili ortaya çıkan soruşturma sorunlarına çözüm bulmak için Avrupa Konseyi tarafından başka bir Uzmanlar Komitesi kurulmuştur. 1995 yılında söz konusu Uzmanlar Komitesi, siber suçlarla ilgili R (95) 13 numaralı

[263] Dülger, **a.g.e.**, s. 197.
[264] Özüdoğru, **a.g.m.**, s.65.
[265] Akarslan, **a.g.e.**, s. 152; Dülger, **a.g.e.,** s. 197; Özüdoğru, **a.g.m.**, s. 65.
[266] Bkz: Goodman, **a.g.m.**, s. 330.

tavsiye kararı almıştır[267]. Kararda siber suçların soruşturulması ve kavuşturulmasıyla ilgili detaylı prensipler belirtilmiştir. Yani 1989 yılında alınan tavsiye kararında siber suçlarla ilgili maddi hukukunun ihtiyacı vurgulanırken, 1995'te alınan tavsiyede usul hukukunun ihtiyacına dikkat çekilmiştir. Etkisi sınırlı söz konusu tavsiyelerden hareketle siber suçlarla ilgili bağlayıcı bir sözleşme düzenlemek üzere Avrupa Konseyi tarafından 1997 yılında Siber Alanda Suç Uzmanları Komitesi (PC-CY) kurulmuştur. Bunun sonucunda Macaristan'ın başkenti olan Budapeşte'de2001 yılında Avrupa Konseyi Siber Suçlar Sözleşmesi imzalanmıştır[268].

Söz konusu Avrupa Konseyi tarafından yapılan siber suçlarla mücadelede önemli ve kapsamlı bir çalışma olan Siber Suçlar Sözleşmesi, internet ve bilgilerle işlenen suçlarla ilgili ilk bağlayıcı uluslararası çok taraflı sözleşmedir[269]. Avrupa konseyi üye ve üye olmayan toplam 51 devlet tarafından imzalanan[270] bu sözleşme 2004 yılında yürüklüğe girmiştir[271]. Uluslararası hukuk aracılığıyla siber suçların ortaya çıkardığı sorunlara çözümler sunan sözleşmenin temel amaçları şunlardır[272].

a. Taraf devletlerin siber suçlarla ilgili ulusal maddi mevzuatlarının uyumlu hale getirilmesi.

b. Siber suçların soruşturulması ve kavuşturulmasıyla ilgili ulusal yasaları yeknesak hale getirmektir.

c. Bu suçlarla mücadele etmek üzere uluslararası işbirliği ve adli yardımlaşmaya ilişkin etkin ve hızlı bir mekanizma kurmaktır.

Söz konusu bu sözleşme 48 madde ve 4 ana bölümden oluşmaktadır. Birinci bölümde siber suçlarla ilgili terimler açıklanmaktadır. İkinci bölümde üye devletlerin

---

[267] Dülger, **a.g.e.,** s. 197.
[268] Marc Goodman, **a.g.m.**, s. 330-331; Amalie M. Weber, "The Council of Europe's Convention on Cybercrime", **Berkeley Technology Law Journal**, Vol. 18, No.1, 2003, s. 428-429.
[269] Goodman, **a.g.m.**, s. 331; Weber, **a.g.m.**, s. 430.
[270] Siber suç soruşturmaları için hayati önem eken iki ülke, Rusya ve Çin, söz konusu Sözleşme'yi onaylamamışlardır. Bu durum siber suçlarla global mücadeleye olumsuz bir şekilde etkileyebilmektedir. Jan-Jaap Oerlemans, **Investigating Cybercrime**, Amsterdam, Amsterdam University Press, 2017, s. 60.
[271] Dülger, **a.g.e.**, s. 198.
[272] Fafinski, **a.g.e.**, s. 210; Goodman, **a.g.m.**, s. 331.

siber suçlarla ilgili alması gereken iki tedbir belirtilmektedir. Bunların ilki ulusal maddi hukukunda siber suçlarla ilgili cezaya tabi tutulması gereken eylemler[273] ve tanımlar, diğeri ise ulusal usul hukuku ve yetki sorunlarıyla ilgili hükümlerdir. Üçüncü bölümünde uluslararası işbirliği ve adli yardımlaşmaya yönelik özel hükümler içermektedir. Son bölümünde ise sözleşmenin uygulanması ve katılımına dair kurallara yer verilmektedir[274].

Sözleşmeye ek olarak 2003 yılında Avrupa Konseyi tarafından "Bilişim Sistemleri Aracılığıyla İşlenen Irkçı ve Yabancı Düşmanlığı Suçları" ile ilgili bir protokol imzalanmıştır[275]. Protokol'ün temel amacı, siber alanda ırkçı ve yabancı düşmanlığı içeren her çeşit faaliyetlerin ulusal yasalarda suç olarak düzenlenmesidir. Bu tür eylemlerin ayrı bir metinde ele alınmasının nedeni, bu eylemler üzerinde uzlaşmaya varılmamış olunmasıdır. Kimi devletler, bu eylemelerin suç olarak düzenlenmesinin ifade özgürlüğünü kısıtlayabileceğinden endişe duymaktadır[276]. Ayrıca Avrupa Konseyi tarafından 2007 yalında Avrupa Konseyi Çocukların Cinsel Sömürü ve İstismara Karşı Korunması Sözleşmesi akdedilmiştir. Sözleşmenin temel amacı çocuğun hakların korumak, çocuk istismarı suçları önlemek ve bu suçlarla mücadele noktasında üye devletler arasında işbirliği sağlamaktır. Sözleşme'nin getirdiği en önemli husus çocuk pornografisi eylemleri üye devletlerin ulusal yasaların suç olarak düzenlenmesi için gereken önlemleri yapmaları yükümlüğüdür[277].

Söz konusu Avrupa Konseyi Siber Suç Sözleşmesi çeşitli yönlerden eleştirilmektedir[278]. İlk eleştiri, Sözleşme'nin çekincelere büyük bir şekilde imkan sağlaması, temel amacı olan devletlerin ulusal yasalarının uyumlu hale getirmekle

[273] Bkz: bu çalışma, birinci bölüm, s. 30.
[274] Aliusta, Benzer, **a.g.m.**, s. 38. Akarslan, **a.g.e.**, s. 153-154.
[275] Akarslan, **a.g.e.**, s. 154.
[276] Dülger, **a.g.e.**, s. 202.
[277] Merve Erdem, Gürkan Özocak, "Siber Güvenliğin Sağlanmasında Uluslararası Hukukun ve Türk Hukukunun Rolü", **Ankara Üniversitesi Hukuk Fakültesi Dergisi,** C. LXVI, S.1., 2019, s. 160
[278] Murat Önok, "Avrupa Siber Suç Sözleşmesi Işığında Siber Suçlarla Mücadelede Uluslararası İşbirliği", **Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi**, C.IX, S.2, 2013, s. 1245.

bağdaşmamaktadır[279]. İkinci eleştiri siber suçların akıl almaz bir hızla gelişmesine karşı Sözleşme'nin 44. Maddesinde yer alan değişiklik yapma süreciyle ilgili zorunlu şartlara bağlanması, söz konusu gelişmelere ayak uydurulmamasına yol açabilmektedir[280]. Ancak bu durumda ortaya çıkan aksaklıklar protokoller aracılığıyla düzeltilebilmektedir[281]. Üçüncü eleştiri, Sözleşme, devletlerin arasındaki teknik yeteneklerine riayet etmemektedir. Diğer anlatımla Sözleşme'ye göre siber suçluları yakalayabilmek için devletler tarafından birçok prosedür benimsemesi gerektirmektedir. Ancak düşük kapasiteli bazı devletler bunu uygulamamaktadır. Bu noktada Sözleşme gelişmekte ve az gelişmiş olan devletler için tasarlanmamıştır[282]. Neticede teknik bakımından düşük kapasiteli devletler siber suçlulara güvenli sığınak olabilmektedirler.[283] Sözleşme için dile getirilen diğer bir eleştiri, üçüncü bölümde detaylı bir şekilde üzerinde durulacağı üzere, siber suçlarla ilgili ulusal sınırlar dışı yargı sorununa etkin bir çözüm getirememesidir[284].

Bu eleştirilere rağmen, siber suç Sözleşmesi şimdiye kadar imzalanan en önemli ilk uluslararası sözleşmedir. Sözleşme'den sonra siber suçlarla ilgili yapılan her türlü çalışmalar için temel bir metin teşkil etmektir. Ayrıca sınır aşan siber suçlarla mücadelede devletler arası işbirliği ve adli yardımlaşmaya zemin hazırlamasında, önemli bir adım olup küresel düzeyde bu tür suçlarla mücadelede referans olarak kabul edilmektedir.

2.2.1.2. Avrupa Birliği

1957 yılında Roma Anlaşması'yla kurulan Avrupa Ekonomik Topluluğu, daha sonra 1992'de Maastricht Antlaşması'yla Avrupa Birliği'ne dönüşmüştür. Bünyesinde

[279] Marco Gercke, "Siber Suç Sözleşmesi İle 10 Yıl: Avrupa Konseyi'nin İnternet Bağlantılı Suçlara Karşı Mücadele Belgesinin Başarları ve Kusurları", **İnternet Hukuku**, Ed. Yener Ünver, Ankara, seçkin, 2013, s. 109
[280] Weber, **a.g.m.**, s. 442.
[281] Sınar, **a.g.m.**, s. 778.
[282] Gercke, **a.g.m.**, 113
[283] Nain, Donaghy, Goodman, **a.g.m.**, s. 205-206.
[284] Weber, **a.g.m.**, s. 443-444.

28 üye devlet bulunan Avrupa Birliği, ekonomik, siyasal, kültürel sosyal v.s. alanlarda faaliyetler yürütmektedir[285]. AB siber suçlarla mücadele doğrultusunda girişimleri bilgi toplumuyla birlikte gelişmektedir. Bilişim teknolojilerinden faydalanmak için 1999 yılında Avrupa Komisyonu tarafından ortaya atılan E-Europe girişimi ile, bilgi toplumuna geçişe yönelik önemli bir adım atılmıştır. Ardından 2000'de Avrupa Konseyi ağ güvenliği ve siber suçlarla mücadele konularının göze çarpmasını vurgulayan bir E-Europe eylem planı izlenmiştir[286]. 2001'de Avrupa Komisyonu, siber suç sorununu analiz eden ve bu tür suçlarla mücadele için etkin araçların ihtiyaç olduğunu vurgulayan "Bilgi Altyapılarının Güvenliğini Artırarak ve Bilgisayarla İlgili Suçla Mücadele Ederek Daha Güvenli Bir Bilgi Toplumu Yaratmak" başlıklı bir iletişim yayınlamıştır[287].

Uzun tartışmalı bir müzakere ve koordinasyon sürecinin sonucunda, AB tarafında 2013 yalında AB siber güvenliğinin temelini oluşturan AB Siber Güvenlik Stratejisi kabul edilmiştir[288]. AB'de siber güvenliğini güçlendirmeyi amaçlayan işbu strateji, beş prensip getirmektedir. Bunlar: siber alanda esnekliğin gerçekleştirilmesi, siber suçların büyük ölçüde önlemesi, siber güvelikle ilgili ortak savunma politikaları ve kapasitelerinin geliştirilmesi, siber güvenlikle ilgili endüstriyel ve teknolojik kaynakların geliştirilmesi ve AB için tutarlı bir uluslararası siber politika oluşturmak ve temel AB değerlerini teşvik etmektir[289].

AB, siber güvenliği korumak ve bu konuda koordinasyon sağlamak amacıyla Avrupa Birliği Ağ ve Bilgi Güvenliği Ajansı'nı (European Union Agency for Network and Information Security ENISA) kurmuştur. ENISA, üye devletlerin kritik altyapı kontrol sistemlerinin korunmasında etkin rol oynamaktadır[290]. Öte yandan, özellikle

[285] Broadhurst, **a.g.m.**, s. 425; Ünver, Canbay, Mirzaoğlu, **a.g.e.**, s. 19.
[286] Christou, **a.g.e.**, s. 90.
[287] Marco Gercke, "Europe's Legal Approaches to Cybercrime", **ERA Forum**, Vol.10No.3, 2009, s. 411.
[288] László Kovács "Cyber Security Policy and Strategy in the European Union and Nato", **Land Forces Academy Review**, Vol. 23, No 1, 2018, s. 17.
[289] European Commission, Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace, Brussels, 2013, s. 4-5.
[290] Bkz: Mehmet Eren , "Avrupa Birliği'nin Siber Güvenlik Stratejisi İçin Kuramsal Çerçeve Ve Strateji Belgesi Öncesi AB'nin Eylemleri", **Cyberpolitik Journal**, Vol. 2, No. 3, 2017, s. 42-43.

organize suçlar ve siber suçlarla mücadele etmek ve bu suçları tespit etmek konusunda üye devletlerin polis teşkilatlarının arasında işbirliği ve koordinasyon sağlamak için Avrupa Polis Teşkilatı (Europol) etkin bir rol oynamaktadır[291]. Europol'ün içinde söz konusu bu amaçları gerçekleştirmek amacıyla Yüksek Teknolojili Suçlar Merkezi (High Tech Crime Centre) EC3 kurulmuştur. Bu kurum dolandırıcılık gibi örgütler tarafından işlenen siber suçlar, internet üzerinden çocuk istismarı suçları ve kritik altı yapılara gerçekleştirilen saldırı suçları üzerinde görev yapmaktadır[292]. Ayrıca siber AB içinde işbirliğini güçlendirmek ve gelişen siber suçlarla mücadele yöntemlerini teknolojik bakımından geliştirmek için Avrupa siber suç gücü (European Cybercrime Task Force) kurulmuştur[293].

AB'nin üye devletlerin ceza yasalarını uyumlu hale getirmek için düzenlemeler yapma yetkisi bulunmaktadır. Özelikle 2009'de Lizbon Antlaşmasının yürürlüğe girmesiyle birlikte söz konusu yetki daha da genişletilmektedir[294]. Zira AB'nin İşleyişine İlişkin Antlaşma 83. Maddesindeki yer alan terörizm ve insan ticareti gibi sınır aşan suçların yanında düzenlenmiş olup AB tarafından on suçu "Eurocrimes" kapsamına dahil edilmiştir[295]. AB tarafından siber suçlarla etkin bir mücadele sağlamak için birçok çerçeve karar ve direktif suretiyle düzenlemeler yapılmıştır.

2.2.1.2.1.Siber Suça ilişkin Avrupa Birliği Çerçeve Kararları

AB Konseyi tarafından 2004 yılında internet üzerinden çocuk istismarı ve pornografisini önlemek üzere bir çerçeve kararı kabul edilmiştir[296]. Kararın temel amacı çocuk pornografisi suçlarıyla mücadelede üye devletlerin ilgili teşkilatları

[291] Özüdoğru, **a.g.m.**, s. 58; Broadhurst, **a.g.m.**, s. 425; George, **a.g.e.**, s. 88.
[292] George Christou, "The Challenges of Cybercrime Governance in the European Union", **European Politics and Society,** Vol. 19, No. 3, 2018, s. 363.
[293] Aliusta, Benzer, **a.g.m.**, s. 37.
[294] Gercke, **a.g.e.**, s. 139; Oerlemans, **a.g.e.**, s. 61.
[295] Laviero Buono, "Fighting cybercrime between legal challenges and practical difficulties: EU and national approaches", **ERA Forum**, Vol, 17, No.3, 2016, s. 344.
[295] Council Framework Decision (2004/68/JHA) on combating the sexual exploitation of children and child pornography.
[296] Council Framework Decision (2004/68/JHA) on combating the sexual exploitation of children and child pornography.

arasında işbirliği sağlanmasıdır.[297] Kararda üye devletlerin çocuk pornografisi konusunda ceza yasalarının uyumlu hale getirilmesi için asgari standartlar belirtilmiştir[298].

2005 yılında AB Konseyi tarafından bilgi ve iletişim sistemlerine karşı saldırılara ilişkin alınan çerçeve kararında bilişim sistemlerine gerçekleştirilen saldırıların ceza yargılanmaları hakkında üye devletler arasında işbirliği amaçlanmıştır[299]. Avrupa Konseyi Siber Suç Sözleşmesi'ne uyumlu olan bu Kararda üye devletler arasında uzlaşma sağlanması gereken üç siber saldırı belirlenmiştir. Bunlar: yasa dışı bilgi ve iletişim sistemlerine erişim, bilgi ve iletişim sistemlerine müdahale ve verilere yasa dışı müdahaledir[300]. Ayrıca kararın 11. maddesinde devletler arasında söz konusu saldırılarla ilgili bilgi paylaşımı kolaylaştırılarak 7/24 operasyonel iletişim noktası kurulması zorunlu kılınmıştır. Üye devletlerin bu saldırıları gerçekleştiren kişilere makul caydırıcı para cezası içeren düzenlemeler yapmalarının zorunlu olduğu belirlenmiştir[301].

2002 yılında terörizme dair kabul edilen çerçeve kararı AB'nin terörle mücadele politikasının temelini teşkil etmektedir[302]. Özellikle üzerinde tartışılan terör suçlarının tanımı üye devletler arasında yeknesak hale getirilmesi ve terörle mücadele politikasının temel insan hakları ve hukukun üstünlüğü çerçevesinde gerçekleştirilmesi gerektiği belirlenmiştir[303]. Ancak söz konusu karar internet üzerinden yapılan terör eylemleriyle ilgili hükümler içermemiştir. Dolayısıyla bu kararın boşlukları doldurulmak için 2008'de tadil edilmiştir.[304] Kararın 4. maddesine göre internet, terör eylemlerine bireyleri teşvik etmek için ve terör eylemlerinin

---

[297] Nadina Foggetti, "Transnation Cyber Crime, Differences Between National Laws and Development of European Legislation: By Repression", **Masaryk University Journal of Law and Technology**, Vol. 2, No. 2, 2008, s. 33.
[298] George, **a.g.e.**, s. 93.
[299] Bkz: Council Framework Decision (2005/222/JHA) on Attacks Against Information Systems.
[300] Christou, **a.g.e**., s.93; Ulrich Sieber "Instruments of international law: against terrorist use of the Internet", **A War on Terror?**, New York, Springer, 2010, s. 177.
[301] Mehmet Eren, **Avrupa Birliği'nin Siber Güvenlik Politikası**, İstanbul, Beta Yayınları, 2017, s. 76.
[302] Council Framework Decision (2002/475/JHA) on Combating Terrorism.
[303] Cristos Velasco, "Cybercrime jurisdiction: past, present and future", **ERA Forum,** Vol. 16., No. 3. 2015, s. 339.
[304] Gercke, **a.g.e.**, s. 143.

yöntemleri ve araçları hakkında bilgi almak +için "Sanal eğitim kampı" olarak kullanılmaktadır[305].

2.2.1.2.2.Siber Suça İlişkin Avrupa Birliği Direktifleri

AB 1995 yılında 95/46 sayılı Veri Korunması Direktifinde bireylerin kişisel verilerinin işlenmesi sürecinde hak ve özgürlüklerinin korunması amaçlanmıştır. Nitekim direktifte işleme tabi tutulan kişisel verilerin üye devletler içerisinde serbestçe dolaşımını sağlamak üzere uygulanması gereken hükümler koyulmuştur. Bu direktifin tamamlayıcı niteliğine sahip olan 2002/58 sayılı Elektronik Haberleşme Sektöründe Gizliliğin Korunması Direktifi, gelişen teknoloji karşısında elektronik iletişimde bireylerin hak ve özgürlüklerin yanı sıra özel hayatın gizliliğini ve şahsi verilerin korunmasını amaçlamıştır[306]. Keza 95/46 sayılı direktifte bulunan ve bu tamamlayıcı direktifte bulanmayan hükümlerin geçerli olduğu belirlenmiştir[307].

AB 2016'da 95/46 sayılı direktifi iptal edilmiş ve bunun yerine işlenen kişisel verilerin korunması ve üye devletler arasında serbestçe dolaşımına ilişkin 679 sayılı yeni yasa düzenlemesi kabul edilmiştir[308]. Ancak birlikte 2002/58 sayılı direktifin hükümleri geçerli sayılmıştır. Kişisel verilerin korunmasıyla ilgili daha belirleyici ve detaylı kurallar koyan, verilerin özel kategorilerini (Kritik veriler) ele alan yeni direktif, verilerin korumasına ilişkin üye devletlerde doğrudan uygulanabilecek ortak standartlar gelişmektedir[309]. Keza kişisel verilerin tanımı, anonim veriler ve verileri silme hakkı gibi üzerinde tartışılan sorunlara çözüm gerdirmektedir. Dolayısıyla kamu

[305] Council Framework Decision 2008/919/JHA of Amending Framework Decision 2002/475/JHA on Combating Terrorism.
[306] Directive (2002/58/EC), Concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector (Directive on Privacy and Electronic Communications).
[307] Eren, **a.g.m.**, s. 43.44.
[308] Bkz: Arnold Roosendaal, v.d., "Data Protection Law Compliance for Cybercrime and Cyberterrorism Research" **Combatting Cybercrime and Cyberterrorism Challenges, Trends and Priorities**, Ed., Babak Akhgar , Ben Brewster, Switzerland, Springer, 2016, s. 87-88.
[309] Regulation (EU: 2016/679) on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation).

ve özel sektörler için kişisel veriler konusunda temel bir referans kaynağı olarak kabul edilmektedir[310].

AB, 2006'da verilerin saklanmasına ilişkin direktifte 2002/58 sayılı direktifte değişiklik yapmıştır[311]. siber suçluların yerlerinin tespit edilmesi ve kavuşturulmasını sağlamayı amaçlayan Direktifte, internet ve iletişim hizmeti sağlayıcılarının veri saklamasına ilişkin hükümleriyle ilgili üye devletlerin yasal düzenlemeleri uyumlu hale getirilmesi zorunlu kılınmıştır.[312] Bu bağlamda direktifin 6. maddesi uyarınca iletişim ve internet hizmeti sağlayıcıları, verileri 6 aydan az ve 2 yıldan fazla olmamak şartıyla verileri saklama hükmüyle bağlanmıştır. Fakat tartışmalara neden olan bu direktife itiraz edilmiş ve Avrupa Adalet Mahkemesi tarafından 2014'te iptal edilmiştir[313].

AB 2004/68/JHA sayılı çocuk pornografi ve internet üzerinden çocuk istismarına ilişkin çerçeve kararı, 2011/92/EU sayılı yeni direktifiyle değiştirilmiştir[314]. Lizbon Antlaşması onaylandıktan sonra siber pornografi suçlarıyla ilgili ortaya konulan ilk söz konusu direktifte bilişim teknolojileri aracılığıyla çocuk istismarı ve çocuk pornografisi suçlarının kolaylıkla işlenebilir olduğu belirlenmiştir. Dosyalısıyla direktif, bu suçlarla mücadele etmek için uluslararası standartlar kabul etmiştir[315]. Zira direktifin 25. maddesinde üye devletlerin çocuk pornografisi içeren

---

[310] Ariadna Ripoll Servent, "Protecting or Processing? Recasting EU Data Protection Norms", Privacy, **Data Protection and Cybersecurity in Europ,** Ed. Wolf J. Schünemann, Max-Otto Baumann, Switzerland, Springer International Publishing, 2017, s. 120-121.

[311] Directive (2006/24/EC) on the Retention of Data Generated or Processed in Connection with the Provision of Publicly Available Electronic Communications Services or of Public Communications Networks and Amending Directive (2002/58/EC).

[312] Foggetti, **a.g.m.**, s. 33.

[313] Avrupa Adalet Mahkemesinin kararına göre direktifte yer alan kişisel verilerin korunma prosedürleri siber suçluların tespit edilmesi ve yargılanmasını amaçlamaktadır. Fakat söz konusu prosedürler AB Antlaşmasında öngörülen temel insan hakları olan özel yaşama saygı ve kişisel verilerin korunması için ciddi ihlal teşkil etmektedir. Ayrıca orantılılık ilkesiyle ötüşmemektedir. Dolayısıyla söz konusu direktif geçersiz sayılmıştır. bkz: Court of Justice of the European Union, Judgment of the Court (Grand Chamber), 8 April 2014, Joined Cases C-293/12 and C-594/12 Digital Rights Ireland and Others.

[314] Directive 2011/92/EU of the European Parliament and of the Council on Combating the Sexual Abuse and Sexual Exploitation of Children and Child Pornography, and Replacing Council Framework Decision 2004/68/JHA.

[315] Gercke, **a.g.e.**, 144.

web sitelerini ortadan kaldırmak için gerekli tüm tedbirler alması zorunlu kılınmıştır. Üye devletler, ayrıca söz konusu sitelere erişimi belli şartlarda engelleyebilir.

AB 2013 yılında düzenlenen bilgi sistemlerine karşı saldırılara ilişkin büyük önem taşıyan direktifi, 2005/222/JHA sayılı çerçeve kararının yerini almıştır[316]. Direktifin temel amacı bilgi sistemlere karşı yapılan saldırılar konusunda üye devletlerin yasalarında koordinasyon ve bu saldırılarla mücadelede devletler arasında işbirliği sağlamaktır[317]. Siber suçlarla mücadeleye daha önem veren işbu direktifte, yasa dışı müdahale (6.madde) ve siber suç işlemek için kullanılan araçların üretimi, satışı, kullanımı, ithalatı, dağıtımı veya başka bir şekilde kullanılabilir hale getirilmesi (7.made) suç olarak sayılmış olup bilgi sistemlere karşı saldırı suçlarına daha sert yaptırımlar koyulmuştur. Direktif hükümlerine göre üye devletler arasında yapılabilecek acil bilgi talebelerine maksimum olarak 8 saat içinde yanıt verilmesi gerekmekte ve 7/ 24 iletişim noktası kurulması zorunlu kılmıştır[318].

Yeni direktifin getirdiği en önemli husus siber suçlara yeni özellikler eklemesidir. Buna göre bilgi sistemlere yetkisiz erişimin suç olarak sayılması için güvenlik tedbirleri ihlal edilmesi temel şartı haline getirilmiştir. Dolayısıyla söz konusu bu şart direktifin temel hedeflerine engel olabilmektedir. Ayrıca bilişim sistemleriyle ilgili suçluları cezaya tabi tutulması için ihlal edilmesi gereken güvenlik tedbirinin tanımı yapılmamıştır[319].

---

[316] Adrian Haase , "Harmonizing Substantive Cybercrime Law through European Union Directive 2013/40/EU – From European Legislation to International Model Law?", **2015 First International Conference on Anti-Cybercrime (ICACC)**, 2015, S. 1-6-, s. 1-2.

[317] Directive 2013/40/EU of the European Parliament and of the Council, on Attacks Against Information Systems and Replacing Council Framework Decision 2005/222/JHA.

[318] European Parliamant, Dirctorate General for Internal Policies, Policy Deparment C: Citizens' Right and Constitutional Affairs Civil Liberties, Justice and Home Affairs, The law enforcement challenges of cybercrime: are we really playing catch-up ?, 2015, s. 31.

[319] Bkz: Pedro Miguel F. Freitas, Nuno Gonçalves, "Illegal access to information systems and the Directive 2013/40/EU" **International Review of Law, Computers ands Technology**, Vol. 29, No.1, 2015, s. 59.

2.2.2. Siber Suçla Mücadelede Arap Devletlerinin Girişimleri

Siber suçlar Arap bölgesinde de yaygın bir şekilde ortaya çıkmıştır. Ancak bu devletlerde siber suçlarla mücadele daha güçtür. Bunun nedeni bu devletlerde siber suçlalar ilgili etkili yasaların olmamasının yanı sıra mevcut yasaların çoğu elektronik ticaretle ilgili suçlara odaklamaktadır. Dolayısıyla diğer siber suçlarla mücadelede eksikler bulunmaktadır[320]. Buna rağmen, Arap devletleri son zamanlarda bu konuya büyük önem vererek önemli girişimlerde bulunmaktadırlar. Söz konusu bu girişimleri, Birleşik Arap Emirlikleri'nin bilgi teknolojisi suçlarıyla ilgili mücadelede yol gösterici yasası, siber suçlara ilişkin 2010 Arap Sözleşmesi ve Körfez Arap Ülkeleri İşbirliği Konseyi bilgi teknoloji suçlarıyla mücadelede yeknesak kanun için Riyad Antlaşması'dır.

2.2.2.1.Birleşik Arap Emirlikleri Bilgi Teknolojisi Suçlarıyla Mücadelede Model (Yol Gösterici) Kanunu

2003 yılında Arap Ligi kapsamında Arap Adalet Baklanları Konseyi[321] ve İçişler Bakanları Konseyi[322] tarafından Birleşik Arap Emirlikleri'nde Bilgi Teknolojisi Suçlarıyla Mücadelede Model Kanunu kabul edilmiştir. Siber suçlara ilişkin temel kuralları ortaya çıkaran bu kanunu, Arap yasa koyucusunun bu tür suçlarla ilgili gerek ceza hukukta düzenlemeleri gerekse ayrı bir düzenleme tahsis etmesinde yol göstermektedir. Kanuna bu şekilde adlandırılmasının nedeni Birleşik Arap Emirlikleri tarafından tavsiye edilmesidir.

Söz konusu model kanun 27 maddeden oluşmaktadır. Yasanın içerdiği en önemli suçlar: bilgisayar programlarının kopyalanması, bilişim sisteminde veya başka bir şekilde depolanan verilerin veya belgelerin sahteciliği, bilişim teknolojileri

[320] Muna Eleşker Cbur, **El-sibraniye Hacis el-Asır**, Beirut, El-mekez El-Arabi li-albuhus el-kanunniye ve el- Kazaye, Cami'at el- düvel El arabiye, 2016, s. 111.
[321] Arap Adalet Baklanları Konseyi, 19/ 495/2003 numaralı kararı.
[322] Arap İçişler Baklanları Konseyi, 21/417/2004 numaralı kararı.

aracılığıyla para akalam (siber- aklama), bilişim sistemlerine yetkisi erişim ve bilgi hırsızlığıdır. Burada en önemli husus kanunun herhangi bir cezaya yer vermemesidir. Cezaları belirleme konusunda üye devletlerin kendi kültürel, siyasal ve sosyal yapısına göre karar vermektedir. Bu noktada yasa koyucu isabetli olduğu düşülmektedir[323].

Model kanunu siber suçlarla mücadelede önemli ve etkili bir adım olarak kabul edilmektedir. Yasanın getirdiği kapsayıcılık sayesinde Arap Ligi'ne üye devletlerin siber suçlarla mücadele eden bir yasa çıkarmasını ve mevcut olan ceza yasların güncelleştirmesini sağlamaktadır. Yani üye devletlerin ceza yasalarını reform etmekte oldukça önemli bir kaynaktır. Ayrıca Bilgi Teknolojisi Suçlarına İlişkin 2010 Arap Sözleşmesi'ne devletlerin katılımın yolunu açmaktadır.

2.2.2.2. Bilgi Teknolojisi Suçlarına İlişkin 2010 Arap Sözleşmesi (Arap Birliği)

Siber suçlarla mücadele kapsamında Arap Ligi'nin 2010 yılındaki sözleşmeden önce birçok çalışmaları bulunmaktadır. 1998 yılında Tunus'ta yapılan kongrede birçok tavsiye kararı alınmıştır. Tavsiyelerde üye devletlerin bilgisayar ve internet kullanımıyla ilgili çalışmalar yapmak, gereken güvenlik tedbirlerini almak ve ceza düzenlemeler yapmak üzere bir komite kurmalarına davet edilmiştir. Ayrıca üye devletlerin siber suçlarla mücadele ve bunula ilgili yeni ortaya çıkan gelişmeleri takip etmek için özel birimler oluşturmasının önemli olduğu belirtilmiştir[324].

2010 yılında Arap Birliği tarafından imzalanan Bilgi Teknolojisi Suçlarına İlişkin Arap Sözleşmesi ise Arap devletleri düzeyinde en önemli sözleşme olarak kabul edilmektedir. Sözleşmenin temel amacı 1. maddesinde belirlendiği gibi söz konusu siber suçlara karşı yeknesak ceza bir strateji benimsemek suretiyle Arap toplumunun

---

[323] Model kanunuun tam metni için bkz: https://carjj.org/sites/default/files/qnwn_lmrt_lrby_lstrshdy_lmkfh_jrym_tqny_lmlwmt.pdf. Erişim Tarihi, 11.12.2019.

[324] Abdulkerim Alredaide, **El ceraim el Müstahdese ve İstiratijiyet Müvacehetiha**, Umman, Dar ve Mektebet Hamid li Neşir ve el Tavzii, 2013, s. 257.

güvenliği ve menfaatinin bu tür suçlardan korunması ve bu suçlarla mücadelede Arap devletler arasında işbirliği sağlanmasıdır. Nitekim temel amaç insan haklarının korunması ve insan haklarına saygı duyulmasının sağlanmasıdır[325].

Söz konusu Arap sözleşmesi 43 maddeden ve 5 ana bölümden oluşmaktadır. Birinci bölümde genel hükümler ve siber suçlarla ilgili terimlerin tanımlarına (bilgi teknolojisi, hizmet sağlayıcı, veri, program v.s.) yer verilmektedir. İkinci bölümünde maddi hukuk yer almaktadır. Bu bağlamda üye devletlerin siber suç olarak düzenlenmesi gereken eylemler tanımlanmaktadır[326]. Üçüncü bölüm usul hukukuyla ilgili usul hükümlerin uygulanması, bilişim sisteminde depolanan verilerin hızlı bir şekilde korunması, kullanıcının verilerinin acil toplanması, depolanan verilerin aranması veya el konması hükümleri içermektedir. Dördüncü bölümde Arap devletleri arasında adli ve yasal işbirliği, karşılıklı yardımlaşma ve suçluların teslim edilmesine ilişkin hükümler yer almaktadır. Beşinci bölüm ise ve sözleşmenin yürüklüğe girmesi ve kapanışla ilgili hükümler içermektedir.

Sözleşme Arap bölgesinin özelliğini dikkate alarak her devletin kamu düzenine, ahlak ve dini ilkeleri özellikle İslami şeriatına göre uygun bir şekilde düzenlenmiştir. Bu durum Sözleşme'nin 12. maddesinde somutlaştırıldığı görülmektedir. Söz konusu bu madde uyarınca pornografiyle ilgili içeriğin internet veya diğer ağları aracılığıyla satın alınması, üretilmesi, dağıtılması ve görüntülenmesi gibi eylemler yasaklanmıştır. Hüküm gerek çocuk pornografisi gerekse diğer her türlü pornografi için geçerlidir. Burada çocuk pornografisi suçları için daha ağır cezalar öngörülmektedir. Avrupa Konseyi Siber Suç Sözleşmesi'nin maddi hükümlerine bakıldığında sadece çocuklarla ilgili pornografisinin yasak olduğu görülmektedir.

Adı geçen sözleşme çeşitli eleştirilere maruz kalmaktadır. Maddi hukuku bakımından en önemli eleştirilerden biri, Sözleşme'nin Avrupa Sözleşmesi'nin izlediği yolun aksine çok çeşitli suçları içermesidir. Bunu nedeni Avrupa bölesinde

[325] Talal Ebu Afiefe, **Usul İlmi el İcarm ve el İkap ve Ahir el Cühüd el Düveliye ve el Arabiye li Mükafehet el Cerime el Münezeme Aber el Vataniye**, Kudüs, Dar el Cündi li Neşir ve el Tavzii, 2013, s. 422.
[326] Bkz: bu çalışma, birinci bölüm, s. 32.

Avrupa Konseyi ve Avrupa Birliği gibi organizasyonlar, sözleşmeler dışında devletlerin yasalarına etkileyecek araçlara (yukarda açıklamaya çalıştığımız çerçeve kararlar ve diriktiler) sahiptir. Buna benzer araçlar Arap organizasyonların bünyesinde bulunmamaktadır[327].

Diğer yandan sözleşmede oldukça geniş terimlerin kullanılmasıdır. Örneğin, "Bilgi teknolojisi suçları" terimi net olmamasıyla birlikte çok kapsamlıdır. Aynı şekilde 9. ve 18. maddelerde çok geniş ve birçok farklı yorumlara yok açabilmektedir. Ayrıca Sözleşme 'de kullanıcının gizliliğini koruyacak normlar belirtilmemektedir[328].

Sözleşme'nin usul hukuku ise 30.-43. maddelerde Arap devletler arsında hukuki ve adli işbirliği düzenlenmektedir. Aslında Arap Sözleşmesi'nin usul hukuku Avrupa Sözleşmesi'nin adli yardımlaşma ve suçluların iadesine ilişkin hükümlerine çok büyük ölçüde benzemektedir.

2.2.2.3. Körfez Arap Ülkeleri İşbirliği Konseyi Bilgi Teknolojisi Suçlarıyla Mücadelede Yeknesak Yasa için Riyad Antlaşması

Körfez Arap devletlerin arasında işbirliği sağlamak üzer yapılan bir dizi düzenleme bağlamında Körfez Arap Ülkeleri İşbirliği Konseyi tarafından 2012 yılında Bahreyn'de düzenlenen oturmada Bilgi Teknolojisi Suçlarıyla Mücadelede Yeknesak Yasa için Riyad Antlaşması kabul edilmiştir. Söz gelimi yasa yol gösterici nitelikte olup Arap Körfez bölesinde bilişim teknolojilerinin kötü kullanımını önünü geçmeyi amaçlamaktadır[329].

39 maddeden oluşan bu yasada, bilişim sistemine yetkisiz erişim, verilere ve belgelere zarar verme, sahtecilik, verilerin müdahale edilmesi, silinmesi,

---

[327] Diya Yahya el Sadat, **Mebadi İstihdam el Hasib el Ali ve el İnternet ve Cühud Mükafehet el Ceraim el Naşie**, İskenderiye, Menşe el Mearif, 2012, s. 188.
[328] **A.e.**
[329] Bkz:Körfez Arap Ülkeleri İşbirliği Konseyi, "Bilgi Teknolojisi Suçlarıyla Mücadelede Yeknesak Yasa için Riyad Antlaşması", (Çevrimiçi), https://cutt.ly/jaYImom, Erişim Tarihi: 09.04.2020.

değiştirilmesi, nefret söylemi, internet üzerinden komar oynama ve pornografi, internet üzerinden uyuşturucu satma veya bununla ilgili propagandası suçları öngörülmektedir.

2.2.3. Siber Suçla Mücadelede Diğer Bölgesel Girişimler

2.2.3.1. İngiliz Milletler Topluluğu (Commonwealth of Nations)

İngiliz Milletler Topluluğu, üye devletlerin siber suçlara dair ulusal düzenlemeler geliştirmesinde destek olmak ve ulusal yasaları uyumlu hale getirmek amacıyla model mevzuatlar düzenlemektedir. 2002 yılında topluluğun sekreterliği tarafından (Model Law on Computer and Computer Related Crimes) Bilgisayar ve Bilgisayarla İlgili Suçlar Kanunu başlıklı model mevzuat kabul edilmiştir[330]. Söz konusu model mevzuat, Avrupa Konseyi Siber Suç Sözleşmesinde yer alan standartları göz önünde bulundurmakta ve her ülkenin diğer İngiliz Milletler Topluluğu ülkeleri ile uyumlu mevzuatı düzenlemek için kullanabileceği ortak ilkelere örnek olarak görülmektedir. Ayrıca kolluk kuvvetlerinin siber suçlarla mücadele edebilmesi kapsamında yeni araçlar geliştirmektedir[331] .

Amacı bilgisayar sistemlerinin bütünlüğünü ve gizliliğini, verilerin ulaşılabilirliğini ve doğruluğunu korumak, bu tür sistemlerin kötüye kullanımını önlemek ve elektronik delillerin kullanımını ve toplanmasını desteklemek olan söz konusu model kanunda ulusal ceza kanunlarında düzenlenmesi gereken suçlar olarak yetkisiz erişim, bilgisayara veya verilere yetkisiz müdahale, siber suç işlemek maksadıyla cihaz üretimi veya bulundurulması ve çocuk pornografisi suçları öngörülmektedir. Diğer yandan model kanunda bu suçların soruşturmasını kolaylaştırmak için üye devletler arasında yardımlaşamaya yönelik tavsiyeler düzenlenmiştir. Bu tavsiyelerle devletler arasında Commonwealth Devletleri arasında

[330] Stein Schjolberg , "The History of Global Harmonization on Cybercrime Legislation–The Road to Geneva", **Journal of International Commercial Law and Technology**, Vol.1, No.12, 2008, s. 14.
[331] Angers, **a.g.m.**, s. 41; Schjolberg, **a.g.e.**, s. 81.

cezai hususlarda uluslararası işbirliği Programında (Commonwealth Schemes for International Cooperation in Criminal Matters) bilgisayarda verileri saklama yükümlülüğü eklenmiştir[332].

Model kanun, Commonwealth devletlerinde önemli bir etki yaratmıştır. Milletler Topluluğu' unda Bahamalar, Saint Lucia, Gana ve Brezilya gibi bazı üye devletler model kanunu yol gösterici olarak görüp bu suçlara dair yasalar düzenlemek için girişimlerde bulunmaktadır. Aynı zamanda siber suçlarla ilgili yasası olmayan birçok üye devlet mevcuttur[333].

Commonwealth Model Yasası'nın temel amacı üye devletlerin siber suçlarla ilgili kanun taslağı hazırlama sürecindeki çabalarını minimuma indirmektir. Ancak bu üye devletlerin bu yasayı kabul etmek zorunda oldukları anlamına gelmemektedir. Üye devletler kendi şartlarına göre bu yasayı kabul edebilmekte veya hiç kabul etmemektedir. Yani bağlayıcı bir kanun söz konusu değildir[334].

Commonwealth Hukuk Bakanları tarafından 2011 yılında Sidney'de yapılan toplantıda üye devletlerin siber suça ilişkin yasalarının güncellemesinin acil bir gereklilik olduğu kabul edilmiştir. Ardından paydaşlarını bir araya getiren Commonwealth İnternet Yönetişim Forumu tarafından Commonwealth Siber Suç Girişimi'ni başlatılmıştır[335]. Üye devletlerin siber suçlarla mücadele konusunda yeteneklerini geliştirmeye çalışan söz konusu Commonwealth Siber Suç Girişimi, Interpol, Amerikan Devletleri Örgütü Avrupa Konseyi , İngiliz Milletler Topluluğu Telekomünikasyon Örgütü ve ITU dahil olmak üzere 35 uluslararası örgütü birleştirerek Commonwealth devletlerinde siber alanda oldukça disiplinli programlara katkıda bulunmaktadır[336]. Diğer yandan Commonwealth Genel Sekretaryası

---

[332] Fafinski, **a.g.e.**, s. 226.
[333] Xingan Li "International Actions against Cybercrime: Networking Legal Systems in the Networked Crime Scene" **Webology**, Vol. 4, No. 3, 2007, s. 3.
[334] Fafinski, **a.g.e.**, s. 227.
[335] Subhash Chandra Singh, "High-Tech and Computer Crimes: Global Challenges, Global Responses", **Contemporary Issues in International Law Environment, International Trade, Information Technology and Legal Education,** Ed. B.C. Nirmal, Rajnish Kumar Singh, New Delhi, Springer Singapore, 2018, s. 428.
[336] Gercke, **a.g.e.**, s. 149.

tarafından siber suçlarla mücadelede etkin araçlar geliştirmek ve bölgesel ve uluslararası kuruluşlarla işbirliği sağlamak üzere çok disiplinli uzmanlardan oluşan bir grup kurulmuştur[337].

2.2.3.2. Afrika Birliği (AU)

Her ne kadar Afrika devletleri, gelişmekte olan devletler kategorisinde yer alsa da, son yıllardan beri bilgi ve teknoloji alanında çok büyük bir gelişme kaydetmektedirler. Yeni istatistiklere göre Afrika'da internet kullanıcıları 2000 yılında 4,515 milyon kişiyken 2017 yılında 453,3 milyon kişiye yükseldiği görülmektedir. 2022 yalına kadar Afrika'da bir milyar kişi internet erişimine sahip olacaktır[338]. Bu durum yaklaşık olarak Afrika'nın nüfusunun yüzde 35,2'sinin internet kullandığını göstermektedir[339]. Afrika'da bazı ekonomiler[340], ekonomik faaliyetlerin yüksek derecede dijitalleşmesi dolayısıyla siber suçların hedefi olup 2017 yılında 3.5 milyar dolar değerinde kayba neden olmuştur[341]. Bu nedenle siber güvenlik istikrarıyla ilgili endişeler de artmakta olup, Afrika Kıtası'nda siber güvenlik ve siber suçlara ilişkin düzenlemelere ihtiyaç duyulmaktadır. Bunu farkına varan Afrika Birliği ve Afrika Ekonomik Komisyonu tarafından siber suçlarla ilgili düzenleme yapma çabaları sonucunda 2012 yılında siber güvenliğe ilişkin Afrika sözleşme taslağı ortaya koyulmuştur[342]. Teknik sorunlar, sözleşme taslağıyla ilgili endişeler ve bazı sivil toplum örgütlerinin taslağa karşı çıkmaları dolayısıyla sözleşmenin imzalama süreci

---

[337]Commonwealth Secretariat, "Report of the Commonwealth Working Group of Experts on Cybercrime", **Commonwealth Law Bulletin**, Vol.40, No. 3, 2014, s. 503.

[338] Nir Kshetri, "Cybercrime and Cybersecurity in Africa", **Journal of Global Information Technology Management,** Vol. 22, No. 2, 2019, s. 77.

[339] Uchenna Jerome Orji "The African Union Convention on Cybersecurity: A Regional Response Towards Cyber Stability?", **Masaryk University Journal of Law and Technology,** Vol. 12, No. 2, 2018, s. 92.

[340] Güney Afrikalıları'nın % 86'sı çevrimiçi bankacılık hizmetlerini kullanılmaktadır. Bu oran Orta Doğu'daki birçok ülkeden ve Türkiye'den daha yüksektir. bkz: Kshetri, **a.g.m.**, s. 78.

[341] Kshetri, **a.g.m.**, s. 77.

[342] Adam Palmer ,"Mutual Legal Assistance: Understanding the Challenges for Law Enforcement in Global Cybercrime Cases Issue Brief", **Center for Cyber and Homeland Security at Auburn University,** 2018,(Çevrimiçi), https://www.jstor.org/stable/resrep20738?seq=1#metadata_info_tab_contents, Erişim Tarihi: 12.02.2020, s.17.

uzamıştır. Ancak Sözleşme'nin taslağı Afrika Birliğine üye devletlerin başkanları tarafından gözden geçirildikten sonra 2014 yılında "Afrika Birliği Siber Güvenlik ve Kişisel Verilerin Korunmasına İlişkin Sözleşmesi" olarak kabul edilmiştir[343].

Söz konusu Sözleşme'nin temel amacı, kişisel verileri koruma, elektronik ticaret, siber güvenlik yönetimi ve siber suçlarla mücadeleyle ilgili üye devletlerin yasalarının uyumlu hale getirilmesidir. Nitekim Afrika'daki bilgi toplumu için hedefler tanımlanmakta ve üye devletlerde ve bölgesel ekonomik topluluklarda mevcut bilgi teknolojileriyle ilgili yasalarını güçlendirmeyi amaçlanmaktadır[344].

Sözleşme'de siber güvenliğin yönetimi ve siber suçlarla mücadele için cezalar ve maddi ve ulusal hükümler düzenlenirken "nötr teknoloji"[345] dili kullanılmaktadır. Diğer yandan sözleşme, üye devletlere siber güvenliğin istikrarını güçlendirmek maksadıyla bir takım önlemler ve uygulama yükümlülükleri getirmektedir. Söz konusu üye devletlerin alması gereken önlemler: ulusal bir siber güvenlik çerçevesi oluşturulması, siber güvenlik kültürünün teşvik edilmesi, ulusal siber güvenlik yönetim yapılarının oluşturulması, kritik bilgi altyapısının korunması, siber suç suçlarının ve usul tedbirlerinin oluşturulması, uluslararası işbirliğinin ve yasal uyumun teşvik edilmesidir[346]. Dolayısıyla Afrika Birliği Sözleşmesi siber suçlarla mücadele etmek için üye devletlerin maddi ve ceza usul kanunlarında düzenlemesini ve uluslararası işbirliği mekanizmaları kurmasını gerektirmesi nedeniyle Avrupa Konseyi Siber Suç Sözleşmesi'nin ötesine geçmektedir[347].

Afrika Birliği tarafından yapılan siber güvenlik ve siber suçlarla ilgili bu Sözleşme önemli bir gelişme söz konusudur. Ancak Afrika'da sözleşmenin uygulanmasını engelleyen çeşitli zorluluklar bulunmaktadır. Bu zorluklar, siber

---

[343] Orji, **a.g.m.**, s. 98.
[344] Bkz: African Union Convention on Cyber Security and Personal Data Protection, Preamble, s. 1-3.
[345] İngilizcede technology neutrality ya da technological neutrality terimi, İnternet, telekomünikasyon ve veri koruma ile ilgili düzenlemenin temel araçlarından biri olmakla birlikte kullanılan teknolojilerden bağımsız bir şekilde aynı düzenleyici ilkelerin uygulanması gerektiği anlamına gelmektedir. bkz: Winston J. Maxwell, Marc Bourreau, "Technology Neutrality in Internet, Telecoms and Data Protection Regulation", **Computer and Telecommunications Law Review**, Vol. 31, 2014, s. 1.
[346] Bkz: Orji, **a.g.m.**, s. 100- 109.
[347] Orji, **a.g.m.**, s. 99.

güvenlik politikaları geliştirecek ve uygulayacak personel uzman bakımından kapasitenin bulunmaması, siber suç kolluk kuvvetleri açısından kurumsal kapasitelerin gerekli düzeyde olmaması (örneğin bazı Afrika devletlerinde kolluk kuvvetleri hala siber suçları tespit etme kapasiteleri ve kaynakları bulunmamaktadır) ve Siber güvenlik girişimlerinin finansmanının yetersiz olmasıdır[348].

2.2.3.3.Amerikan Devletleri Örgütü (OAS)

Siber suçluluk konusu, ilk kez 1999 yılında Amerikan Devletleri Örgütü bünyesinde gerçekleştirilen üye devletlerin adalet bakanlarının ikinci toplantısında bu alanda çalışma grubu oluşturulmasıyla ele alınmıştır. İş bu çalışma grubu, üye devletlerin siber suçlara bakış açılarının farklılıklarına dikkat çeken bir rapor yayınlamıştır[349]. Keza siber suçlarla mücadele etmek için mevzuatlar ve prosedürler geliştirmek ve üye devletler arasında uyumlu hale getirmek için bir politika önermiştir. Buna ek olarak, üye devletlerin G7 Örgütü'nün yapmış olduğu 7/24 iletişim noktasına katılmalarını önermiştir[350].

2004 yılında OAS'in Güvenlik Komitesi (OAS Daimi Konseyi'nin bir parçası), OAS'e bağlı olan Terörizme Karşı Amerikan Komitesi (CICTE), Amerikan Devletler Arası Telekomünikasyon Komisyonu (CITEL) ve Siber Suç Alandaki Hükümet Uzmanları grupları (REMJA) tarafından hazırlanan "Siber Güvenliğe Tehditlerle Mücadelede Kapsamlı Amerikan Devletleri için Stratejisi: Siber Güvenlik Kültürü Yaratmak İçin Çok Boyutlu Bir Yaklaşım" adlı politikasını kabul etmiştir. Stratejinin temel amacı yarımkürede bir siber güvenlik kültürü oluşturmak için uluslararası ve çok disiplinli bir yaklaşım meydana getirmek, üye devletlerin Bilgisayar Güvenliği Olay Müdahale Ekipleri kurmalarını teşvik etmek üye devletler arasında işbirliği sağlamak

[348] Orji, **a.g.m.**, s. 119-120.
[349] Schjolberg, **a.g.m.**, s. 14.
[350] Nain, Donaghy, Goodman, **a.g.m.**, s. 211-112; Gercke, **a.g.e.**, s. 152.

ve Amerikalar Arası Uyarı, İzleme ve Uyarı Ağı'nın oluşturulmasında Terörizmle Mücadele Komitesi'nin desteklemektir[351].

OAS, birçok bölgesel ve uluslararası kuruluşlarla ortaklık kurarak siber güvenlikle ilgili atölye çalışmaları düzenlemektedir. En önemlisi 2005 yılında Madrid'de OAS, Avrupa Konseyi'yle birlikte siber suçlara ilişkin konferans düzenlenmiştir[352].

Siber suçlarla mücadele bölgesel düzeyde yapılan gerişimler yukardaki bahsedilenlerle sınırlı değildir. Buna ek olarak 2001 Bağımsız Devletler Topluluğu Bilgisayar Esaslı Bilgiye Karşı Saldırıyla Mücadele Hakkında İşbirliği Sözleşmesi, 2009 Şangay İşbirliği Örgütü Uluslararası Bilgi Güvenliği Alanında İşbirliği Anlaşması, 2009 Batı Afrika Devletleri Ekonomik Topluluğu Siber Suçla Mücadele Direktifi Taslağı, Bağımsız Devletler Topluluğu Bilgisayar ve Bilgisayarla İlişkili Suçlar Hakkında Model Kanun ve Doğu Afrika Topluluğu Hukuki Çerçeve Taslağı gibi oldukça önemli girişim bulunmaktadır[353].

Sonuç olarak bağlayıcı olan veya yumuşak (bağlayıcı olmayan) siber suçlara karşı yapılan tüm düzenlemelere ve girişimlere bakıldığında, uluslararası işbirliğine, devletlerin yaslarının yeknesaklaştırılmasına, siber suçlarla ilgili yargı yetkisine yoğunlaştığı görülmektedir. Diğer ifadeyle siber suçlarla mücadele etmek amacıyla yapılan bütün çalışmaların ortak noktaları şunlardır: siber suçlara karşı devletler arasında işbirliğinin ve koordinasyonun gerçekleştirilmesi ve güçlendirilmesi, devletlerin siber suçlara ilişkin ulusal maddi ve usul yasaların uyumlaştırılması suretiyle siber suçlara global kapsamlı bir mücadele sağlamak ve siber suçun ortaya çıkarabileceği yargı yetisi gibi sorunlara çözüm üretmektir. Dolayısıyla söz konusu

---

[351] Michael Portnoy, Seymour Goodman, **Global Initiatives to Secure Cyberspace An Emerging Landscape,** Ed. Michael Portnoy, Seymour Goodman, New York, Springer Science, 2009, s. 57.

[352] **A.e.**

[353]Bkz: Erdem, Özocak, **a.g.m.**, s. 162- 163; Adonis Palustre, David Croasdell, "The Role of Transnational Cooperation in Cybersecurity Law Enforcement**", Proceeding Softhe 52nd Hawaii International Conference on System Sciences,** 2019, s 5599- 5600; Sandy Gordon, "Regionalism and Cross-border Cooperation Against Crime and Terrorism in the Asia-Pacific", **Security Challenges**, Vol. 5, No.4, 2009; Schjolberg, Hubbard, **a.g.m.**, s. 7-10; Schjolberg, **a.g.m.**, s. 15-18.

konuların bu çalışmanın üçüncü bölümünde detaylı olarak üzerinde durulması uygun görülmektedir.

ÜÇÜNCÜ BÖLÜM

SİBER SUÇLA MÜCADELEDE KARŞILAŞILAN ZORLUKLAR VE ULUSLARARASI İŞBİRLİĞİ

3.1. Siber Suçla Mücadele Zorlukları

3.1.1. Siber Suçun Doğasından Kaynaklanan Zorluklar

Bilgi ve İletişim Teknolojisinin karmaşık doğası nedeniyle geleneksel cezalar adalet dünyasına aşina olmamaktadır. Bu suçların soruşturulması, kavuşturulması ve takip edilmesi için donanımlı profesyoneller gerekmektedir. Ayrıca profesyoneller teknoloji sektörünün hızlı gelişmeleriyle ile mümkün kılınan yeni teknikler ve yeni çalışmalara hazırlanmak için sürekli olarak yeniden eğitilmelidir[354].

Siber suçun soruşturulmasının ve kavuşturulmasının önüne geçen zorluklarından biri siber suçluların kimliklerinin anonim olmasıdır. Suçlular kullanılmasında herhangi bir kısıtlama bulunmayan bilişim sistemlerini kullanarak dünyanın dört bir yanına ulaşabilmektedirler[355]. Dolayısıyla siber uzayda suçluların tespit edilmesi çok zor olmakla birlikte bunların takip edilmesini sağlayan bir mekanizma da bulunmamaktadır. Siber suçlunun tespit edilmesi için IP adresleri aracılığıyla sağlanabilmektedir. Ancak suçluya ait gerçek adres bilgilere uluşmak her zaman mümkün olmamaktadır. Suçlu başka birine ait bilişim sistemi, internet kafedeki bulunan bilişimi ya da havaalanlarında, restoranlarda veya otellerde halka açık internet bağlantılarını kullanarak suç işleyebilmektedir[356]. Üstelik IP adresi tespit edilse de

---

[354] Francesco Calderoni, "The European legal framework on cybercrime: striving for an effective implementation", **Crime, Law and Social Change**, Vol. 54, No. 5, 2010, s. 341.

[355] Jonathan Clough, "Cybercrime", **Commonwealth Law Bulletin,** Vol. 37, No. 4, 2011, s. 673.

[356] 2009 yılında Hollanda'da bir çocuk "4chan.org" web sitesinde okuldaki sınıf arkadaşlarını öldüreceğini söylemiştir. Polis tarafından tespit edilen IP adres bilgileri takip edilmiştir. Olayda, şüpheli çocuk komşusunun internet bağlantısını kullanarak kolluk kuvvetlerini şüphelinin ikametgahı yerine komşusunun evine yönlendirmiştir. Kolluk kuvvetleri şüphelinin komşularının evine geldiğinde, komşular giriş kimlik bilgilerini yanında oturan bir çocukla paylaştıklarını belirtmiştir. Kolluk

suçlunun kimlik bilgilerinin hizmet sağlayıcıda açıklanmaması[357] veya gerçek bilgileri vermemesi sorunu ortaya çıkabilmektedir[358].

Kimlikleri gizlemek için TOR (The Onion Router)[359] veya Psiphon gibi farklı iletişim araçlar kullanılması da ayrı bir sorundur. Bu durum IP adresinin takip edilmesini imkânsız denecek kadar zorlaştırmaktadır[360]. Örneğin dünya çapında kötü yazılım üreten ve para kıtırı yöneten Avalanche platformu aksaklıktan kaçınmak ve kimliğini gizlemek için hızlı akı tekniği (fast-flux technique) kullanmıştır. Hızlı akı aracılığıyla botnetler vasıtasıyla IP'le ilgili verilerin bir veya birden fazla internete bağlı bilgisayardan bir sürü farklı bilgisayara hızlıca taşınması sağlanmaktadır. Böylece bilgisayarın hem IP adresinin kayıtlarını hem de IP adresini oluşturan servisleri değiştirmektedir[361].

Her ne kadar bir devletin siber suçlarla ilgili kanunları iyi olursa olsun siber suçlular tespit edilmediği sürece bu kanunlar uygulanmaz. Başka ifadeyle siber suçları ele alan yasaların boşlukta işlenmesi mümkün değildir. İş bu zorluğunun üstesinden gelebilmek için bilişim sistemlerinin kullanımında kullanıcının kimliğini tanıtması zorunlu kılınmalıdır. Ancak insan hakları savunanları bu durumun bireylerin gizlilik haklarını ihlal ettiği gerekçesiyle karşı çıkmaktadırlar[362].

Diğer bir zorluk siber suçlarla ilgili delillerin kolluk kuvvetleri tarafından elde edilmesi ve korunmasıdır. Gerçek siber suçlunun tespit edilmesi de failin işlediği

kuvvetleri çocuğun evinde arama gerçekleştirmiştir. Bunun sonucunda bahsi geçen tehdit suçunun çocuk tarafından işlendiğini kanıtlayan bir dosya tespit edilmiştir. Oerlemans, **a.g.e.**, s. 37.

[357] Emmanuel Femi Gbenga Ajayi, "Challenges to Enforcement of Cyber-Crimes Laws and Policy", **Journal of Internet and Information Systems**, Vol. 6, No.1, 2016, s. 4.

[358] R. E. Bell, "The Prosecution of Computer Crime", **Journal of Financial Crime**, Vol. 9, No. 4, s. 314.

[359] Roberta Liggett, vd, "The Dark Web as a Platform for Crime: An Exploration of Illicit Drug, Firearm, CSAM, and Cybercrime Markets", **The Palgrave Handbook of International Cybercrime and Cyberdeviance**, Ed., Thomas J. Holt, Adam M. Bossler, Switzerland, Palgrave Macmillan, 2020, s. 93-94.

[360] Ajayi, **a.g.m.**, s. 4.

[361] Palustre, Croasdell, **a.g.m.**, s. 5600.

[362] Ajayi, **a.g.m.**, s. 4.

suçun ayrıca kanıtlanması gerekmektedir[363]. Söz konusu bu suçları kanıtlayacak delilerin çeşitleri ve toplama yöntemleri klasik suçlara göre tamamen farklıdır. Genellikle siber alanda işlenen suçların insan organlarıyla fark etmek mümkün değildir[364]. Siber suçun işlendiği mahal bilişim sistemidir[365]. Bu nedenle suçun işlendiğine dair delileri bu sistemlerde aranmaktadır. Ancak bu maddi olmayan delillerin doğası geçici niteliğe sahip olup her anda tamamen ya da kısmen kaybolabilmektedir[366]. Aynı zamanda bu deliler kolayca değiştirilebilmekte veya kodifiye edilebilmektedir[367].

Ayrıca günümüzde siber suçun aracı olan bilişim sistemin depolanma kapasitesinin oldukça arttığı görülmektedir. Bir delil bulabilmek için yüz binlerce verilerin aranması gerekmektedir. Bazı durumlarda siber suçlarla ilgili veriler birçok devletlerde bulunan bilişim sistemlerde depolanmış olabilmektedir. Bu durum kolluk kuvvetleri için yeni bir zorluk teşkil etmekte ve aynı zamanda delillerin elde etme süreci de çok karmaşık hale getirmektedir[368]. Öte yandan verilerin şifrelenebilmektedir. Dolayısıyla verilerin şifresini çözemeden kolluk kuvvetlerinin okuması imkansız hale gelmektedir[369]. Daha ziyade Şifreleri çözebilmek için uzun zaman ayrılması gerekmektedir[370]. Dolayısıyla bu sanal alemde delilerin elde edebilmesi ve analiz edilebilmesi için adli bilişim konusunda yüksek seviyede bilgiye

---

[363] Siber suçların soruşturulması kapsamında dijital ortamda delileri elde etme, muhafaza etme ve analiz etme süreci "adli bilişim" olarak adlandırılmaktadır. bkz:Yusuf Başlar, "Adli Bilişim Sürecinde Karşılaşan Sorunlar ve Çözüm Önerileri", **TBBD**, S. 148, s. 49-50.

[364] Susan W. Brenner ,"Cybercrime Metrics: Old Wine, New Bottles?", **Virginia Journal of Law and Technology**, Vol. 9, No. 13, 2004, s. 11.

[365] Bkz: Yanbo Wu, vd, "Research on Investigation and Evidence Collection of Cybercrime Cases", Journal of Physics: Conference Series, Vol.1176, No. 4, 2019, s. 2-3.

[366] Shiuh-Jeng Wang, "Measures of Retaining Digital Evidence to Prosecute Computer-based Cyber-Crimes" , **Computer Standards & Interfaces**, Vol. 29, No. 2, 2007, s. 217,

[367] Kim-Kwang Raymond Choo, "Organised Crime groups in Cyberspace: a Typology", **Trends Organ Crim**, Vol.11, No. 3, 2008, s. 287; Singh, **a.g.m.**, s. 221.

[368] Peter Grabosky, "Requirements of Prosecution Services to Deal with Cyber Crime", **Crime Law Soc Change**, Vol.47, No. 4-5, 2007, s. 214; Brenner, **a.g.m.**, s. 11.

[369] Kolluk kuvvetleri siber suçlarla ilgili verilerin şifrelenme sorunu iki aşamada karşılaşmaktadır. İlki aktarılan verilerin şifrelemesi, diğeri ise bilgisayarda depolanan verilerin şifrelenmesidir. bkz: Oerlemans, **a.g.e.**, s. 46-51.

[370] Bell, **a.g.m.**, s. 313.

sahip ciddi bir bilişim uzmanlığı gerekmektedir. Devletlerin çoğu söz konusu bilişim uzmanlarına ve altyapılara sahip değildir[371].

Siber alanda delilerle ilgili diğer zorluk söz konusu bu deliler mahkeme tarafından usul hukukuna uygun olarak kabul edilmesidir. Bu tür delilere yargı makamlar tarafından itibar edilmemektedir. Mahkemeler genellikle suçun kanıtlanması için maddi deliller talep etmektedir. Çoğu zaman siber suçlara ilişkin maddi deliller sağlamak mümkün olamamaktadır[372]. Dolayısıyla bazı durumlarda siber suçluların yargılanması nerdeyse imkânsız kılınmıştır.

3.1.2. Hukuki Zorluklar

3.1.2.1. Ulusal Hukuk Düzeyinde Zorluklar

Ulusal ceza hukuku belirli bir bölgede kamusal değerlerin ve genelgelerin korunmasının aracıdır[373]. Bu kapsamda ulusal yasalar belli bir yargı alanda işlenen suçların düzenlenmesi, soruşturulması ve kavuşturulması için etkin bir şekilde gerçekleşebilmektedir. Suçun bir ülkede ikamet eden bir fail tarafından aynı ülkede bulunan bilişim sistemi aracılığıyla aynı ülkede bulunan diğer kişiye (mağdur) karşı işlenmesi halinde, sadece o ülkenin yargı makamlarının yetki alanına girmiş olacaktır[374]. Yani suçun tüm unsurları tek yargı alanda gerçekleştirilmiş olacaktır. Örneğin, bilişim sistemleri üzerinden kimlik hırsızlığı, dolandırıcılık, telif hakkı ihlalleri, çocuk pornografisi, zorbalık gibi suçlar[375]. Söz konusu suçların herhangi bir

[371]Art Ehuan, "Cybercrime and Law Enforcement Cooperation", **CyberForensic Understanding Information Security Investigations**, Ed. Jennifer Bayuk, Germany, Springer, 2010, s. 138.
[372] Ajayi, **a.g.m.**, s. 7.
[373] Perloff-Giles, **a.g.m**,. s. 204.
[374] Susan W. Brenner, "Cybercrime jurisdiction", **Crime, Law and Social Change,** Vol. 46, No. 4-5, 2006, s. 193-194.
[375] **A.m**., s. 204.

unsurunun ülkenin sınırları dışında gerçekleştirilebilmesi ulusal ceza hukuku hiçbir anlam ifade etmemektedir[376].

Buna karşılık siber suçların yargılanmasının en büyük problemi bu suçlara ilişkin ulusal mevzuatların yetersizliğidir. Daha pratik bir anlatımla bazı devletlerde bu suçlarla ilgili düzenlemeler bulunamamaktadır. BM'nin 201 üyelerinin (gözlemci ve sınırlı bir şekilde tamamlanan üyelerle birlikte) çoğu Avrupa ülkesi olmak üzere sadece 79'u siber suçlarla ilgili yasalara sahiptir[377]. Yani dünyadaki devletlerin sadece %40'ından daha azı siber suçları cezaya tabi tutmaktadır[378]. Bu durum siber suçlulara herhangi bir endişe duymadan suç işleme imkanı vermektedir. Özellikle Afrika kıtasında, 54 devletten sadece 4 devlet (Kamerun, Kenya, Güney Afrika ve Zambiya) bu tür yasalara sahiptir[379]. Ancak son yıllarda imzalanan Afrika Birliği Siber Güvenlik ve Kişisel Verilerin Korunmasına İlişkin Sözleşmesi'yle devletlerin siber suçlarla ilgili düzenlemeler yapması ve politikalar geliştirmesi zorunlu kılınmıştır[380].

Ceza kanunları temel prensipleri olan kanunilik ve kıyas yasağı gereğince suçların düzenlenmesi büyük önem taşımaktadır. Siber suçlara dair yasaların yokluğunu açıklayan en iyi örnek "Love Bug" virüsü olayıdır. Bilişim sistemlerdeki bulanan verileri ve şifreleri çalan bu virüs kısa bir süre içinde baş döndürücü bir hızla birçok ülkeye yayılmış 45 milyon kullanıcıya etkileyip yaklaşık 10 milyar dolar değerinde hasara neden olmuştur. Virüs uzmanları tarafından yapılan hızlı bir şekilde takip sonucunda virüsün Filipin'den kaynaklandığı tespit edilmiştir. Hizmet sağlayıcıların sunduğu bilgiler aracılığıyla FBI ve Filipin ulusal soruşturma mercileri tarafından virüsü üreten ve yayan şüpheli Filipin vatandaşı olan Onel de Guzman'ı tespit edilmiştir. Ancak siber suçları düzenleyen bir yasa olmadığı Filipin'de virüs üretilmesi veya yayılması suç sayılmaz. Dolayısıyla virüsün üretmesiyle veya

[376]Peter Csonka, "The Council of Europe's Convention on Cyber-crime and Other European Initiatives", **Revue İnternationale de Droit Penál** , Vol. 77, No. 3, 2006, s. 477.
[377] Irak'ta siber suçlara ilişkin hazırlanan yasa mecliste kabul görmemiştir. Dolayısıyla Irak'taki genel ceza düzenlemeleri uygulanmaktadır. Kawther Hazim Sultan, "Mekuf el Kanun ve el Kada'a min el Cerime El'elektroniye", **Mecelet Küliyet el terbiye el Esasiye**, C.XXII, S. 96, s. 993.
[378] Ajayi, **a.g.m.**, s. 9.
[379] Ajayi, **a.g.m.**, s. 9.
[380] Bkz: bu çalışmada Afrika Birliği girişimleri, s. 84.

yayılmasıyla ilgili deliler bulmak için kolluk kuvvetlerinin şüphelinin dairesini arama işlemlerini aksamıştır[381].

Şüpheli hakkında arama kararı alınması günler sürmüştür. Bu süre failin suçla ilgili tüm temel delileri ve verileri ortadan kaldırabilmesi için yeterlidir. Sonunda alınan arama kararı infaz edildikten sonra kolluk kuvvetleri eski bilgisayar mühendisliği öğrencisi olan şüpheli Guzman'nın "Love Bug" virüsünün ürettiği ve yaydığına dair deliler bulmuşlardır[382]. Filipin ulusal ceza kanunda bilişin sistemlerinde arama ve el koyma usullaeriyle ilgili bir düzenleme olmadığı ve virüs üretmek ve yaymak eylemleri suç sayılmadığı için şüpheli yargılanamaz. Ancak şüpheli yargılama yetkilileri tarafından virüsün amacının şifreleri veya verileri çalmak olması nedeniyle kredi kartı hırsızlığı ve dolandırıcılığı suçlarıyla suçlanmıştır. Ancak Filipin ulusal mahkemeleri tarafından bu suçları asılsız ve delilerin elverişli olmaması gerekçesiyle davaları ret edilmiştir. Sonuç olarak Filipin'de Guzman'ın yargılanması mümkün olmamıştır. Aynı zamanda bu eylem Filipin'de bir suç teşkil etmediği için Guzman siber suçlarla ilgili yasaların olduğu ABD veya virüsten etkilenen diğer devletlere iade edilemez. Ayrıca suçluların iadesi aşağıda açıklanacağı üzere karşılıklı antlaşmalar ve çifte cezalandırılabilirlik koşulu gerektirmektedir. Bu iki koşul Guzman davasında sağlanmış değildir[383]. Böylece suçlu olan Guzman cezasız kalmıştır.

Bu olaydan sonra dünyada siber suçları düzenlemek gerekliliğiyle ilgili büyük bir farkındalık oluşmuştur. Siber suçlarla ilgili yasaların olmadığı devletler siber suçlular için güvenli sığınak teşkil etmiş[384] olup sadece kendi güvenliği değil, tüm uluslararası toplumun güvenliğini tehdit eder bir hale gelmiştir. Dolaysıyla Filipin'de bu olaydan kısa bir süre sonra virüs üretmek veya yaymak gibi birçok siber suçu cezalandıran yasalar çıkarmıştır[385]. Bu noktada bu suçların ulusal ceza kanununda ya

[381] Susan W. Brenner , Bert-Jaap Koops, "Approaches to Cybercrime Jurisdiction", **Journal of High Technology Law,** Vol. 4, No. 1, 2004, s. 7.
[382] Goodman , Brenner, **a.g.m.**, s. 141; Brenner, Koops, **a.g.m.**, s. 7.
[383] Goodman , Brenner, **a.g.m.**, s. 141.
[384] Mücahid Özbek, "The Impacts of European Cybercrime Convention on Turkish Criminal Law", **GSI Articletter**, S. 13, 2015, s. 75.
[385] Andri Winjaya Laksana, "Cybercrime Comparison Under Criminal Law In Some Countries", **Jurnal Pembaharuan Hukum** Vol. 5, No. 2, 2018, s. 225; Goodman , Brenner, **a.g.m.**, s. 143.

da ayrı bir yasa olarak düzenlenmesi önem arz etmektedir. Ancak burada dikkat edilmesi gereken husus dünya genelinde üzerinde görüş birliği sağlanan gerek siber suçlar (bilişim sistemine yetkisiz giriş, verilerin yetkisiz bir şekilde ele geçilmesi, silinmesi, değiştirilmesi, nakledilmesi, bilişim sisteme veya verilere zarar verilmesi) gerekse bilişim sistemleri aracılığıyla geçekleştirilen (dolandırıcılık, hırsızlık gibi) klasik suçların kapsanmasıdır[386].

Siber suçların düzenlenmemesi sorununun yanı sıra mevcut siber suçlarla ilgili yasaları hükümlerin siber suçlulara caydırıcı[387] ve etkin olmadığını belirtmek gerekir. Maddi caza hukuk siber suçlara karşı etkin bir şekilde durabilmek için ön şarttır. Ancak sadece somut delileri arama ve el koyma kararların alınmasına izin veren eski usul hukuku (Love Bug davasında olduğu gibi) buna bir engel teşkil edebilmektedir. Dolayısıyla siber suçun doğasına uygun maddi olamayan delilerin elde edilmesine ve analiz edilmesine ilişkin hızlı prosedürler öngörülmesi gerekmektedir[388]. Aynı zamanda siber suçun sürekli ve hızlı gelişmesi ve yeni yöntemlerinin ortaya çıkması ceza yasalarının bu gelişmelere ayak uydurarak sürekli geliştirilmesini zorunlu kılmaktadır[389].

Son olarak belirtilmesi gerekir ki, bazı ülkelerde uluslararası düzeyde imzalanan antlaşmaların ulusal düzeyde geçerli hale getirilebilmesi için yasayla düzenlenmesi gerekmektedir. Çoğu zaman bu konu yasama organı tarafından ihmal edilmekte ve kanun düzenlenmesinde gecikme söz konusu olmaktadır. Dolayısıyla antlaşmaların ulusal bazda uygulanmasına bir engel teşkil edebilmekte veya antlaşmanın uygulanmasının gecikmesine yol açmaktadır[390].

---

[386] Dülger, **a.g.e.**, s. 256.
[387] Avustralya'daki ceza yasalar siber suçların cezaları çocuk pornografi dışında 1-3 yıl hapis cezasıyla, Birleşik Krallık'ta DOS saldırıları dışında en fazla 10 yıl hapis cezasıyla, Güney Afrika'nın yasası ise en fazla 5 yıl hapis cezasıyla cezalandırılmaktadır. bkz: Ajayi, **a.g.m.**, s. 9.
[388] Goodman , Brenner, **a.g.m.**, s. 143.
[389] Bkz: Gercke, **a.g.e.**, s. 86.
[390] Ajayi, **a.g.m.**, s. 10; Oerlemans**, a.g.e.**, s. 56.

3.1.2.2. Uluslararası Hukuk Düzeyinde Zorluklar

3.1.2.2.1. Yargı Yetkisi Zorluğu

Uluslararası hukukta yetki, devletin kişiler ve eşyalar üzerinde etkileme gücü veya tasarruf hakkı olarak tanımlanabilmektedir[391]. Bu anlamda yetki, yasama yetkisi (yasa öngörme yetkisi), yürütme yetkisi (yasa uygulama yetkisi) ve yargılama yetkisi (anlaşmazlıkları çözme yetkisi) olmak üzere üç temel kavramı kapsamaktadır[392]. Klasik olarak söz konusu bu üç yetki türleri temelde ülkesellik (mülkilik) prensibine dayanmaktadır. Ancak bazı durumlarda[393] bu prensip yetersiz kaldığı için kişilik prensibi, koruma prensibi veya evrensel yargı prensibi ülkesellik prensibinin tamamlayıcısıdır[394].

Ülkesellik prensibi uyarınca devletin yetkisi kendi coğrafi sınırları içeresinde bulunan kara, sular, hava ve uzay alanlarda uygulayabilmektedir[395]. Yani devlet bu alanlarda eylemin hangi suçun maddi unsurunu teşkil edip etmeyeceği konusunda karar verme, yetkili yargı makamları ve uygulanacak hukuku belirleme yetkisine sahiptir. Diğer anlatımla kanun infazı ve ceza adaleti egemen devletin temel taşlarındandır[396]. Dolayısıyla devletler bu yetkiyi değer bir devletlerin yetki alanında kullanamaz.

---

[391] Malcolm N. Shaw, **International Law**, 8.bs., England, Cambridge University Press, 2017, s. 645.
[392] Ikenga K.E. Oraegbunam, "Jurisdictional Challenges in Fighting Cybercrimes: Any Panacea From International Law?", **Nnamdi Azikiwe University Journal of International Law and Jurisprudence,** Vol. 6. 2015, s. 58-59.
[393] İstisnai olarak devlet kendi coğrafi sınırları dışında yargılama yetkisine sahip olabilmektedir. Öreğin, açık denizlerde işlenen suçlar, sahtecilik suçlar, vatandaşlar tarafından işlenen suçlar, savunma mensupları tarafından işlenen suçlar. sing, **a.g.m.,** s. 420.
[394] Mutlu Dinç Keçeligl, "Evrensel Yargı Yetkisi: Ceza Hukuku Bağlamında Evrensellik İlkesine Bakış" **Terazi Hukuk Dergisi,** C.XIII, S.143, 2018, s. 126; Jun Li, Jidong Jia, "Confusion and Relief of Criminal Jurisdiction of Cybercrimes" **Advances in Computer Science Research, Volume 65,** 2018 3rd International Conference on Communications, Information Management and Network Security (CIMNS 2018), Atlantis Press, 2018, s.51.
[395] Anders Henriksen, **International Law**, 2. bs., United Kingdom, Oxford Universty Press, 2019, s. 85.
[396] Brenner, **a.g.m.**, s. 6.

Söz konusu klasik yetki alanlarının kara, su, hava ve uzayda belli ve sabit sınırları bulunmaktadır. Bu alanlarda suç işlendiğinde nerede işlendiği ve sonuçta hangi devletin yetki alanına gireceğini belirtmek zor değildir. Ancak siber suçlar bu çalışmanın farklı yerlerinde ifade edildiği gibi sınır tanımayan ve herhangi devletin yetkisi altında olmayan siber uzayda işlenmektedir[397]. Bilişim ağlarına bağlı bir bilgisayar aracılığıyla evde oturan bir kimse tarafından dünyanın her bir yerinde suç gerçekleştirilebilmektedir. Bu durumda karşımıza uygulanacak hukuk ve yetkili mahkeme tayin etmek için suçun işlendiği yer sorunu ortaya çıkabilmektedir[398].

Siber suçların eylemlerinin yerini tespit etmek oldukça güçtür. Özellikle siber suçu oluşturan maddi unsuları her biri farklı devletlerde gerçekleştirilmesi durumunda yetki sorunu daha karmaşık hale gelmektedir[399]. Suçun hangi unsuruna göre (fail, mağdur, netice, nedensellik bağ v.s.) işlenmiş sayılacağı ve suçun nerede işlenmiş sayılacağı[400] ayrı bir sorundur[401]. Örneğin bilişim teknolojisi aracılığıyla nefret söylemi veya çocuk pornografisi gibi içerikle ilgili suçlarda maddi unsurun gerçekleştiği ve bilişim sistemin bulunduğu yeri tespit etme gibi zorluklarla karşılaşmaktadır. Ayrıca içerik bir yerde yüklenmeye başlar ve başka ülkede biter veya fail bir ülkedeyken içeriği oluşturmuş ve başka bir ülkede kamu erişimine sunmuş olabilmektedir[402]. Dayısıyla bir siber eylem birden çok ülkenin yetki alanına

---

[397] Li, Jia, **a.g.m.**, s. 51.
[398] Sing, **a.g.m.**, s. 419.
[399] David L. Speer, "Redefining Borders: The Challenges of Cybercrime", **Crime, Law and Social Change**, Vol. 34, No. 3, 2000, s. 260.
[400] Siber suçların işlendiği yerin tespit edilmesi bilişim sisteminin, hizmet sağlayıcının bulunduğu yer, verilerin geçtiği yer, veya düğmenin basıldığı yer gibi kriterlere göre gerçekleştirilebilmektedir. Bu durum ülkeye göre farklık göstermektedir. Öğrenin ABD ve bazı Avrupa ülkeleri hareketin gerçekleştiği yerde suçu işlenmiş olduğu yer olarak değerlendirilmektedir. bkz Özbek, **a.g.m.**, s. 117. Ancak Malezya ve Singapur ülkelerinde bilişim sistemin bulunduğu yeri suçun işlendiği kabul edilmektedir. Brenner, **a.g.m.**, s. 1 4-16.
[401] Yargı sorununa dikkat çeken davalardan biri Kuvvet'te bir bankada çalışan İngiliz programcının bankaya ait bilişim sisteminde manipülasyon yaparak büyük miktarda para müşteri hesaplarından kendine özel bir hesaba aktarmasıdır. İngiltere'ye dönen sanığın talebi üzerinde banka paranın İngiltere'deki hesabına aktarmıştır. İngiltere'deki kanuna göre dolandırıcılık yoluyla para kazanmak suçundan yarılanmış ve hapis cezasıyla mahkûm edilmiştir. Bu karara suçun unsurları Kuveyt'te gerçekleştirildiğinden dolayı İngiliz mahkemenin yargı yetkisi olmadığı gerekçesine dayanarak itiraz edilmiştir. Ancak suçun parayı talep edilmesiyle tamamlanmış olduğunu belirleten mahkeme itirazı ret etmiştir. Tarık İbrahi Eldusuky, **EL'emin Elmalumaty**, İskenderiye, Dar Elcamiaa Elarabiye, 2009, s. 603.
[402] Brenner, **a.g.m.**, s. 16.

girebilmektedir[403]. Bunun gibi sorunları çözebilecek uluslararası düzeyde bir makam veya bir mahkeme bulunmadığı için devletler kendi ulusal yasalarında yer alan yetki kurallarıyla bu sorunu çözmeye çalışmaktadırlar[404] .

Yetki sorunu Avrupa Konseyi Siber Suç Sözleşmesi'nin 22. maddesinde düzenlenmiştir. Sözleşme, siber suçların yetki kuralarını tesis ederken ülkesellik ve şahsilik olmak üzere iki prensibe dayanmaktadır [405]. Ancak bu durum aynı maddenin 4. Fıkrası uyarınca devletlerin yargı yetkisinin belirlenmesinde başka normları benimsemesine engel teşkil etmemektedir.

22. maddenin a,b,c fıkralarında yer alan ülkesellik prensibi uyarınca devletler kendi ülkesinde, bayrağını taşıyan gemisinde veya yasalarına göre kayıtlı uçakta işlenen suçlara ilişkin yetkiye sahiptir. Bu anlamda saldırıya maruz kalan bilişim sisteminin bulunduğu devlet, saldıran kişi başka devlette olsa bile yetkili olacaktır [406]. d. fıkrasında düzenlenen şahsilik prensibi ise devlet yetkili ülke sınırları dışında kendi vatandaşı tarafından başka bir ülkede suç olarak sayılan bir eylem işlenmesi veya herhangi bir devletin ülkesel yetki alana girmeyen bir alanda halinde yine yetkili olacaktır.

2. fıkra gereğince taraf devletlerin b,c,d fıkralarında yer alan yetki hükümlerini uygulama haklarını saklı tutabilmektedir. Pratik bakımından siber suçlar genellikle aynı anda birçok devlette etki yaratabilmektedir. Söz konusu bu koşul işlenen suçtan dolayı herhangi bir devletin yargı yetkisi talep etmemesine neden olabilmektedir. Dolayısıyla bu fıkrada işlenen suçtan etkilenen devletlerin, suçun kavuşturma önceliğe sahip devleti belirlemek amacıyla birbirine danışma yükümlülüğü öngörülmelidir [407].

---

[403] Albert I. Aldesco, "The Demise of Anonymity: A Constitutional Challenge to the Convention on Cybercrime", **Loyola of Los Angeles Entertainment Law Review**, Vol.23, No.1, 2002, s. 89.
[404] Yetki sorunları çözebilmek amacıyla "reasonable" makul veya mantıklı prensibi Brenner tarafından geliştirilmektedir. Bkz: Brenner, **a.g.m.**, s. 29.
[405] Armando A. Cottim ,"Cybercrime, Cyberterrorism and Jurisdiction: An Analysis of Article 22 of the COE Convention on Cybercrime", **European Journal of Legal Studies,** Vol.2, No.3, 2010, s. 63.
[406] Council of Europe, Explanatory Report to the Convention on Cybercrime, Budapest, 2001, par, 233, s. 40.
[407] Cottim, **a.g.m.**, s. 64; Calderoni, **a.g.m.**, s. 347.

Ancak devletlerin 3. Fıkraya göre a. bendinde düzenlenen ülkesellik prensibi veya "aut dedere aut judicare" iade et ya da kovuştur prensibi çerçevesinde çekince koyamaz. Yani suçun başka bir devlette işlenmesi durumunda sanığın bulunduğu devletin Sözleşme'nin 24. Maddesine göre, sanığın teslim talebini kendi vatandaşı olması nedeniyle reddedilmesi halinde ulusal yasalarında yer alan prosedürleri uyarınca yargılaması gerekmektedir[408].

22. maddenin son fıkrasında olumlu yetki uyuşmazlıklarına çözüm getirmeye çalışılmıştır. Suçun işlendiği devletlerin suçun kavuşturulması için uygun yeri belirlemek noktasında birbirlerine danışacaklardır. Bu hüküm sadece olumlu yetki uyuşmazlığıyla uygun olabilmektedir[409]. Devletlerin bazı durumlarda çözüm olarak tek bir yer seçebilmektedirler. Diğer durumlarda daha etkin olarak suç işleyenlerin birçok ülkede yargılanmasını tercih edebilmektedir. Ancak söz gelimi danışma yükümlülüğü mutlak değildir. Taraf devletin gerekli olmadığında veya suçun kavuşturulmasına olumsuz bir şekilde etkilendiğinde danışmayı erteleyebilmekte veya reddedebilmektedir.

Sözleşme 'de siber suçların yargı yetkisinin sorunları çözülmüş değildir. Suçun işlendiği yer konusunda bir açıklık getirilmemiştir[410]. Bir ülkede bulunan fail tarafından çocuk pornografisiyle ilgili içerik başka bir ülkede bulunan bilişim sistemine iletilebilmektedir[411]. Dünyanın herhangi yerinden kişiler söz konusu içeriği indirebilmekte veya görebilmektedir. Ancak bu sorunu zorlaştıran durum, o içeriği gören veyahut yükleyen kişinin suç olarak sayılmayan bir ülkede bulunmasıdır. Dolayısıyla ülkesellik ve şahsilik prensibi siber suçların çıkardığı yetki ve işlendiği yerle ilgili sorunlara karşı aciz kalmaktadır. Bu sonuna Avrupa Birliği tarafından yapılan direktifler ve çerçeve kararlarda bir çözüm getirilmeye çalışılmıştır. Ancak

[408] Cottim, **a.g.m.**, s. 65.
[409] Calderoni, **a.g.e.**, s. 347.
[410] Bkz: Ellen S. Podgor,"Cybercrime: National, Transnational, or International?", **Wayne Law Review**, Vol. 50, No. 1, 2004, s. 107.
[411] Cottim, **a.g.m.**, s. 67.

Avrupa Konseyi Siber Suçlar Sözleşmesi'nde olduğu gibi siber suçlarla ilgili yetki sorunu çözülmüş değildir[412].

Bu soruna uluslararası ceza hukuku açından bakıldığında siber suçlara özel bir uluslararası mahkeme var mı? veya siber suçlar Uluslararası Ceza Mahkemesi'nin (ICC) yargı yetkisi alanına girebilir mi?

Hâlihazırda siber suçlarla ilgili uluslararası düzeyde özel bir makam veya mahkeme bulunmamaktadır. ICC 'in yargı yetisi alanına giren suçlar ise Roma Statüsü'nün 5. maddesine göre uluslararası toplumu tehdit eden soykırım suçları, savaş suçları, insanlığa karşı suçlar ve saldırı suçlardır [413]. Bu bağlamda siber suçlar Roma Statüsü'nde açıkça yer almamaktadır. Ancak bazı yazarlara göre siber eylemler olarak anılan suçların işlenmesinde yeni bir yöntemi oluşturabilmekte, işlenmesi için kolaylaştırılmakta veya teşvik edebilmektedir. Bu nedenle söz konusu eylemler ICC'in yargı yetkisi alanına girebilmektedir[414]. Siber eylemlerin ilk bakışta saldırı suçu kapsamında değerlendirilebileceği görülebilmektedir[415].

Siber saldırı, saldırı suçu oluşturabilmesi için belli kriterleri sağlaması gerekmektedir. Roma Statüsü'ne eklenen 8 bis maddenin 1. fıkrasına göre saldırı suçu gerçekleşmesi için devletin askeri ve siyasi eylemlerini etkili bir şekilde kontrol etme veya yönetebilme gücüne sahip biri tarafından işlenmiş olmalıdır [416]. Bu liderlik

---

[412] Bkz: Velasco, **a.g.m.**, s. 339- 340.
[413] Orçun Ulusoy, **Uluslararası Ceza Mahkemesi**, Ed. Utku Kılınç, İzmir, Etki Matbaacılık Yayıncılık, 2008, s. 22- 29.
[414] Marco Roscini, "Gravity in the Statute of the International Criminal Court and Cyber Conduct That Constitutes, Instigates or Facilitates International Crimes", **Criminal Law Forum**, Vol. 30, No. 3, 2019, s. 249.
[415] Chance Cammack "The Stuxnet Worm and Potential Prosecution by the International Criminal Court under the Newly Defined Crime of Aggression", **Tulane Journal of International & Comparative Law**, Vol. 20, No. 1, 2011, s. 319-324.
[416] 2002 yılında yürüğe giren Roma Statüsü'nde, Uluslararası Ceza Mahkemesi'nin yargı yetkisine giren suçları düzenlenirken saldırı suçuyla ilgili bir tanım yapılmamıştır. Kampala'da 2010 yılında düzenlenen Roma Statüsü'nün ilk gözden geçirme konferansı sonucunda saldırı suçun tanımını ve unsurlarını yapan ve bu suçla ilgili Mahkeme'nin yargı yetkisini düzenleyen 6 sayılı karar alınmıştır. karar uyarıca statü'nün 5. maddesi 2. fıkrası kaldırılmış ve ayrıca statü'ye saldırı suçun tanımıyla ilgili 8 bis, yargı yetkisiyle ilgili 15 bis ve 15 ter maddeler getirilmiştir. bkz: Nergiz Emir, "Uluslararası Ceza Mahkemesi'nin Yargı Yetkisi Bakımından Saldırı Suçu", **Anadolu Üniversitesi Hukuk Fakültesi Dergisi** C.I, S.2, 2015, b.a.; Claus Kreb, Leonie Von Holtzendorff, The Kampala Compromise on the Crime of Aggression, **Journal of International Criminal Justice**, Vol. 8, No. 5, 2010, s. 1210-1215;

koşulu genellikle siber saldırılarda sağlanmamaktadır. Ancak DOS saldırılarında bu koşul istisnai durumlarda sağlanabilmektedir. Örneğin, 2008 yılında Gürcistan hükümetine karşı Ruslar tarafından gerçekleştirilen DOS saldırıları neticesinde Gürcistan hükümetinin kendi vatandaşlarıyla iletişim kurması engellenmiştir[417] .

Siber 8 bis maddenin 2. fıkrasına göre saldırı suçu oluşturan eylemler klasik anlamada bir devletin işgal edilmesi, ülkesine karşı bombardıman yapılması veya herhangi bir şekilde kuvvet kullanılması, bir devletin limanlarının veya kıyılarının ablukaya alınması, kara, deniz veya hava kuvvetlerine ya da deniz ve hava filolarına karşı saldırıda bulunulması, kabul edilen bir antlaşma uyarınca ülkede bulunan silahlı kuvvetlerin antlaşmanın amacına aykırı davranması ya da antlaşma anlaşmanın sona ermesinden sonra ülkede kalması, bir devletin topraklarının diğer devlet tarafından üçüncü bir devlete karşı bir saldırı eyleminde kullanımına izin vermesi ve başka

---

Sergey Sayapin, **The Crime of Aggression in International Criminal Law**, Netherlands, Asser Press, 2014, s. 55- v.d. 8 bis maddeye göre:
"1. Bu Statü'nün amacı bakımından "saldırı suçu", bir devletin siyasi veya askeri eylemlerini etkili biçimde kontrol edebilme veya yönetebilme konumunda bulunan bir kimse tarafından, karakteri, ağırlığı ve boyutu itibariyle Birleşmiş Milletler Şartı'nı açıkça ihlal eden bir saldırı fiilinin planlanması, hazırlanması, başlatılması veya icrasını ifade eder.
2. Paragraf 1'in amacı bakımından "saldırı fiili", bir devlet tarafından, bir başka devletin egemenliğine, toprak bütünlüğüne veya bağımsızlığına karşı veya Birleşmiş Milletler Şartı'na aykırı başka şekillerde silahlı kuvvet kullanılmasıdır. Aşağıdaki eylemlerden her biri, savaş ilan edilmiş olup olmamasına bakılmaksızın, BM Genel Kurulu'nun 14 Aralık 1974 tarih ve 3314 (XXIX) sayılı kararına uygun olarak saldırı fiili biçiminde değerlendirilir:
(a) Bir devletin silahlı kuvvetlerince, bir diğer devletin topraklarına yönelik olarak yapılan istila veya taarruz ya da ne kadar geçici olsa da, bu tür bir istila veya taarruzdan kaynaklanan herhangi bir askeri işgal veya kuvvet kullanarak başka bir devletin topraklarının tümünün ya da bir bölümünün ilhakı;
(b) Bir devletin silahlı kuvvetleri tarafından, başka bir devletin ülkesine karşı yapılan bombardıman veya bir devlet tarafından diğer devletin ülkesine karşı gerçekleştirilen herhangi bir silah kullanımı;
(c) Bir başka devletin silahlı kuvvetleri tarafından, bir devletin limanlarının veya kıyılarının ablukaya alınması;
(d) Bir devletin silahlı kuvvetleri tarafından, bir başka devletin kara, deniz veya hava kuvvetlerine ya da deniz ve hava filolarına saldırı;
(e) Kabul eden devletle yapılan bir anlaşma uyarınca o devletin ülkesinde bulunan bir devletin silahlı kuvvetlerinin, o anlaşmada belirtilen koşullara aykırı olarak kullanılması veya anlaşmanın sona ermesinden sonra da bu topraklardaki varlığını devam ettirmesi;
(f) Topraklarını başka bir devletin kullanımına tahsis eden bir devletin, topraklarının diğer devlet tarafından üçüncü bir devlete karşı bir saldırı eyleminde kullanımına izin vermesi;
(g) Bir başka devlete karşı yukarıda sayılan fiiller düzeyinde silahlı kuvvet eylemleri gerçekleştiren silahlı çetelerin, grupların, düzensiz birliklerin veya paralı askerlerin bir devlet tarafından veya bir Devlet adına gönderilmesi ya da o Devletin bu eylemlere önemli ölçüde katılması". bkz: İbrahim Kaya, **Uluslararası Hukukta Temel Belgeler,** Ankara, Seçkin Yayıncılık, 2013, s. 412-414.
[417] Perloff-Giles, **a.g.m.**, s. 221.

devlete silahlı çeteler, gruplar, düzensiz birlikler veya paralı askerler bir devlet tarafından veya bir devlet adına gönderilmesi ya da o devletin bu eylemlere önemli ölçüde katılmasıdır. Söz konusu eylemler örnek olarak sayılıp saldırı suçu bu eylemlerle sınırlı değildir.

Saldırı suçun gerçekleştirilmesi için Birleşmiş Milletlerin Antlaşması'na açıkça aykırı bir şekilde kuvvet kullanması gerekmektedir. Siber uzayın araçları zarar vermek için bir silah olarak kullanılabilmektedir. Eylemin, saldırı suçu olarak sayılması için belli bir ağırlığa ulaşması gerekmektedir. Bazı araştırmacılara göre siber saldırıların sivil veya askeri bilişim ağlarına zarar verip neticede ölüm gibi maddi zararlara neden olması gerekir, ciddi ölçüde etki yaratan elektrik kesintileri, ölümcül kazalara neden olan uçak bilişim sistemine zarar vermek gibi durumunda saldırı suçu teşkil etmiş olacaktır[418]. Siber saldırının verdiği zarar büyük olmayabilir veya hacmi bilinemeyebilir[419]. Keza siber eylemlerinin kuvvet kullanımını içerip saldırı suçu olarak sayılması büyük hukuki tartışmalara yol açmaktadır[420]. Nitekim siber saldırıyı düzenleyen NATO tarafından hazırlanan Siber Savaşa Uygulanacak Hukuk Hakkında Tallinn El Kitabı'nda her siber saldırının, saldırı suçu oluşturmayacağı ifade edilmişidir. Ona göre "belli sayıda insanın yaralanmasına ya da ölümüne neden olması ya da mallarında önemli derecede zarara ya da yıkıma sebep" olması halinde, saldırı suçu olarak sayılabilecektir[421]. Bu noktada her siber saldırının saldırı suçu teşkil edemeyeceği anlamına gelmektedir. Ayrıca Statüsü 'nün 22. maddesine göre yorum kapsamı dar bir şekilde tutulup kıyas aracılığıyla ICC'nin yargı alanının genişletilmemesi gerektiği vurgulanmaktadır. Dolayısıyla siber eylemler saldırı suçu kapsamında değerlendirilmemektedir.

Görüldüğü gibi siber suçlar Roma Statüsü uyarınca ICC'nin yargı yetkisi alanına girmemektedir. Siber suçların ICC'nin yetki alanına eklenmesi veya siber

[418] Bkz: Erdem, Özocak, **a.g.m.**, s. 138-139.
[419] Roscini, **a.g.m.**, s. 250; Perloff-Giles, **a.g.m.**, s. 222.
[420] Bu noktada 2010 yılında yapılan Kampala'da Roma Statüsü'yle ilgili konferansında görüşmeler esnasında heyetler saldırının suçu siber eylemleri kapsamayacağı konusumada endişelerini ifade etmişlerdir. Roscini, **a.g.m.**, s. 250; Erdem, Özocak, **a.g.m.**, s.139.
[421] Erdem, Özocak, **a.g.m.**, s. 139.

suçlarla ilgili özel yeni uluslararası düzeyde bir mahkeme kurulması siber suçların işlendiği yer, bununla ilgili yargı yetkisi, sınır ötesi delillerin toplanması ve devletlerin hukuk sistemlerinin farklılığı sorunları çözmek için etkili bir mekanizma teşkil edebilmektedir. Aynı zamanda böyle bir mahkeme bulunması siber suçluların cezasız kalmasının önlenmesinde büyük katkı sağlanmış olacaktır.

Uluslararası hukukta söz konusu uluslararası veya herhangi bir ulusal mahkemenin siber suçlarla ilgili yargı yetkisine sahip olmasını sağlayan iki yol bulunmaktadır. İlki evrensel yargı yetkisi ya da evrensellik ilkesi, diğeri ise tamamlayıcılık ilkesidir[422]. Evrensellik ilkesinin uluslararası işbirliği gerektiren sınır aşan suçlara uygulanmasında önem arz etmektedir[423]. Bu ilkeye göre devletler uluslararası toplumun bütününü tehdit eden suçların işlendiği yere, failin veya mağdurun vatandaşlığına bakılmaksızın üzerinde yargı yetkisine sahip olabilmektedir. Başka ifadeyle mülkilik, kişilik ya da korunma ilkeleri uyarınca yetkili olmayan devletin insanlığa karşı işlenen deniz haydutları, uluslararası terörizm gibi organize sınır aşan suçların yargılamasında kendini yetkili olarak saymasıdır[424]. Evrensellik ilkesi uluslararası veya herhangi bir devletin ulusal mahkemesinin suçlu üzerinde yargı yetki istemesini sağlamakta ve siber suçların çıkardığı sorunlara çözüm üretebilmektedir.

İnsan ırkının düşmanı "hostis humani generis" olarak sayılan korsanlık suçları işlendikleri yerde yargılanabilmektedir. 1994 yallında yürürlüğe giren Birleşmiş Milletler Deniz Hukuku Sözleşmesi ve uluslararası teamül hukuku uyarınca açık denizlerde işlenen korsanlık suçları herhangi bir devlet tarafından yargılanabilmektedir. Aynı şekilde siber suçlular insan düşmanı olarak ve siber uzay açık deniz olarak kabul edilebilmektedir. Korsanlık suçları üzerinde evrensel yargı yetkisi uygulanmasının gerekçesi uluslararası ticaretin tehlikeye sokulması, DOS saldırıları da büyük ticari web siteleri devre dışı bırakabilir ve zarar görmesine neden

[422] Perloff-Giles, **a.g.m.**, s. 223.
[423] Tezcan, Erdem, Önok, **a.g.e.**, s. 129.
[424] Keçeligl, **a.g.m.**, s. 7; Tezcan, Erdem, Önok, **a.g.e.**, s. 128.

olabilmektedir [425]. Dolayısıyla uluslararası ticarete tehdit teşkil edebilmekte hatta uluslararası barışın güvenliğine ve ekonomisine tehlike kaynağı oluşturmaktadır. Bu durumda siber suçlara evrensel yargının uygulanmasında öncelik verilmesi gerekmektedir. Ancak siber suçların kapsamının belirlenmesi evrensellik ilkesinin siber suçlara uygulanmasında bir zorluk teşkil edebilmektedir. Söz konusu siber suçların kapsamının dikkatli bir şekilde çizilmesi durumunda siber suçlarla mücadelede caydırıcı bir araç olabilmektedir[426].

Tamamlayıcılık ilkesine göre ulusal mahkemeler işlenen suçlara yargı yetkesinin kullanmasında önceliğe sahiptir. Bu ilke Roma Konferansı öncesinde "uluslararası ceza yargısının ulusal ceza yargısını tamamlayıcılığı" ifadesiyle vurgulanmıştır[427]. Fakat ulusal mahkemelerin suçu kavuşturmadığı (isteksiz olma) veya kavuşturmak için yeterli teknik kapasitesine sahip olmadığı (yetersiz olma) durumlarda ICC bu suç üzerinde yargı yetkisine sahip olabilmektedir. Böylece tamamlayıcılık ilkesi devletlerin ulusal egemenliğine saygı göstermektedir. Bu durum söz konusu uluslararası mahkemenin devletlerin Roma Statüsü gibi bir anlaşmaya katılma olasılığı daha yüksek hale getirebilmektedir. Tamamlayıcılık ilkesi bazı devletlerin siber suçluları yargılamaması ve teslim etmemesi sorununu çözebilmektedir. Ancak siber suçun birçok farklı devletin kanununun kapsamına girmesi sorununa çözüm getirmemektedir[428]. Bu sorun ancak ulus üstü bir mahkeme veya merci tarafından çözülebilmektedir.

3.1.2.2.2. Uluslararası İşbirliğine İlişkin Zorluklar

Uluslararası işbirliğinin amacı çeşitli ülkelerde suç işleyenlerin cezasız kalmalarını önlemektir. Suçlularla mücadele faillerin işledikleri suçun karşılığında alacakları cezaları öngörmeyi gerektirmektedir. Suçun sadece işlendiği ülkenin değil

[425] Perloff-Giles, **a.g.m.**, s. 224; Li, Jia, **a.g.m.**, s. 52.
[426] Perloff-Giles, **a.g.m.**, s. 225.
[427]Selcen Erdal, "Uluslararası Ceza Mahkemesinin Ulus-Devlet Egemenliğine Etkisi", **Selçuk Üniversitesi Hukuk Fakültesi Dergisi** , C.XVIII, S. 1, 2010, s. 171.
[428] Perloff-Giles, **a.g.m.**, s. 225.

aynı zamanda bütün ülkelerin güvenliğini tehdit edebilmektedir[429]. Özellikle siber suç söz konusu olduğunda yukarıda açıklamaya çalışıldığı gibi hem devletin kendi ülkesel sınırlarını geçmekte hem de bu tür suçların failleri cezasız kalma ihtimali daha yükselmektedir. Dolayısıyla bütün devletlerin ve uluslararası organizasyonların birbirleriyle işbirliği sağlamak üzere birlikte hareket etmeleri gerekmektedir.

Her ne kadar devletler siber suçlara ilişkin iyi ve etkili maddi ve usuli düzenlemeler yapsa da yeterli olmayacaktır. Bu suçlarla mücadele devletler arası işbirliğinin mekanizmalarına dayanmaktadır[430]. Öğretide ifade edildiği gibi siber suçlarla mücadele[431] "ya global olacak ya da hiçbir anlamı olmayacaktır"[432]. Yani uluslararası işbirliği "olmazsa olmaz" bir şart olarak görülmektedir[433]. Birkaç devletin katılmaması durumunda suçlular, suçluların iadesine ve adli yardımlaşmaya ilişkin sözleşmelere katılmayan devletleri sığınak olarak kullanıp oradan eylemleri gerçekleştirmeye devam edebilmektedirler[434]. Ancak söz gelimi uluslararası işbirliğinde aşağıda değinilecek üzere devletlerin hukuki sistemlerin farklılığı, anlaşmaların eksikliği ve pörsüdüklerin hantal ve uzun olması gibi zorluklar bulunmaktadır.

3.1.2.2.2.1. Hukuk Sistemlerinin Farklılığı

Hukuk sistemleri toplumların farklı ihtiyaçlarına ve gerçekliklerine göre şekillendirilmektedir. Kanunlar toplumdaki din, kültür, tarih, sosyoloji, bulunduğu

---

[429] Tezcan, Eredem, Önok, **a.g.e.**, s.149.
[430] Anna-Maria Osula, "Mutual Legal Assistance & Other Mechanisms for Accessing Extraterritorially Located Data", **Masaryk University Journal of Law and Technology**, Vol. 9, No. 1 ,2015, s. 44.
[431] Arias Sanchez'e göre Devlet tek başı siber güvenliğe yönelik gerçekleştirilen tehditlere karşı duramaz. Dolayısıyla uluslararası ilkeler kazandıracak ve küresel düzeyde devletler arasında hızlı bir koordinasyonu sağlayan bir uluslararası çerçeveye acil ihtiyaç duyulmaktadır. bkz; Joachim Vogel, "Towards a Global Convention against Cybercrime", First World Conference of Penal Law. Penal Law in the XXIst Century, Guadalajara (Mexico), 2007, (çevrimiçi), http://www.penal.org/sites/default/files/files/Guadalajara-Vogel.pdf, Erişim Tarihi: 11.02.2020, s. 10.
[432] Dülger, **a.g.e.**, s. 188.
[433] Erdem, Özocak, **a.g.m.**, s. 2.
[434] Choo, **a.g.m.**,s. 289-290.

coğrafya gibi birçok faktörün yansımasıdır[435]. Bunun doğal sonucu olarak devletlerin farklı maddi ve usuli ceza yasalarına sahip olmaktadır[436]. Siber suçlar söz konusu olduğunda sorun daha da artmaktadır. Maddi hukuk bakımından hangi eylemin suç olarak sayılması devletler arasında büyük farklılık göstermektedir[437]. Birinci bölümde ele alındığı üzere şimdiye kadar suçun ne terimi konusunda ne de tanımı konusunda görüş birliği bulunmamaktadır. Gerçekleşen eylemin mağdur ülkesinde suç olup failin olduğu ülkede suç olarak sayılmamış veya faklı bir şekilde tanımlanmış olabilmektedir[438]. Örneğin "nasyonal-sosyalist" ile ilgili propaganda Almanya ve Avusturya'da suç olarak sayılıp cezalandırırken ABD, Avustralya ve Kanada'da düşünce özgürlüğü kapsamında değerlendirilmekte ve suç teşkil etmemektedir[439]. Aynı şekilde nefret söylemi eylemleri Avrupa ülkelerinde nefret suçu teşkil etmekte ancak ABD'de ifade özgürlüğü kapsamında nitelendirilmektedir.

Bu konuda "Yahoo! v. LICRA" davası en bariz örnektir[440]. Yahoo! siteleri üzerinden Fransız ceza hukukuna aykırı olarak Nazi ile ilgili fotoğraf, satış, değişim veya Üçüncü Reich hatıra görüntülenmesi gibi materyallere erişim sağlanmaktadır[441]. Bundan dolayı 2000 yılında Fransız kar amacı gütmeyen Irkçılık ve Antisemitizme Karşı Uluslararası Birliği (LICRA) tarafından Yahoo! şirketine karşı açılan dava sonucunda Paris mahkemesi Yahoo! şirketinin Nazi'yle ilgili tüm materyallerinin erişimini engellemek için gerekli tedbirleri almasına karar vermiştir. Fransa'daki Yahoo! (www.yahoo.fr) mahkemenin kararına uyarak bütün Nazi materyallerini kaldırmıştır. Ancak Paris mahkemesinin söz konusu içeriği Fransızların erişebildiği Yahoo!'nün global internet sitesinden kaldırılmasını istemiştir. Bu isteği ret eden

---

[435] Ahmet Gökcen, Caner Yenidünya, Mehmet Emin Artuk, **Ceza Hukuku Genel Hükümleri**, 8.bs., Ankara, Adalet Ayayıevi, 2014, s. 3.
[436] Matthew R. Zakaras, "International Computer Crimes, General Report", **Revue internationale de droit pénal,** Vol. 72, No. 3, 2001, s. 827.
[437] Laksana, **a.g.m.**, s. 221.
[438] Servet Yetim, "Bilişim Suçları ve Etkin Mücadele Yöntemleri", **Terazi Hukuk Dergisi**, C.IX, S.95, 2014, s. 83; Osula, **a.g.m.**, s. 45.
[439] Özbek, **a.g.m.**, s. 113.
[440] Marc H. Greenberg, "A Return to Lilliput: The LICRA v. Yahoo! Case and the Regulation of Online Content in the World Market", **Berkeley Technology Law Journal** , Vol. 18, No. 4, 2003, s. 1193.
[441] Bkz: Mark Hunter, Marc Le Menestrel,Henri-Claude de Bettignies, "Ethical Crisis on the Internet: the Case of Licra vs. Yahoo!", **Business Ethics and the Electronic Economy**, Ed. Peter Koslowski, Christoph Hubig, Peter Fischer Berlin, Springer, 2004, s. 188.

yahoo! Paris Mahkemesi'nin içeriğin global web sitesinden (www.yahoo.com) kaldırılmasına ilişkin kararının ifade özgürlüğü düzenleyen Amerikan Anayasası'na aykırı olduğunu iddia edip Kaliforniya Kuzey Bölgesi Mahkemesi'nde dava açmıştır. Söz konusu bu mahkeme Paris Mahkemesi'nin kararını Amerikan Anayasası'na aykırı ve ABD'de uygulanamaz olduğuna karar vermiştir[442].

Devletlerin ceza maddi yasaları farklı olduğu gibi öngörülen prosedürleri de farklıdır[443]. Bir devlette yapılan suçun soruşturma, kavuşturma ve ilgili delilerin toplanma yöntemleri bir devlette etkin bir şekilde gerçekleştirilebilmektedir. Fakat başka bir devlette yetersiz veya yasal olmayabilmektedir. Bu uyumsuzluk devletlerin ulusal yasalarının arasında çatışmaların ortaya çıkmasına neden olmaktadır. Örneğin uzaktan arama tedbirleri ABD'de ve Birleşik Karalık'ta suçlarla ilgili delilerin elde etme yasal yöntemlerden biridir. Ancak diğer ülkede bireyin gizlilik haklarının ihlali teşkil edip hukuka aykırı bir tedbir olarak değerlendirilmektedir[444]. Nitekim bir siber suçun soruşturmasında en kritik konulardan beri verilerin saklanmasıdır. Devletler veri saklama konusunda farklı gereksinimlere sahiptir[445].

Devletlerin ceza hukuk sistemlerinin farklılığı siber saçlarla ilgili hükümlerin birbiriyle bağdaşmaması ve hukukun çarpışmasına neden olmaktadır[446]. Ayrıca uluslararası işbirliğine bir engel teşkil etmektedir. Adli yardımlaşmanın ve suçluların iadesi gibi işlemleri gerçekleştirilmesi için çifte cezalandırılabilirlik ön şartıdır. Bu şart uyarınca adli yardımlaşma talebine konu olan suç hem talepte bulunan devletin hem de talep edilen devletin ceza yasalarında suç olarak düzenlenmiş olması gerekmektedir[447]. Çifte cezalandırılabilirlik koşulun sağlanmaması uluslararası işbirliği kapsamında yapılan delilerin elde edilmesi gibi işlemlerin aksamasına yol

[442] Elissa A. Okoniewski, "Yahoo!, Inc. v. LICRA: The French Challenge to Free Expression on the Internet", **American University International Law Review,** Vol. 18., No.1, 2002, s. 214-220.
[443] Zakaras, **a.g.m.**, s. 828.
[444] Susan W. Brenner, "Law, Dissonance, and Remote Computer Searches", **North Carolina Journal of Law & Technology**, Vol. 14, No.1, 2012, s. 50, 84.
[445] Ehuan, **a.g.m.**, s. 138.
[446] Malby v.d., **a.g.e.**, s. 56.
[447] Ajayi, **a.g.m.**, s. 10.

açabilmektedir[448]. Ayrıca "jurisdiction shopping" olarak adlandırılan kavramı gerçekleşmiş olacaktır. Buna göre suçlular siber suçları cezaya tabi tutmayan veya daha az ceza uygulayan devletlerde bulunup faaliyetleri sürümektedirler[449]. Yani eylemin bir ülkede suç olarak düzenlenmesi ve diğer bir ülkede suç sayılmaması suçlunun yargılama sürecini zorlaştırmakta ve uluslararası işbirliği imkansız hale getirmektedir[450].

Bu sorunun üstünden gelinebilmek için devletlerin siber suçlara ilişkin yasalarını uyumlaştırması gerekmektedir[451]. Ancak devletlerin yapı, tarihi, kültürü, sosyal dinamikleri, hukuki gelenekleri gibi farklı faktörler doğrultusunda söz konusu uyumlaştırma süreci oldukça zor görülmektedir. "Tek beden herkese uyar" ilkesi siber suçlar konusunda uygun değildir. Dolayısıyla bu suçlarla mücadele devlerin farklı iç şartlarına dikkat eden bir uyumlaştırma gerektirmektedir[452]. Yeri gelmişken belirtmek gerekir ki, yasaların uyumlaştırılması özdeş "identical" anlamına gelememektedir. Bundan maksat önemli olan tamamlayıcılıktır. Yani ulusal ve bölgesel farklılıklarının uygulama mekanizmalarının etkin bir şekilde çalışmasını sağlayacak şekilde azaltılması ve mümkün olduğu kadar uzlaştırılmasıdır[453].

3.1.2.2.2.2. Uluslararası Antlaşmaların Eksikliği

Devletler arası işbirliğinin en önemli mekanizmaları suçluların iadesi ve adli yardımlaşmadır. Geçmiş yıllarda çerçevesi dar tutulan adli yardımlaşmanın gün geçtikçe söz konusu kapsamı genişlemektedir. Günümüzde adli yardımlaşma bilgi verme ve adli sicil bilgilerinin gönderilmesi, mahkeme kararı ve yargılamayla ilgili

[448] Jonathan Clough , "A World of Difference: The Budapest Convention On Cybercrime And The Challenges Of Harmonisation", **Monash University Law Review**, Vol. 40, No.1, 2014, s. 701; Dülger, **a.g.e.**, s. 188.
[449] Choo, **a.g.m.**, s. 289-290.
[450] Csonka, **a.g.m.**, s. 477.
[451] Malby v.d., **a.g.e.**, s. 57.
[452] Angers, **a.g.m.**, s. 43.
[453] Uluslararası sözleşme, Siber suçlarla ilgili yasaların uyumlaştırılmasının aracıdır. Ancak söz konusu bu sözleşmenin üç norm göz önünde bulundurması gerekmektedir. Bunlar: siber suçlarla ilgili zorlukların kapsaması, temel hakların korunası ve devletlerin farklı hukuk sistemlerin temsil edilmesidir. bkz :Clough, **a.g.m.**, s. 208-225.

belgelerin tebliği, tanık, bilirkişi ve sanıkların dinlenmesi, delil amaçlı arama ve el koyma kararı, eşya veya belge gönderilmesi ve tutuklanan kişinin başka ülkeye gönderilmesi gibi konuları kapsamaktadır[454].

Devletler arası antlaşmaların yokluğunda uluslararası hukukta devletin diğer devletlerle siber suç veya herhangi suçlar konusunda işbirliği sağlama yükümlülüğü bulunmamaktadır[455]. Dolayısıyla bu hususta uluslararası hukukta ciddi eksiklikler bulunmaktadır[456]. Yani söz konusu adli yardımlaşma ve suçluların iadesi işlemleri ancak devletlerin arasındaki imzalanan karşılıklı ikili veya çoklu[457] (Avrupa Konseyi Siber Suç Sözleşmesi, Ceza İşlerinde Karşılıklı Adlî Yardım Avrupa Sözleşmesi gibi) antlaşmalar aracılığıyla yürütülmektedir[458]. Ancak hâlihazırda siber suçlarla mücadeleye ilişkin uluslararası düzeyde bir sözleşme bulunmamakta, akdedilen bütün antlaşmalar bölgesel niteliktedir[459]. İkili veya çoklu bölgesel anlaşmaların etkinliği katılan devletlerle sınırlıdır[460]. Bu durum nedeniyle siber suçlara karşı global mücadelede büyük bir zorluk söz konusudur.

Siber suçlarla ilgili işbirliğine ilişkin antlaşmaların olamamasına en önemli örnek 2000 yılında gerçekleştirilen Gorshkov ve Ivanov olayıdır. Rus bilişim korsanları olan Vasiliy Gorshkov ve Alexey Ivanov tarafından Amerikan şirketlerinin bilişim sistemlerine yasa dışı bir şekilde saldırlar gerçekleştirilerek verileri elde edilmiş ve şantaj yapılmıştır[461]. ABD ve Rusya arasında suçlular iadesi antlaşması

---

[454] Tezcan, Erdem, Önok, **a.g.e.**, s. 150; Kemal Şimşek, "Uluslararası Adli Yardımlaşma Konusunda Uygulamada Karşılaşılan Sorunlar ve Çözüm Önerileri Üzerine", **Adalet Dergisi**, S.45, 2013, s. 148

[455] Inger Marie Sunde, "Cybercrime Law", **Digital Forensics**, Ed.André Årnes, Hoboken John Wiley & Sons, 2018, s. 111; Vatis, **a.g.m.**, s. 220.

[456] Ehuan, **a.g.m**., s. 38.

[457] Adli yardımlaşamaya ilişkin sözleşme bulunmadığı durumunda devletler aralarında işbirliği karşılıklılık ilkesine dayanarak gerçekleştirebilmektedirler. Söz konusu bu ilkeye göre talep edilen devlet gelecekte talep eden devletin istemini aynı ölçüde yardımlaşma sağlayacağı taahhütte bulunması halinde talebi yerine getirmektedir. Tezcan, Erdem, Önok, **a.g.e.**, s. 164; Sunde, **a.g.m.**, s. 112; Oerlemans, **a.g.e.**, s. 63.

[458] Baki Yiğit Çakmakkaya, Teoman Akpınar, "Bilişim Suçları İle Mücadelede Karşılaşılan Sorunlar", **Balkan ve Yakın Doğu Sosyal Bilimler Dergisi**, C.IV, S. 3, 2018, s. 125; Osula, **a.g.m**, s. 46,

[459] Erdem, Özocak, **a.g.m.**, s. 5.

[460] Perloff-Giles, **a.g.m.**, s. 207.

[461] Susan W. Brenner, Joseph J. Schwerha IV, "Transnational Evidence Gathering and Local Prosecution of International Cybercrime", **The John Marshall Journal of Information Technology & Privacy Law**, Vol. 20, No. 3, s. 347-348.

olamadığından dolayı şüphelilerin Rusya tarafından teslim edilmesi mümkün olmamıştır. Dolayısıyla FBI suçun soruşturması ve kavuşturması yapmak üzere şüphelileri ABD'ye çekmiştir. FBI ajanların kurduğu "Invita" adlı gerçek olmayan bir bilişim şirketi aracılığıyla şüphelileri ABD'ye getirilmiş ve görüşme bir parçası olarak, kendi bilgisayar becerilerini göstermek için, FBI tarafından kurulan ağı hecelemeleri istenmiştir. Şüphelilerin ABD'de kullandıkları bilgisayarlarına önceden gizli yazılımlar yükleyen FBI, Rusya'daki bilgisayarlara erişim sağlamış şifreleri ve verileri ele geçirmiştir[462]. Böylece Rusya'da bulunan bilgisayarlardaki verileri ve delilleri kullanılarak şüphelileri yargılanıp mahkum edilmesi sağlanmıştır. Rusya buna itiraz ederek suçluların iadesini istemiş fakat sözleşme olmadığı için ABD söz konusu talebe önem vermemiştir[463].

3.1.2.2.2.3. Prosedürlerin Uzun ve Hantal Olması

Siber suçlarla ilgili suçluların iadesi ve adli yardımlaşma taleplerinin iletilmesi, kabul edilmesi ve daha sonra yapılacak prosedürler her iki devlette bulunan geleneksel diplomatik veya yargı makamlar aracılığıyla yapılmaktadır[464]. BM tarafından 2013 yılında yapılan bir aştırmaya göre devletler arası gerçekleştirilen işbirliğinin %70'i resmi geleneksel yöntemlere dayandığı ifade edilmiştir[465]. Bu araçlar (hukuki işlemler, evraklar çevrilmesi, v.s.) uzun ve karmaşık olması nedeniyle inanılmaz bir hızla sürekli gelişen ve sınır aşan siber suçlara karşı aciz kalmaktadır[466]. Başka ifadeyle Geleneksel uluslararası adli yardım rejimi genellikle bir siber suç sırasında meydana gelen yardım taleplerini karşılayamamakta ve yetersiz kalmaktadır. Örneğin bilişim teknolojileri alanında dünyadaki en gelişmiş devlet olan ABD, elektronik delilerin

[462] Aldesco, **a.g.m.**, s.206-.
[463] Jean-Baptiste Maillart, "The limits of Subjective Territorial Jurisdiction in the Context of Cybercrime", **ERA Forum**, Vol. 19., No. 3., 2019, s. 384.
[464] Ehuan, **a.g.m.**, s. 138.
[465] Malby vd, **a.g.e.**, s. 201.
[466] Osula, **a.g.m.**, s. 51.

kayıtlarıyla ilgili diğer devletlerin taleplerini yerine getirmek için ortalama olarak on ay veya daha fazla süre harcamaktadır[467].

Fail suçu işlerken iletişiminin birçok ülkeden geçmesi halinde adli yardımlaşama süreçleri daha da uzayacaktır. Bu durum suçla ilgili verilerin ve delilerin kaybolma ihtimalini arttırmaktadır. Bu nedenle devletler arasında klasik işbirliği yönetmelerinden vazgeçilip yeni hızlı yöntemlerin bulunması gerekmektedir. Örneğin soruşturmacıların diğer ülkelerdeki bulunan uzmanlarla iletişim kurabilmeleri için uluslararası acil durumlar için 7/24 ağlarını geliştirmektir[468].

Uluslararası işbirliğinin geleneksel yöntemlerinin yetersiz kalmasına ek olarak uygulamada da adli yardımlaşmaya ilişkin işlemlerin evraklarında bulunan her türlü eksikliğin iade gerekçesi yapılması, adli yardımlaşma evraklarının gönderilmesi hususunda mahkemelerin doğrudan Adalet Bakanlığı ile yazışma yapmaması, kolluk kuvvetlerinin yeterli kadar hukuk bilgisine sahip olmaması, soruşturma işlemlerinin eksik bir şekilde yapılması, yabancı dil bilen yeterli sayıda görevli olmaması gibi birçok zorluk bulunmaktadır[469].

3.2. Avrupa Konseyi Siber Suç Sözleşmesi'nde Uluslararası İşbirliği

Avrupa Konseyi Siber Suç Sözleşmesi, siber suçlara ilişkin devletler arası işbirliği hükümleri kapsamlı bir şekilde düzenleyen ilk uluslararası sözleşme olarak kabul edilmektedir[470]. Bu sözleşme daha sonra gerek ulusal gerekse uluslararası düzeyde yapılan düzenlemelere yol gösterici nitelikte bir metindir[471]. Dolayasıyla söz konusu Sözleşme'nin üçüncü kısmında yer alan uluslararası işbirliğine dair hükümleri incelemek büyük önem arz etmektedir.

---

[467] Perloff-Giles, **a.g.m.**, s. 207.
[468] Csonka, **a.g.m.**, s. 481.
[469] Şimşek, **a.g.m.**, s. 150-155.
[470] Osula, **a.g.m.**, s. 49.
[471] Richard W. Downing, "Shoring Up the Weakest Link: What Lawmakers Around the World Need to Consider in Developing Comprehensive Laws to Combat Cybercrime", **Columbia Journal of Transnational Law**, Vol.43, No. 3, 2004, s. 761.

3.2.1. Uluslararası İşbirliğine Dair Genel Prensipler

Sözleşme'nin 23. maddesinde uluslararası işbirliğine ilişkin üç genel prensip öngörülmüştür. Bunların ilki taraf devletler arasında uluslararası işbirliği "mümkün olan en geniş biçimde" gerçekleştireceklerdir[472]. Devletler arasında işbirliğinin önemini ifade eden bu prensipten maksat taraf devletler arasında etkin bir işbirliği, delillerin toplanma ve bilgilerin paylaşma sürecinin uluslararası düzeyde hızlı ve doğru olmasındaki zorlukları minimuma kadar indirilmektir[473]. Bu soyut hükmün çizdiği soyut çerçeveyi[474] 23. maddede yer alan aşağıda değinilecek diğer ilkelerle doldurulmaktadır.

İkinci prensip 23. maddede öngörülen uluslararası işbirliğinin kapsamını belirlemektedir. Buna göre işbirliğinin hükümleri siber suçları ve klasik suçları kapsamaktadır. Yani işbirliğinin yükümlülüğü hem bilişim sistemleri aracılığıyla veya bu sistemlere karşı işlenen suçlarda hem de delillerin dijital ortamda toplanmasını gerektiren klasik suçlarda da olabilmektedir[475]. Örneğin yurt dışında kasten öldürme suçunun işlenmesinde e-posta hizmeti kullanılması halinde söz konusu işbirliğinin hükümleri uygulanabilmektedir.[476] Sözleşme'nin uygulama alanının geniş tutulması çok önem taşıyan özelliklerinden biridir.[477] Bununla birlikte suçluların iadesi (24.m), trafik verilerinin gerçek zamanlı olarak toplanması konusunda yardımlaşma (33.m) ve içerikle ilgili verilerinin takip edilmesi konusunda yardımlaşma (34.m) konularında taraf devletlerin farklı bir yaklaşım benimsemelerine istisna olarak hak verilmektedir[478].

---

[472] Sunde, **a.g.m.**, s. 112.
[473] Explanatory Report to the Convention on Cybercrime, par, 242, s. 42.
[474] Önok, **a.g.m.**, s. 1249.
[475] Explanatory Report to the Convention on Cybercrime, par. 243, s. 42; Broadhurst, **a.g.m.**, s. 421, Angers, **a.g.m**., s. 49.
[476] Gercke, **a.g.e.**, s. 287.
[477] Michael A. Vatis, "The Council of Europe Convention on Cybercrime", National Research Council, **Proceedings of a Workshop on Deterring Cyberattacks : Informing Strategies and Developing Options for U.S. Policy,** Washington, D.C., National Academies Press, s. 208.
[478] Explanatory Report to the Convention on Cybercrime, par. 243, s. 42.

Son olarak işbu işbirliği Sözleşme'nin adli yardımlaşmayla ilgili hükümlerinin ve aynı zamanda devletler arasında akdedilmiş olan ceza işlerinde uluslararası işbirliğine dair tek taraflı veya karşılıklı sözleşmelerin ve ulusal mevzuatların bir arada uygulanması aracılığıyla gerçekleştirilmektedir[479]. Bu prensip uyarınca Sözleşme'nin 3. bölümünde yer alan uluslararası işbirliğine ilişkin hükümleri mevcut uluslararası işbirliğiyle ilgili uluslararası sözleşmelere üstün değildir.[480] Bunun nedeni bu Sözleşme yeni bir tür sözleşme olup uluslararası düzeyde ceza konularında delillere ulaşmayı sağlamak için tasarlanmaktadır[481]. Öte yandan bu Sözleşme'nin adli yardımlaşmaya ilişkin ayrı bir rejim tesis etmeyi amaçlamaması dolayısıyla yalnızca yürüklükte olan antlaşmaların, yasaların ve düzenlemelerin bu tür hükümleri öngörmediği durumlarda, Sözleşme gereğince her taraf devletin uluslararası işbirliğinin yürütülmesini sağlamak için yasal bir dayanak oluşturması yükümlülüğü yerine getirmesi gerekmektedir[482]. Ayrıca Sözleşme'nin hükümleri uluslararası işbirliğiyle ilgili ulusal yasaya da üstün olmamaktadır. Sınırlı istisnalar haracında her devlet kendisine ait kanunları uygulamaktadır[483].

3.2.2. Suçluların İadesi

Sözleşme'nin 24. maddesinin 1. fıkrasında suçluların iadesinin genel çerçevesi belirtilmiştir. Suçluların iadesi sadece Sözleşme'nin 2. -11. maddelerde sıralanan suçlarda, iki taraf devletlerin yasalarına göre üst sınırı en az bir yıllık hapis cezası ya da daha ağır nitelikli bir cezayla cezalandırılabilir olması şartıyla geçerli olacaktır[484]. Sözleşme'de söz konusu alt sınırının öngörülmesinin nedeni taraf devletlerin bazı

[479] Explanatory Report to the Convention on Cybercrime, par. 244, s. 42.
[480] Bu prensip 24. madde (suçların iadesi), 25. madde (adli yardımlaşmayla ilgili hükümler), 26.madde (kendiliğinden bilgi verme), 27. madde (uluslararası anlaşmaların yürürlükte bulunmadığı durumlarda gelen adli yardım talepleri), 28. madde (kullanımda gizlilik ve sınırlama), 31. madde (depolanan veriler hakkında arama el koyma), 33. madde (trafik verilerinin gerçek zamanlı olarak toplanması konusunda yardımlaşma) ve 34. maddelerde (içerik verilerinin takip edilmesi) vurgulanmaktadır. Explanatory Report to the Convention on Cybercrime, par. 244, s. 42.
[481] Weber, **a.g.m.**, s. 442.
[482] Gercke, **a.g.e.**, s. 287.
[483] Önok, **a.g.m.**, s. 1249.
[484] Calderoni, **a.g.m.**, s. 347.

suçlara (örneğin 2. Maddede yer alan izinsiz erişim ve 4. maddede yer alan verilere müdahale) daha kısa süreli bir hapis cezası belirleyebilmesidir.[485] Ancak bir suçun iadeye konu olup olmadığını belirleme noktasında somut olayda verilen cezaya değil, yasanın öngördüğü en üst ceza sınırına bakılacaktır[486].

Taraf devletler arasında daha farklı bir ceza alt sınırını içeren tek taraflı veya karşılıklı suçluların iadesine ilişkin sözleşmelerin olması durumunda bu hükümler uygulanacaktır. Örneğin, suçluların iadesine ilişkin birçok sözleşmede suçun iadeye konu olabilmesi için hapis cezası en az bir yıllık veyahut daha ağır bir ceza olması şart olarak öngörülmüştür. Dolayısıyla bu hükümler geçerli olacaktır[487]. Ayrıca Sözleşme'nin bazı hükümlerinde çekince koyma imkanı sağlamasıyla ilgili sorunlardan kaçınarak çifte cezalandırılabilirlik ilkesine dayanmaktadır[488].

24. maddenin 2. fıkrası uyarınca 1. fıkrada yer alan suçlar taraf devletler arasında suçluların iadesine ilişkin yürüklükte olan ve ilerde imzalanacak sözleşmelerde iadesi olabilir suçlar olarak ifade edilmektedir.

Maddenin 3.fıkrasına göre taraf devletler arasında suçluların iadesine ilişkin sözleşme olmadığı veya yürüklükte olan sözleşme söz konusu Sözleşme'nin belirlediği suçlar için talepleri kapsamadığı halde iade işlemlerini yapamayan taraf devlet, bunu yapmak zorunda olmamak kaydıyla Sözleşme'yi hukuki dayanak olarak kabul edip buna göre iade işlemlerini yapabilmektedir. Öte yandan 4. fıkrada taraf devletler arasında iade işlemlerinin sözleşmeler yerine genel yasalara göre yapılması halinde Sözleşme'nin saydığı suçların da dahil edileceği belirtilmiştir.

5. fıkrada suçluların iadesinin talep edilen taraf devletin kanununa veya mevcut olan suçluların iadesine ilişkin sözleşmelere uygun olarak gerçekleştirileceği belirtilmiştir[489]. Bu durum taraf devletler arasındaki işbirliğiyle ilgili uluslararası

---

[485] Mike Keyser, "The Council of Europe Convention on Cybercrime", **Journal of Transnational Law & Policy,** Vol. 12, No.3, s. 317.
[486] Explanatory Report to the Convention on Cybercrime, par. 245, s. 42.
[487] Havuz, **a.g.e.**, s. 187.
[488] Gercke, **a.g.e.**, s. 287.
[489] Türkiye bakımından Suçluların İadesine Dair Avrupa Sözleşmesi ve TCK m. 18'de öngörülen hükümler uygulanır. Önok, **a.g.m.**, s. 1250.

sözleşmelerin, ulusal yasaların ve karşılıklı düzenlemelerin bağlamında gerçekleştirilmesinin gerekliliğini vurgulayan başka bir örnektir. Suçluların İadesine Dair Avrupa Sözleşmesi ve Ek Protokolleri'nde öngörülen sınırlamalar ve şartlar bu sözleşmenin taraflarına uygulanacaktır. Örneğin, Suçluların İadesine Dair Avrupa Sözleşmesi'nin 3.maddesine göre suçun siyasi nitelikli veyahut kişinin ırkı, dini, milliyeti veya siyasi görüşü sebebiyle iade talebi edildiği anlaşıldığı halinde bu durum talebin reddine neden olacaktır[490].

Maddenin 6. fıkrasın (aut dedere aut judicare) ya iade et ya yargıla ilkesine göre düzenlenmiştir. İade talep edilen taraf devletler genellikle kendi vatandaşları olduğundan iade talebini reddetmektedir. Suçlular vatandaşı oldukları devletteki yetkili makamlar gereken işlemler yapmak zorunda olmadığı durumlarda başka bir taraf devlette işlemiş oldukları suçun sorumluluğundan kurtulabilmektedir. Bu fıkrasına göre iade talebi devletin vatandaşı olduğu gerekçesiyle reddedilirse, talep edilen taraf devletin, talepte bulunan taraf devletin isteği üzerine gereken işlemleri gerçekleştirmek için kendi yerel yetkili makamlarına sevk etmesi gerekmektedir. Talebi reddedilen devletin suçun soruşturması ve gereken işlemleri talep etmediği, iade talebi edilmediği veya talep edilen vatandaş dışındaki nedenden dolayı reddedildiği durumunda talep edilen devlet bu işlemleri gerçekleştirmek zorunda olmayacaktır. Ayrıca yerel soruşturma ciddi ve hızlı bir şekilde gerçekleştirilecek ve bunun soncunu talep eden taraf devlet bilgilendirilecektir[491].

7. fıkrasında ise taraf devletlerin iade ve geçici tutuklama talepleri yönelmesi gereken makamları belirtilmek için makamların isim ve adreslerini Avrupa Konseyi Genel Sekreteri'ne bildirmeleri yükümlülüğü getirilmiştir. Ancak bu hüküm sadece taraf devletler arasında bir sözleşme olmadığı halde geçerlidir. Sözleşme olduğunda iade ve geçici tutuklama talepleri konusunda taraf devletler kayıt yaptırma yükümlülüğü olmaksızın hangi makamlara başvuracaklarını bilmektedirler.

[490] Explanatory Report to the Convention on Cybercrime, par. 250, s. 43.
[491] Explanatory Report to the Convention on Cybercrime, par. 251, s. 43.

3.2.3. Adli Yardımlaşma

3.2.3.1. Adli Yardımlaşma Genel Prensipleri

Taraf devletler arasında adli yardımlaşmayı sağlayabilmek için Sözleşme'nin 25. maddesinde genel prensipler belirtilmektedir. 25. maddesinin 1. fıkrasına göre adli yardımlaşma taraf devletler arasında "mümkün olan en geniş biçimde" gerçekleştirilmesi gerekmektedir. Yani 23. maddede kapsamı geniş tutulan bu prensip adli yardımlaşma konusunda da geçerlidir. Buna göre adli yardımlaşma yükümlülüğü siber suçlara ve aynı zamanda delilleri dijital ortamda toplanmasını gerektiren geleneksel suçlara uygulanabilmektedir. Fakat 34. ve 35. maddelerde taraf devletlerin bu hükümleri uygulamasında faklı bir yaklaşım benimseyebileceği belirtilmiştir.

Söz konusu adli yardımlaşmanın yükümlülüğü yürürlükte olan sözleşmeler, yasalar ve düzenlemelerde aranan koşular çerçevesinde gerçekleşmek gerekliliği açıktır. Taraf devletler 29. - 35. maddelerdeki tedbirler başta olmak üzere Sözleşme'de öngörülen tüm mekanizmaları yerine getirmek için gereken hukuki temeli sağlamalıdır[492]. Adli yardımlaşamaya ilişkin yasalarında yeterli esnekliğe sahip olan devletler Sözleşme'deki doğrudan uygulanabilir hükümleri yerine getirip bu konuda yeni bir mevzuat çıkarması gerekmemektedir. Aksi takdirde devletler söz konusu hükümleri yerine getirmek için adli yardımlaşmaya ilişkin yeni bir yasayı hızlı bir şekilde çıkarmakla yükümlüdür[493].

Sözleşme'nin 25. maddesinin 3. fıkrasında adli yardımlaşma taleplerinin iletilmesini kolaylaştıracak önemli bir hüküm öngörülmektedir. Buna göre taraf devletler acil durumlarda adli yardımlaşma taleplerini faks, e-mail veya başka hızlı bir iletişim aracılığıyla gerçekleştirecektir. Bunun nedeni elektronik verilerin geçici doğası ve hızlı bir şekilde silinebilmesi[494]ve bu tür suçların soruşturulmasının uzun

[492] Explanatory Report to the Convention on Cybercrime, par. 254, s. 44.
[493] Explanatory Report to the Convention on Cybercrime, par. 255, s. 44
[494] Grabosky**, a.g.m.**, s. 214.

sürmesidir[495]. Bu durum suçun takibini ve soruşturulmasını zorlaştırmaktadır. Bu yükümlülük hem talep hem de yanıt için geçerlidir. Sözleşmenin Açıklayıcı raporuna göre yavaş ve hantal olan geleneksel talep yöntemlerinin (yazılı , mühürlü belgeler v.s.) yerine hızlı elektronik yöntemlerle gerçekleştirilmesi gerekmektedir. Aynı zamanda talebe cevap verecek taraf devletin de söz konusu hızlı yolları izlemesi gerekmektedir. İletişim aracı olan Faks ve e-mail örnek olarak sayılmaktadır. Dolayısıyla taraf devletler uygun olan başka iletişim araçlarına başvurabilmektedir. Ayrıca ilerde ortaya çıkacak daha gelişmiş iletişim araçları da adli yardımlaşma taleplerinde kullanılabilecektir. Ancak burada önemli olan husus güvenlik ve doğruluk koşullarının sağlamış olmasıdır. Taraf devletler kendi aralarında şifreleme dahil olmak üzere iletişim sürecinin doğruluğunu sağlayacak tedbirleri alabilmektedirler. Fakat daha sonra da talebin onayını resmi yöntemlerle teyit edilebilecektir[496].

Adli yardımlaşma genel prensip olarak taraf devletler arasındaki sözleşmelerin ve ulusal yasaların hükümleri kapsamında yürütülecektir. Ancak 4. fıkrada geçen "bu bölümde aksi açıkça belirtilen durumlar" ifadesi, söz konusu prensiple ilgili bir çok kısıtlamanın bulunduğu anlamına gelmektedir. Bunların ilki 25. maddenin 2. fıkrasında taraf devletlerin arasında mevcut sözleşmelere, eşdeğerdeki düzenlemelere veya ulusal yasalara bakılmaksızın diğer maddelerde yer alan işbirliği koruma, arama ve el koyma, verilerin gerçek zamanda toplanması, 7/24 iletişim ağının kurulması gibi mekanizmaları düzenleme yükümlülüğü belirtilmektedir. İkinci kısıtlama adli yardımlaşma talepleriyle ilgili sözleşme veya eşdeğer düzenleme olmadığı durumlarda talep edilen devletin yasası uygulanmak yerine 27.maddede düzenlenen prosedürler uygulanacaktır. 4. fıkrada öngörülen özel istisna Sözleşme'nin 2.-11. maddelerinde sayılan suçların sadece mali suçlar olarak nitelendirilmesi nedeniyle reddedilmeyecektir. Son kısıtlama ise 29. maddedeki bilgisayar verilerinin korunması çifte cezalandırılabilirlik şartına dayanarak reddedilmeyecektir[497].

[495] Gercke, **a.g.e.**, s. 288.
[496] Explanatory Report to the Convention on Cybercrime, par. 256, s. 45.
[497] Calderoni, **a.g.m.**, s. 348.

25. maddenin 5. fıkrasında ise çifte cezalandırılabilirliğinin tanımı ortaya konulmaktadır. Buna göre eylemin talep edilen taraf devletin yasasında faklı bir suç kategorinde yer alarak veya başka bir terimle ifade edilerek suç oluşturması halinde çifte cezalandırılabilirlik koşulu sağlanmış olacaktır. Diğer anlatımla söz konusu çifte cezalandırılabilirliği koşulunun gerçekleştirilmesi için eylemin maddi unsurları her iki taraf devletlerin yasal sistemlerinde suç teşkil etmesi yeterlidir[498]. Öte yandan taraf devletlerin 2.-11. maddelerde yer alan suçları iç yasalarında düzenlemesi gerekmektedir. Dolayısıyla bu noktada çifte cezalandırılabilirlik koşulu sağlanmış durumdadır[499]. Ayrıca çifte cezalandırılabilirlik koşulunun kapsamı geniş tutulmakla birlikte adli yardımlaşma işlemlerini kolaylaştıracak şekilde uygulanmalıdır.

Belirtilmesi gerekir ki Sözleşme, siber suçlarla mücadelede sorunlara çözüm getirmek için adli yardımlaşmaya ilişkin ayrı bir sistem oluşturmamakta ve bundan dolayı eleştirilmektedir[500]. Ancak adli yardımlaşmaya ilişkin mevcut sözleşmelerin ve düzenlemelerin dışında ayrı bir sistem oluşturulması pratik bakımından tercih edilmiş bir yöntem değil aynı zamanda böyle bir siber suçlarla ilgili yeni bir sistem kurulması karışıklığa neden olabilmektedir. Dolayısıyla Sözleşme'de mevcut adli yardımlaşma sisteminde bulunan sorunları çözmeye ve dijital ortamda siber suçların kavuşturulmasını kolaylaştırmaya çalışılmaktadır[501].

3.2.3.2. Kendiliğinden Bilgi Verme

Bazen Sözleşme'de düzenlenen suçların soruşturmasına veya soruşturmasının başlatılmasına yardımcı olabilecek ve bunu devletin bilmediği diğer taraf devlette önemli bilgiler bulunabilmektedir. Bu halde adli yardımlaşma talep edilmez. Söz konusu durumu düzenleyen 26. maddenin 1.fıkrasına göre taraf devletin suçun

[498] Önok, **a.g.m.**, s. 1252.
[499] Council of Europe, Project on Cybercrime, International Co-operation under the Convention on Cybercrime, 2009, s. 4.
[500] Weber, **a.g.m.**, s. 241; Calderoni, **a.g.m.**, s. 348.
[501] Mücahid Özbek, "Avrupa Siber Suçlar Sözleşmesi Çerçevesinde Adli Yardımlaşma", **Galatasaray Üniversitesi Sosyal Bilimler Enstitüsü Yayımlanmamış Yüksek Lisans Tezi,** İstanbul, 2015, s. 125.

soruşturmasında önemli olduğunu düşündüğü bilgileri önceden adli yardımlaşma talebi olmaksızın ulusal hukuku bağlamında soruşturma yürüten devlete iletebilmektedir. Ancak bilgilerin bulunduğu devlet bu konuda takdir yetkisine sahip olmakla birlikte bu bilgileri diğer devlete sunmak zorunda değildir[502].

Söz konusu bilgilerin "hassas" olması halinde taraf devlet bu bilgilerin gizli tutulması veya kullanımıyla ilgili şartlar koyabilmektedir. Bunu nedeni bazı durumlarda bilgilerin ifşa edildiğinde bilgiyi ileten taraf devletin önemli menfaatleri tehlikeye maruz kalabilmektedir[503]. Örneğin bir suç grubu hakkında soruşturma başlatıldığının veya bilgi toplama aracının gizlenmesi gereken durumlarda "hassas" bilgi olarak değerlendirilebilmektedir. Bu gibi durumları bilgi veren taraf devletin diğer devlete bildirmesi gerekmektedir. Diğer tarafın bunu kabul etmemesi halinde bilginin bulunduğu taraf devlet bilgiyi vermeme hakkına sahip olacaktır [504].

3.2.4. Adli Yardımlaşmaya İlişkin Geçerli Uluslararası Sözleşmelerin Olmadığı Durumlarda Uygulanacak Prosedürler

Sözleşme'nin 27. maddesinde taraf devletler arasında adli yardımlaşmaya ilişkin sözleşmelerin ya da eş değer düzenlemelerin olmadığı durumlarda uygulanması gereken usulleri detaylı bir şekilde düzenlenmektedir. 1. fıkrada yine genel prensip olan adli yardımlaşmanın taraf devletler arasındaki mevcut sözleşmeler veya düzenlemeler çerçevesinde gerçekleşmek gerekliliği tekrar vurgulanmaktadır. Avrupa Konseyi'ne taraf devletler arasında adli yardımlaşmaya ilişkin birçok sözleşme bulunmaktadır. Fakat Avrupa Konseyi dışında olan bir devlet bu sözleşmelere taraf olmamaktadır. Bu durumda 27. maddede yer alan prosedürler uygulanacaktır. Devletler aralarındaki akdedilen adli yardımlaşmaya ilişkin sözleşmeler mevcutsa uygulamaya devam edeceklerdir[505]. Ancak devletler arasında uygulanacak bir

[502] Vatis, **a.g.m.**, s. 215.
[503] Explanatory Report to the Convention on Cybercrime, par. 261, s. 46.
[504] Gercke, **a.g.e.**, s. 289.
[505] Downing, **a.g.m.**, s. 761.

antlaşma olmaması durumunda ikincil röle sahip olan iş bu Sözleşme'nin 27. maddesi'nde getirilen hükümler geçerli olacaktır[506].

2. fıkrada adli yardımlaşma talepleri gerçekleştirmek, bu taleplere yanıt vermek veya bunla ilgili gereken hukuki işlemleri yapacak makam ya da makamların belirlenmesi yükümlülüğü getirtilmektedir. Bu makamlar siber suçlarla mücadelede oldukça önemli rol oynamaktadır. Aralarında doğrudan bağlantı kurabilir olan makamlar klasik kanallardan daha hızlı ve etkin bir araçlardır[507].

3. fıkraya göre yardımlaşma talebi talep edilen devletin yasalarında öngörülen usullere aykırı olmaması şartıyla talep eden devletin belirlediği usuller uyarınca yerine getirilecektir. Bu hükmün amacı delil elde etme sürecinin talep eden devletin ilgili yasasına uygun olmasını ve neticede mahkemelerde kullanılmasını sağlamaktır. Ancak bu yükümlülük sadece teknik prosedürlerle ilgili durumlarda geçerli olacaktır. Örneğin, talep eden taraf devlet, talep edilen devletin yasallarına aykırı bir şekilde arama veya el koyma gibi işlemler gibi temel konularla ilgili talepte bulunamaz. Ayrıca bazı durumlarda talep eden devletin iç yasasına göre kabul edebilirliğini sağlamak için bazı koşullar aramaktadır. Örneğin tanığın ifadesi yemin şartıyla alınması gibi durumlarda talep reddedilmeyecektir[508].

4. fıkrada adli yardımlaşma taleplerinin reddinin iki nedenine yer verilmektedir. Bunların ilki talebin konusu talep edilen taraf devletin siyasi suç veyahut siyasi suçla ilgili bir suç olarak değerlendirmesi, ikincisi ise talebin yerine getirilmesi kendisinden talep edilen devletin egemenliğinin, kamu düzeninin, güvenliğinin veya diğer temel menfaatlerinin zarara maruz kalma ihtimali bulunmasıdır. Ancak maddede geçen "diğer temel menfaatleri" ifadesinin dar bir şekilde yorumlanması gerekmektedir[509]. Ayrıca taraf devletler arasında işbirliğinin 23.

[506] Önok, **a.g.m.**, s. 1253, Gercke, **a.g.e.**, s. 289.
[507] Keyser, **a.g.m.**, s. 318.
[508] Explanatory Report to the Convention on Cybercrime, par. 267, s. 48.
[509] Gercke, **a.g.e.**, s. 319.

ve 25. maddelerdeki "en geniş biçimde gerçekleştirilmesi" prensibi doğrultusunda söz konusu ret nedenlerine dar ve ölçülü bir biçimde başvurmaları gerekmektedir[510].

Talep edilen devlet taleple ilgili gereken işlemleri yerine getirmesinin kendisinde yürütülmekte olan ceza soruşturma veya kavuşturmasına zarar vermesi veya engel olması halinde, 5. fıkraya göre taleple ilgili işlemleri erteleyebilmektedir. Nitekim 6. fıkra uyarınca talep edilen devletin talebi ret etme veya erteleme hakkını kullanmadan önce talep eden devletle danışarak talebi kısmen veya koşullara bağlı olarak yerine getirebilmektedir.

7. fıkrada talep edilen devlete talebin sonucunu talepte bulunan devlete bildirme ve ret veya erteleme nedenleri açıklaması yükümlülüğü getirilmiştir. Ret ve erteleme nedenlerinin açıklanmasının amacı talep eden devletin talep edilen devletin talebi nasıl yorumladığını anlamasını, ilerde iki taraf devlet arasında işbirliğinin etkinliğini artırmasını ve talep eden devletin deliller ve tanıklar hakkında bilmediği bilgiler sağlamaktır[511].

Yukarda belirtildiği gibi taraf devletlerince belirtilen yetkili makamlar adli yardımlaşma taleplerini gerçekleştirmek üzere birbirleriyle doğrudan bağlantı kurabilmektedir. Ancak 9. fıkranın a. bendine göre acil durumlarda talepler adli yardım isteyen devletin hakim ve savcıları tarafından doğrudan muhatap devletin savcı ve hakimlerine iletilebilmektedir. Aynı zamanda bunu yapan hakim ve savcının muhatap devletin merkezi sorumlu makamlarına göndermek üzere kendi devletin merkezi makamına göndermesi gerekmektedir[512]. b. bendine göre söz konusu taleplerin İnterpol aracılığıyla gerçekleştirilebileceği belirtilmiştir. c. bendi uyarınca, a. bendine göre yapılan talebin makamın yetkisi dışında olması halinde, işbu makamın yetkili makama iletmesi ve bunun sonucu talep eden devlete bildirmesi gerekmektedir. Ayrıca talep eden devletin yetkili makamı d. bendi uyarınca merkezi makamın müdahalesi olmaksızın doğrudan talepler iletebilmektedir. Son olarak e. bendine göre

[510] Explanatory Report to the Convention on Cybercrime, par. 268, s. 48.
[511] Explanatory Report to the Convention on Cybercrime, par. 272, s. 49.
[512] Explanatory Report to the Convention on Cybercrime, par. 274, s. 49.

taraf devlet acil durumlarda etikliğini arttırmak maksadıyla yardım taleplerinin yalnızca merkezi makamlara iletilmek gerekliğini Avrupa Konseyi Genel Sekreterliğine bildirebilmektedir.

Gizlilik ve kullanımın sınırlandırılmasını düzenleyen 28. maddenin 2. fıkrasına göre talep edilen taraf devlet talebin yerine gerdirmek için iki sınırlandırma öngörebilmektedir. Bunların ilki verilerin veya materyallerin gizli tutulması (bu şartın olmaması durumunda talebin yerine gerdirilemeyeceği durumlarda) örneğin gizli bir bilgi kaynağı olduğu durumda. Mutlak gizlilik olması talep eden devletin yaptığı birçok suç soruşturma ve kavuşturmaya engel olabilmektedir[513]. Dolayısıyla burada gizlilik koşulunu çerçevesinin çizilmesi yerindedir. İkincisi ise talep eden taraf devletin bilgileri veya materyalleri talepte belirtilen soruşturma ve kavuşturma dışında kullanmamasıdır. Bu sınırlama şartının uygulanabilmesi için talepte açık bir şekilde ifade edilmesi gerekmektedir. 28. maddenin 3. fıkrası uyarınca talep eden taraf devletin bu şartları kabul etmemesi halinde talep edilen devlete bildirmesi gerekmektedir[514]. 28. maddenin 4. fıkrasına göre 2. Fıkrada yer alan sınırlama şartlarla yardım veren devlet talep eden devletten verilen bilgilerin ve materyallerin nasıl kullanıldığına dair açıklamalar talep edebilmektedir. Son olarak belirtilmesi gerekir ki Sözleşme'nin 28. maddenin hükümleri yalnızca taraf devletler arasında yürüklükte olan tek taraflı veya karşılıklı mevzuata dayanan adli yardımlaşmaya ilişkin sözleşme veya düzenlemeler olmadığı durumlarda geçerli olacaktır.

3.2.5. Adli Yardımlaşmayla İlgili Özel Hükümler

Sözleşme'nin ikinci kısmında (16. -21.m) yer alan taraf devletlerin ulusal düzeyde alması gereken siber suçun soruşturması ve kavuşturmasını geliştirecek birtakım tedbire yer verilmemiştir. Ancak söz konusu bu tedbirler devletlerin egemenliği ilkesi uyarınca yalnızca devletler içinde uygulanabilmektedir. Bu durum sınır ötesi (sınır dışında delillerin toplanması gibi) işlemler gerektiren siber suçların

[513] Explanatory Report to the Convention on Cybercrime, par. 277, s. 49.
[514] Explanatory Report to the Convention on Cybercrime, par. 278, s. 50.

soruşturmasını engelleyebilmektedir. İşte özel hükümler kısmı bu durumu düzenlemektedir[515]. Dolayısıyla Uluslararası işbirliğiyle ilgili özel hükümler, Sözleşme'nin ikinci kısmında yer alan tedbirlerin yansımasıdır[516]. Sözleşme özel hükümleri geçici tedbirlere ilişkin adli yardımlaşma ve soruşturma yetkilerine ilişkin adli yardımlaşma olmak üzere ikiye ayırmıştır.

3.2.5.1. Geçici Tedbirlerin Alınmasına İlişkin Adli Yardımlaşma

Geçici tedbirler olarak adlandırılan depolanmış bilgisayar verilerinin hızlı bir şekilde korunması (29. m) ve açıklanmasına (30. m) ilişkin adli yardımlaşma siber suçların soruşturma sorunlarını çözmeye yönelik Sözleşme'nin uluslararası işbirliği hükümlerinin en önemli kısmını teşkil etmektedir. Sözleşme'nin genel prensibi olarak adli yardımlaşma mevcut sözleşmelere göre gerçekleştirilmekte ve yalnızca sözleşmeler olmadığı durumlarda bu Sözleşme'ye başvurulmalıdır. Ancak söz konusu geçici tedbirler ayrı tutulmakla birlikte taraf devletler arasında adli yardımlaşmaya ilişkin sözleşmeler olsa bile Sözleşme'nin öngördüğü hükümler çerçevesinde gerçekleştirilecektir. Örneğin, bu tedbirlerle ilgili taleplerin Sözleşme'de belirtilen iletişim 7/24 iletişim noktası gibi araçlarıyla iletileceğidir[517].

3.2.5.1.1. Depolanmış Bilgisayar Verilerinin Hızlı Bir Şekilde Korunması

29. maddede düzenlenen işbu tedbir 16. maddede öngörülen ulusal düzeydeki hükmün yansımasıdır. Taraf devlet, diğer devlette bulunan bilişim sisteminde depolanan verilere ilişkin illerde adli yardımlaşma (el koyma gibi) talebi gerçekleştirmek maksadıyla verilerin korunmasını acil bir şekilde ilgili devletten talep edilebilmektedir. Yukarıda belirtildiği gibi veriler geçici bir niteliğe sahip olup çok

[515] Gercke, **a.g.e.**, s. 290.
[516] Önok, **a.g.m.**, s. 1256.
[517] Özbek, **a.g.m.**, s. 133.

hızlı ve geri dönüşü olmayan bir şekilde silinebilmektedir. Dolayısıyla bu tedbirin amacı uzun süren geleneksel resmi adli yardımlaşma yöntemleri sürecinde korumasıdır[518]. Bu tedbir geleneksel adli yardımlaşma yöntemlerine göre daha hızlı olmasıyla birlikte bireylerin haklarına ve özgürlüklerine müdahale etmemektedir. Bu anlamda muhatap devletin yetkili mercilerinin müdahalesi olmadan hizmet sağlayıcıların elinde bulunan verilerin koruması (silmemesi) ve daha sonra yetkili makamlara teslim etmesidir[519].

2. fıkrada verilerin hızlı bir şekilde korunması talebinin içermesi gereken minimum bilgiler belirtilmektedir. Bunlar talebi gerçekleşen makam, talebin konusu olan suçla ilgili temel hususların özeti, korunması talep edilen verilerin suçla ilgisi, verilerin olduğu kişi veya bulunduğu sistemle ilgili herhangi bilgi, verilerin koruması gerekliliği nedenleri ve bu talepte bulunana taraf devletin ilerde korunacak veriler hakkında adli yardımlaşma talep edeceğidir. Ancak bu talep geçici olup hızlı bir şekilde hazırlanmalı ve iletilmelidir[520].

3. fıkraya göre genel bir kural olarak verilerin hızlı bir şekilde korunması talebine yanıt verebilmek için çifte cezalandırılabilirlik koşulu aranmamaktadır. Bunun nedeni verileri koruma tedbirinin bireylerin kişisel verilerine veya özel hayatına bir müdahale teşkil etmemesi ve ayrıca çifte cezalandırılabilirlik koşulunun çok uzun sürebilen tespit sürecinde söz konusu veriler kaybolabilmesidir[521]. Ancak 4. fıkra uyarınca 2. -11. maddeler arasında düzenlenen suçlar dışında taraf devlet çift cezalandırabilirdik koşulunun sağlanmaması gerekçesiyle verilerin hızlı bir şekilde korunma talebini reddedebilmektedir. Pratik bir ifadeyle çifte cezalandırılabilirlik koşulu sadece 2.-11. maddelerde yer alan suçlar bakımından aranmamaktadır.

Buna ek olarak 5. fıkrada talebin ret nedenleri sınırlı bir biçimde belirtilmiştir. Bunların ilki yardım talebine konu olan suç talep edilen devletin siyasi veya siyasi bir suçla bağlantılı suç olarak değerlendirmesi, ikicisi ise talebin yerine getirilmesini talep

[518] Palmer, **a.g.m.**, s. 5.
[519] Explanatory Report to the Convention on Cybercrime, par. 283, s. 51.
[520] Vatis , **a.g.m.**, s. 215; Explanatory Report to the Convention on Cybercrime, par. 284, s. 51.
[521] Explanatory Report to the Convention on Cybercrime, par. 285, s. 51.

edilen devletin ulusal güvenliğine, egemenliğine, kamu düzenine veya diğer temel menfaatlerine zarar vermesine neden olabilmesidir.

Talep edilen taraf devlet talebin uygulanması sonucunda talep eden devlet tarafından yürütülen suç soruşturması veya kavuşturmasının gizliliğine veya başka bir şekilde zarar verebilecek durumlar fark edebilmektedir. 6. fıkraya göre talep edilen devletin söz konusu bu durumları adli yardımlaşma diğer seçenekleri ışığında değerlendirmek üzere talep eden devlete hemen bildirmesi gerekmektedir.

7. fıkrada hızlı bir şekilde korunması gereken verilerin en az 6o gün muhafaza edilmesi gerekmektedir. Bunun amacı asıl yapılması gereken adli yardımlaşma talebinin hızlı bir şekilde gerçekleşmesini sağlamaktır[522]. Adli yardımlaşmayla ilgili karar alınıncaya kadar verilerin korunma süreci devam edecektir.

3.2.5.1.2. Korunan Trafik Verilerinin Hızlı Bir Şekilde Açıklanması

Sözleşme'nin 17. maddesinde ulusal düzeyde öngörülen hükmün adli yardımlaşmadaki karşılılığı olarak 30. maddede düzenlenmiştir. Talep edilen devlet 29. madde doğrultusunda iletilen verilerin korunmasına ilişkin talebi yerine getirirken başka bir devlette bulunan hizmet sağlayıcının verilerinin iletme sürecine dahil olduğu tespit edilebilmektedir. Bu durumda 30. maddenin 1. fıkrasına göre talep edilen devletin hizmet sağlayıcının kimliğini ve verilerin aktarılmasında izlediği yolun belirlenmesine yardımcı olacak bilgileri hızlı bir şekilde açıklaması gerekmektedir. Verileri birçok devletten geçebilmektedir. Dolayısıyla bu tedbir talepte bulunan devletin hizmet sağlayıcının kaynağını diğer devletlerde takip etmesini sağlayacaktır[523].

Söz konusu bu bilgiler siber suçların tespitinde ve delillerin toplanmasında oldukça önemlidir. Dolayısıyla 2. fıkrada verilerin açıklanma işlemlerini reddetme

[522] Önok, **a.g.m.**, s. 1257.
[523] Council of Europe, Project on Cybercrime, International Co-operation under the Convention on Cybercrime, s. 8.

nedenleri (29. Maddede olduğu gibi) sınırlı bir biçimde sayılmıştır[524]. Bunların ilki yardım talebine konu olan suç talep edilen devletin siyasi veya siyasi bir suçla bağlantılı suç olarak değerlendirmesi, ikicisi ise talebin yerine getirilmesi talep edilen devletin ulusal güvenliğine, egemenliğine, kamu düzenine veya diğer temel menfaatlerine zarar vermesine neden olabilmesidir.

3.2.5.2. Soruşturma Yetkilerine İlişkin Adli Yardımlaşma

Bu kısımda düzenlenen bilgisayarda depolanmış verilere erişim, verilere sınır ötesi erişim, trafik verilerin gerçek zamanda toplanması ve içerik verilerin el konulması konularında adli yardımlaşma Sözleşme'nin 23. maddesinde yer alan genel prensipleri çerçevesinde gerçekleştirilecektir. Yani 31.-34. maddelerdeki soruşturma yetkilerine ilişkin adli yardımlaşmada taraf devletler arasında adli yardımlaşmaya ilişkin sözleşmeler veya tek taraflı ya da karşılıklı mevzuatlar geçerlidir. Ancak bu hükümlerin devletler arsında mevcut sözleşmeler veya mevzuatlarda yer almaması durumunda Sözleşme'nin getirdiği hükümler uygulanacaktır[525]. Dolayısıyla yukarda da açıklandığı gibi işbu Sözleşme'de adli yardımlaşmaya ilişkin yeni bir sistem tasarlanmamakla birlikte mevcut adli yardımlaşma sisteminin siber suçlarla mücadele bakımından eksikliklerine ve açıklıklarına çözüm getirilmeye çalışılmaktadır.

3.2.5.2.1. Bilgisayarda Depolanmış Verilere Erişim

Bu tedbir Sözleşme'nin 19. maddesinde ulusal düzeyde öngörülen hükümle paralel olarak düzenlenmektedir. 31. maddenin 1. fıkrasına göre taraf devlet diğer tarafta bulunan bilişim sistemi aracılığıyla depolanan verilerin aranması, el konulması, bu verilere erişilmesi veya benzer bir şekilde verilerin güvence altına alınması için ilgili taraf devletten adli yardımlaşma talebinde bulunabilmektedir. 2. fıkrada talep

[524] Explanatory Report to the Convention on Cybercrime, par. 291, s. 52.
[525] Özbek, **a.g.m.**, s. 139.

edilen taraf devletin bunu sağalabilecek durumda olması gerekliliği belirtilmektedir[526]. 3. fıkrada ise bu talebe hızlı bir şekilde yanıt verilmesi gereken iki durum belirtilmektedir. İlki verilerin kaybolmasına veya değiştirilmesine neden olabilecek gerekçelerin olduğu durumlar, ikincisi mevcut sözleşme ya da düzenlemede öngörülen durumlardır.

3.2.5.2.2. Depolanmış Verilere Sınır Ötesi Erişim

Depolanmış verilere sınır ötesi erişim, bir devlet tarafından başka taraf devlette bulunan bilişim sistemlerinde depolanan verilere daha önce ilgili devletten izin veya adli yardımlaşma talep edilmeksizin erişilmesidir[527]. Depolanmış verilere sınır ötesi tek taraflı olarak erişim düzenleyen 32. madde Sözleşme'nin en çok tartışılan maddesidir[528]. Dolayısıyla Sözleşme'yi kaleme alanlar tarafından bu konu ayrıntılı bir şekilde ele alınmıştır. Buna göre sınır ötesi erişime sadece iki durumda imkân verilmiştir. Birincisi depolanan verelerin kamuya açık olması "açık kaynak" durumundadır. Taraf devlet herkes tarafından kullanılabilen ve herhangi bir yerde bulunan verilere herhangi bir izne veya başvuruya ihtiyaç duymadan erişebilmektedir. Örneğin kamuya açık bir internet sitedeki bulunan verilere erişilmesidir[529]. İkincisi ise kamuya açık olamayan ve diğer taraf devlette bulunan bilişim sisteminde depolanan verilerin erişimini sağlamak için verileri açıklama yetisine hukuken sahip kişinin yasal ve gönüllü rızasının alınması durumundadır.

32. maddenin b. bendinde düzenlenen ikinci durum oldukça önemli ve ciddi eleştirilere maruz kalmaktadır. Bir taraf ülkenin ilginin onayını sağlamak suretiyle başka bir ülkede, o ülkenin yetkili makamlarından soruşturma yapmak için izin almadan soruşturma yapması durumunda sadece bireylerin hakları söz konusu değil[530], uluslararası hukukun temel ilkelerinden biri olan devletlerin ulusal egemenliğine de

[526] Explanatory Report to the Convention on Cybercrime, par. 292, s. 52.
[527] Özbek, **a.g.m.**, s. 140.
[528] Vatis, **a.g.m.**, s. 216.
[529] Önok, **a.g.m.**, s. 1258.
[530] Gercke, **a.g.m.**, s. 119.

aykırı[531] bir durum teşkil edebilmektedir[532]. Bu halde Sözleşme'yi onaylayan devletin buna razı olduğunu söylemek mümkündür[533]. Dolayısıyla bazı devletler Sözleşme'yi onaylayıp bu maddeye çekince koymaktadırlar. Diğer yandan 32. maddenin b. bendinde suçun soruşturulmasına ilişkin herhangi bir prosedür öngörülmemektedir. Böyle sınırlamalar 2000 yılında sunulan Sözleşme taslağında bulunmuş, ancak daha sonra 22. taslak metininden kaldırılmıştır[534].

3.2.5.2.3. Trafik Verilerin Gerçek Zamanda Toplanması

Siber suçluların tespit edilmesi için en önemli yolu hizmet sağlayıcıda kaybedilen verilerin takip edilmesidir. Ancak söz konusu veriler kaybedilmeden önce hizmet sağlayıcı tarafından silinebilmektedir. Dolayısıyla Sözleşme'nin 33. maddesinde bu durumu telafi edebilmek için talep edilen taraf devlete talepte bulunan devlet için verileri gerçek zamanda toplama yükümlülüğü getirilmiştir. Bu hükmün amacı siber suçlunun çevrimiçiyken tespit edilmesini sağlamaktır. İşbu konuyla ilgili adli yardımlaşma talepleri mevcut sözleşmelerde ve ulusal hukukta öngörülen usuller çerçevesinde yerine getirilecektir. Maddenin 2. fıkrasına göre bu hükmün uygulama kapsamı ulusal düzeyde benzer davalarda kapsamından daha dar olamamalıdır. 2. fıkrada geçen "en az" ifadesi taraf devletler arasında adli yardımlaşmanın (çift cezalandırabilirlik koşulu olmasa bile) mümkün olan en geniş biçimde gerçekleştirilmek gerektiği anlamına gelmektedir[535].

34. maddede taraf devletlerin içerik verilerin denetlemesi ve kaybedilmesi konusunda, mevcut sözleşmelerin veya ulusal mevzuatların izin verdiği ölçütte, adli yardımlaşama sağlamaları gerektiği belirtilmektedir. Özel hayata müdahale teşkil eden bu konuyla ilgili yeni hükümler getirilmemiştir. Sözleşme'yi kaleme alanlar bu konuda

[531] Bazı yazarlara göre nedenle Rusya Sözleşme'yi imzalamamıştır. Vatis, **a.g.m.**, s. 218
[532] Gercke, **a.g.e.**, s. 291; Osula, **a.g.m.**, s. 55.
[533] Önok**, a.g.m.**, s. 1259.
[534] Gercke, **a.g.e.**, s. 292.
[535] Explanatory Report to the Convention on Cybercrime, par. 296, s. 53.

sadece mevcut sözleşmeler ve ulusal mevzuata yollama yapmakla yetinmektedirler[536]. Diğer yandan talep edilen devletin içerik veriler konusunda yardım sağlamayı engelleyen yargı yetkisi gibi durumları olabilmektedir. Dolayısıyla taraf devlet bu noktada talebi yerine getirmek zorunda değildir[537].

3.2.6. 7/24 İletişim Noktası

35. maddede taraf devletlere aralarında siber suçların soruşturması ve kavuşturmasında veya delillerin dijital ortamda toplanmasında yardımlaşma sağlamak üzere 7 gün 24 saat çalışacak bir iletişim noktası kurma yükümlülüğü getirilmektedir. Sözeleşme'de bu hükmün öngörülmesi G-7 tarafından 1997 yılında tesis edilen iletişim noktası[538] düşüncesinden türetilmiştir[539]. İşbu iletişim noktası amacı siber suçlarla ilgili iletişim sağlamak ve söz konusu suçların soruşturması ve kavuşturmasını hızlandırmaktır[540]. Dolayısıyla böyle bir iletişim noktası kurulması Sözleşme'nin öngörülen temel amaçlarına uygun[541]olup uluslararası işbirliğinin klasik yöntemlerinin yetersiz kaldığından siber suçlarla mücadelenin etkin ve hızlı bir şekilde yürütülmesi için büyük önem arz eden bir araçtır[542]. Aynı zamanda böyle bir iletişim noktası kurulması ve diğer devletlerle paylaşılması için Sözleşme'ye katılmak gerekmemektedir[543].

İletişim noktasının işlevi 35. maddenin 1. fıkrası uyarıca teknik danışmanlık sağlamak, 29. ve 30. maddeler uyarıca verileri korumak, delileri toplamak, hukuki bilgiler sunmak ve şüphelilerin yerlerini tespit etmektir. Hukuki bilgilerden maksat resmi veya resmi olmayan işbirliği sağlamak için gereken şartlar konusunda

[536] Önok**, a.g.m.**, s. 1259.
[537] Vatis, **a.g.m.**, s. 218, Gercke, **a.g.e.**, s. 292.
[538] Bkz: bu çalışma, s. 55.
[539] Önok, **a.g.m.**, s. 1260; Calderoni, **a.g.m.**, s. 349.
[540] Gercke, **a.g.e.**, s. 292; Csonka, **a.g.m.**, s. 496. Explanatory Report to the Convention on Cybercrime, par. 298, s. 54.
[541] Explanatory Report to the Convention on Cybercrime, par. 298, s. 54.
[542] Oerlemans, **a.g.e.**, s. 60.
[543] Gercke, **a.g.e.**, s. 292

danışmanlık vermektir[544]. Ayrıca 2. fıkrada iletişim noktası diğer taraf devletlerdeki iletişim noktalarıyla hızlı iletişim sağlayacak kapasiteye sahip olmasını zorunlu kılmıştır. Yani söz konusu ağın teknik bakımından görevlerini yapabilecek şekilde donatılması ve ilgili personelin bu noktada uzman olması gerekmektedir.

[544] Explanatory Report to the Convention on Cybercrime, par. 298, s. 54.

SONUÇ ve ÖNERİLER

Siber suçlar internet ve bilişim teknolojisinin ortaya çıkmasıyla birlikte kendisini göstermeye başlamıştır. Gün geçtikçe inanılmaz bir hızla gelişen bilgisayar ve bilişim teknolojilere paralel olarak siber suç yeni tiplerle ve daha karmaşık araçlarla karşımıza çıkmaktadır. Özellikle hâlihazırda geliştirilen ve dünyada internetten sonra ikinci teknik devrim olacak olan yapay zeka, 5G, Blockchain ve Bitcoin, teknolojileriyle siber suçlar bütün devletlerin ilk öncelikleri haline gelecektir. Bu suçlarla mücadele devletler arasında işbirliğinin ve koordinasyonun önemini daha da artıracaktır.

Yeni bir kavram olması ve devamlı bir şekilde gelişmesi nedeniyle siber suçun terimlerine, tanımına ve sınıflandırılmasına ilişkin herhangi bir görüş birliği sağlanamamaktadır. Siber suçu ifade edebilmek için dünya çapında birçok terim kullanılmaktadır. İngiliz, Türk ve Arap doktrininde farklı terimler kullanılmakta ve bu noktada herhangi bir uzlaşma sağlanamamaktadır. Siber suçun tanımı ise herhangi bir ulusal ya da uluslararası mevzuata bulunmamaktadır. Yine İngiliz, Türk ve Arap doktrininde uzun tartışmalara neden olan bir konu olup üzerinde hiçbir fikir birliği sağlanamamaktadır.

Doktrinde siber suçla ilgili yapılan bütün çeşitli tanımların ortak noktası siber suçun bilişim sistemi veya diğer bilişim teknoloji araçları vasıtasıyla ya da bunlara karşı veya bilişim sisteminin içeriğine karşı işlenmektedir. Dolayısıyla bu şekilde genel ucu açık bir tanım yapmakta yarar vardır.

Uluslararası ve ulusal mevzuatlarda bu konuda izlenen yol siber suç tanımı yapmak yerine siber suçu teşkil eden eylemlerin dikkatli bir şekilde sayılması ardından söz konusu eylemlerin birer birer tanımı yapılmasıdır. Siber suç kavramın kapsadığı fiilleri belirlemekte fikir birliği sağlamak daha kolay görülmektedir. Bu yaklaşım 2001 Avrupa Konseyi Siber Suç Sözleşmesi ve 2004 Birleşmiş Milletler Yolsuzlukla Mücadeleye İlişkin Sözleşmesi tarafından tercih edilmiştir. Bunun nedeni, üye

devletlerin arasında ortaya çıkacak terim ve tanım farklığının üstesinden gelinebilmesi ve sözleşmeye mümkün olduğunca daha çok katılım sağlamasının amaçlamasıdır.

Siber uzayda siber suçun yanında birçok hukuka aykırı farklı eylem işlenebilmektedir. En önemlileri arasında siber terörizm, siber savaş ve siber saldırı vardır. Bu kavramlar uluslararası hukukta tanımı bulunmamakla birlikte siber suçtan ayrı tutulması gerekmektedir. Siber suç, siber terör ve siber savaş kavramların arasında fail, etki, amaç ve hukuk statüsü bakamından farklıklar bulunmaktadır. Siber saldırı ise söz konusu faktörlere göre siber suç, siber terör ve siber savaş kavramları içinde değerlendirilebilmektedir.

Siber suçlara karşı durmak gerekliliğinin farkındalığına erken varan devletler ve uluslararası ilgili örgütler, siber suçlarla mücadele etmek adına uluslararası ve bölgesel düzeyde girişimlerde bulunmaktadırlar. Uluslararası organizasyonların başında gelen BM siber suçlarla mücadele konusunda Genel Kurulu'nun birçok önemli kararı bulunmakta ve BM Ekonomik ve Sosyal Konseyi tarafından çalışmalar özellikle Suçun Önlenmesi ve Ceza Adaleti Kurultayı büyük önem taşımaktadır. Ancak BM'nin tüm çalışmaları ve girişimleri tavsiye niteliğinde olup siber suçlarla mücadelede istenilen sonuç sağlanmamaktadır. O nedenle son zamanlarda BM, üye devletlere teknik destek sağlamaya ve devletlerin bilişim altyapılarını geliştirmeye yönelik çalışmalar yürütmeye başlamıştır.

Yediler Grubu'nun 7/24 çalışan iler teknoloji suçlarıyla ilgili uluslararası iletişim ağ noktasını ilk olarak kurmasıyla etkin bir rol oynamıştır. Keza siber suçların önlenmesinde ulusal düzeyde tedbirlerin alınması ve uluslararası işbirliğinin gerçekleştirilmesi gerekliliğini vurgulayan on prensip kabul edilmiştir. Söz konu bu prensipler BM tarafından benimsenmiştir.

OECD, siber suçlarla mücadelede ve siber güveliğin korunması konusunda önemli adımlar atmıştır. OECD, uluslararası alanda siber suçlara ceza hukuku uygulama sürecinin sorunlarına ilişkin kapsamlı bir çalışma yürüten ilk kuruluştur. Akabinde OECD tarafından siber suçlarla mücadele birçok çalışmada ve öneride bulunmaktadır. Yumuşak hukuk (bağlayıcı olamayan) olan OECD'nin çalışmaların

siber suçlar konusunda gerek ulusal gerekse uluslararası farkındalık yaratmasında büyük önem arz etmektedir.

Siber suçlar en önemli önceliklerden biri hale getiren ITU ve İnterpol, tarafından siber suçlara karşı devletler arasında işbirliğini ve koordinasyon gerçekleştirmek ve desteklemek için bir sürü adım atılmıştır. Özellikle gelişmekte olan devletlerin teknik altyapılarını ve kapasitelerini siber suçlarla kaşı durabilecek dereceye getirmek için geliştirilmesinde aktif bir rol oynamaktadırlar.

Avrupa çapında yapılan düzenlemeler Avrupa Konseyi ve Avrupa Birliği olmak üzere ikiye ayırılmıştır. Uluslararası düzede yapılan ilk ve en önemli metin 2001 Avrupa Konseyi Siber Suç Sözleşmesi'dir. Sözleşme taraf devletlerin siber suçlarla ilgili ulusal maddi ve usul mevzuatlarını uyumlu hale getirmeyi ve siber suçlarla mücadele etmek üzere uluslararası işbirliği ve adli yardımlaşmaya ilişkin etkin ve hızlı araçlar geliştirmeyi amaçlamaktadır. Sözleşme maddi hukuka ve usul hukukuna ilişkin oldukça önemli hükümler içermektedir.

Avrupa Birliği tarafından siber suçlarla mücadele doğrultusunda Avrupa devletleri arasında işbirliği sağlamak ve ulusal yasaların yeknesaklaştırılması için adımalar atılmıştır. Özellikle 2009'de Lizbon Antlaşmasının yürürlüğe girmesiyle birlikte Avrupa Birliği'nin düzenlemeler yapma yetkisi daha da genişletilmiştir. Bu kapsamda Avrupa Birliği tarafından siber suçlara ilişin önemli birçok çerçeve karar ve direktif düzenlemiştir.

Arap bölgesinde siber suçların önlenmesine ilişkin devletler arasında işbirliği sağlamak maksadıyla birçok düzenleme bulunmaktadır. Birleşik Arap Emirlikleri Bilgi Teknolojisi Suçlarıyla Mücadelede Model (Yol Gösterici) Kanunu, Bilgi Teknolojisi Suçlarına İlişkin Arap Sözleşmesi 2010 ve Körfez Arap Ülkeleri İşbirliği Konseyi Bilgi Teknolojisi Suçlarıyla Mücadelede Yeknesak Yasa için Riyad Antlaşması'dır. Bütün bu düzenlemeler Arap bölgesindeki siber suç olgusu konusunda farkındalığı ve bu suçlarla mücadelede Arap devletler arasındaki işbirliğinin önemini yansıtmaktadır.

Afrika Birliği tarafından düzenlenen Siber Güvenlik ve Kişisel Verilerin Korunması Sözleşmesi büyük önem taşımaktadır. Sözleşme üye devletlere birçok yükümlülük getirmektedir. Bu noktada Afrika Birliği Sözleşmesi, Avrupa Konseyi Siber Suç Sözleşmesi'nin ötesine geçmektedir.

Siber suçlarla mücadele etmek amacıyla yapılan tüm ulus üstü düzenleme ve çalışmaların odak noktası bu suçlara karşı devletler arasındaki işbirliğinin ve koordinasyonun arttırılması ve siber suçlara karşı küresel bir mücadele sağlamak için devletlerin siber suçlarla ilgili ulusal esas ve usul yasaları arasında uyum sağlanmasıdır. Ayrıca önemli bir diğer nokta da siber suçlarla ilgili ortaya çıkan yargılama yetkisi problemlerine de çözümler üretilmeye çalışılmasıdır.

Siber suçların doğasında karmaşık bilişim teknolojileri aracılığıyla işlenmesi nedeniyle geleneksel ceza adalet sistemlerine aşina değildir. Bu suçların soruşturmasını ve kavuşturmasını zorlaştıran öne çıkan faktörler suçluların kimliklerini ve adreslerini gizlemesi, siber suçlarla ilgili delilerin elde edilmesi, değerlendirilmesi ve mahkemece kabul edilmesidir. Dolayısıyla bu suçlarla başa çıkmak için bilişim uzmanlığı gerekmektedir. Kaldı ki sınır aşan siber suçlar genellikle birçok ülkede işlenmesi ve söz konusu faktörler daha zor ve karmaşık hale gelmesinin yanında siber suçlara ilişkin yargı yetkisi zorluluğu meydana gelmektedir. Siber suçlar birden fazla devletin yetki alanına girmektedir. Bu noktada devletler arasında olacak siber uzayla ilgili yetki uyuşmazlıkları çözen uluslararası düzeyde bir ölçüt veya makam bulunmamaktadır. Yetki zorluklarını çözmek için devletler ulusal makaklarına başvurmaktadır.

Siber suçlarla mücadele uluslararası işbirliği olmazsa olmaz olarak vücut vermektedir. Ne var ki ceza konularında uluslararası işbirliğinin geçekleştirilmesinin çifte cezalandırılabilirlik ön koşuludur. Irak gibi siber suçları gerek ceza yasalarında gerekse ayrı bir yasayla hala düzenlemeyen birçok devlet bulunmaktadır. Böyle devletler siber suçular için güvenli bir sığınak teşkil etmektedirler. Yanı sıra devletlerin hem maddi hem de usul hukuk sistemlerinin farklılığı uluslararası işbirliğinin zorluklarının başında gelmektedir. Nitekim uluslararası işbirliği devletler

arası imzalanan ikili veya çoklu sözleşmelere dayanmaktadır. Ancak siber suçlar konusunda yapılan tüm sözleşmelerin bölgesel nitelikte olduğu görülmektedir. Her ne kadar kolay olmasa de, BM bünyesinde uluslararası bir sözleşme yapılması son derece önem arz etmektedir.

Avrupa Konseyi Siber Suç Sözleşmesi'nin siber suçlarla mücadelede karşılaşan zorlukların üstünden gelebilmek için usul hukuka ilişkin hükümleri çok önemli hükümler getirmektedir. Sözleşme siber suçlara ilişkin üye devletler arasında yeni bir adli yardımlaşma sistemi kurmamaktadır. Bunun yerine devletler arasında mevcut adli yardımlaşmaya ilişkin sözleşmelerin ve düzenlemelerin eksikleri ve boşluklarını tamamlamaya çalışılmaktadır. Doyasıyla Sözleşme'nin rolü ikincildir. Devletler arasında adli yardımlaşmaya ilişkin sözleşme veya düzenleme olmadığı durumlarda uygulanacak yedek hükümler getirmektedir. Bunun yanında 7/24 iletişim ağının kurulması Sözleşme'nin düzenlediği siber suçlarla mücadelede en etkin araçtır.

Son olarak Sözleşme'nin çekincelere büyük bir şekilde imkan sağlaması temel amacıyla bağdaşmamakta, siber suçların akıl almaz bir hızla gelişmesine karşı Sözleşme'de değişiklik yapma süreciyle ilgili zorunlu şartlara bağlanması, söz konusu gelişmelere ayak uydurulmamasına neden olabilmektedir. Buna karşın Sözleşme, siber suçlarla global mücadele sağlamak maksadıyla uluslararası hükümlere yer vermekte, Avrupa Konseyi üye devletlerle sınırlı olmamakla birlikte bütün devletlere açık olsa da, bölgesel nitelikte olarak kabul edilmektedir. Buna rağmen Sözleşme'nin siber suçlarla ilgili yapılan her türlü düzemeler için temel bir referans teşkil etmesinde, sınır aşan siber suçlarla mücadelede devletler arası işbirliği ve adli yardımlaşmaya zemin hazırlamasındaki rolü yadsınamaz.

Bu tezde belirtilen siber suçlarla mücadelede yaşanan zorlukların üstesinden gelmek maksadıyla hem ulusal hem de uluslararası düzeyde çözüm önerileri aşağıda yer almaktadır.

Ulusal Düzeyde:

a. Siber suçlarla mücadelenin temelde başlangıç noktası ceza ulusal kanunlarıdır. Siber suçlara ilişkin düzenleme olmadığında devletler siber

suçlular için güvenli sığınak teşkil etmektedir. Dolayısıyla devletlerin siber suçlarla ilgili ulusal maddi ve usul ceza yasaları siber suçların gelişimine paralel olarak düzenlemesi, geliştirmesi ve güncelleştirmesi gerekmektedir.

b. Suçu soruşturma ve kavuşturma klasik araçları siber suçlara karşı yetersiz kalmakta özellikle dijital ortamda delilerin elde edilmesi ve değerlendirilmesi noktasında bilişim uzmanlıkları gerekmektedir. Kolluk kuvvetleri siber suçların soruşturmasında ve kavuşturmasında yeni hızlı yöntemler geliştirmeli, teknik bakamından siber suçları önleyecek şekilde eğilmeli ve donatılmalıdır. Siber suçlarla mücadele özel teşkilatlar kurulmalıdır.
c. Devletler çeşitli bilişim altyapılarını geliştirmeli ve gerekli teknik tedbirleri almalıdır. Bu noktada siber alanda güvenliği ve gizliliği korumaya ve siber saldırıları önlemeye yarayacak kapsamlı projeler yürütülmeli ve stratejik planlar yapılmadır.
d. İşlenen siber suçların çoğu ihbar edilmemektedir. Bunun nedeni mağdur kişinin siber suça maruz kaldığını ve nasıl ihbar edeceğini bilmemesi, aynı zamanda bazı şirketlerin ve kurumların itibarlarının zedeleneceği düşünmesidir. Dolayısıyla siber suçlar hakkında ve bunu nasıl ihbar edileceği konusunda toplumsal farkındalık yaratmak için çalışmalar ve faaliyetler düzenlenmelidir.
e. Ulusal düzeyde kolluk kuvvetleri hem aralarında hem de özel sektörle birlikte etkin işbirliği gerçekleştirilmelidir. Özellikle internet hizmet sağlayıcılar verilere erişim sağlanmasında oldukça önemli ve kritik rol oynamaktadır. Hizmet sağlayıcı bir yandan kolluk kuvvetlerinin suçluların kimlik bilgilerini tespit etme sürecinde yardım sağlaması diğer yandan bireylerin haklarını ve gizliliğini koruması gerekmektedir.

Uluslararası Düzeyde:

a. Siber suçlarla mücadelenin başlangıç noktası ulusal hukuksa, çıkış noktası uluslararası hukukudur. Global suçluluk global mücadele gerektirmektedir. Ulusal hukuk sınır aşan siber suçlara karşı genellikle yetersiz kalmaktadır. Bu bağlamda uluslararası işbirliğini düzenleyen uluslararası düzlemde bağlayıcı bir sözleşmeye ihtiyaç duyulmaktadır. Bunun en önemli aracı Birleşmiş Milletlerdir.
b. Söz konu BM bünyesinde uluslararası sözleşmesinin düzenlenmesinin amacı devletlerin siber suçlarla ilgili maddi ve usuli yasaların yeknesaklaştırılması ve uyumlu hale getirilmesidir. Bu durumda uluslararası işbirliğinin ön koşulu olan çifte cezalandırılabilirlik koşulu gerçekleştirilmiş ve siber suçların soruşuma ve kavuşturma yöntemleriyle ilgili ülkeler arasında uyuşmazlığı ortadan kaldırılmış olacaktır.
c. Geleneksel uluslararası yöntemlerinin hantal ve uzun olması nedeniyle siber suçların doğasına uygun değildir. Siber suçlarla mücadele uluslararası işbirliğinin mekanizmalarının etkin, hızlı ve gelişmiş olası şarttır.
d. Sınır aşan siber suçlar genellikle birden çok devletin yetki alanında işlenebilmektedir. Bunun sonucunda ortaya çıkan yetki sorunu çözen uluslararası bir makam veya bir norm bulunmamaktadır. Siber suç Uluslararası Ceza Mahkemesi'nin yetki alnına girmediği görülmektedir. Bu konuda iki çözüm önerilebilmektedir. İlki siber suçun Uluslararası Ceza Mahkemesi'nin yetkili olduğu suçlar olan savaş, insanlığa karşı, soykırım ve saldırı suçlarına beşinci suç olarak eklenmesidir. Diğeri ise Uluslararası Ceza Mahkemesi'ne benzeyen siber suçlarla ilgili özel uluslararası düzeyde bir mahkeme kurulmasıdır. Her iki durumunda söz konusu siber suçlarla ilgili yetki sorunu kökten çözülmüş olacaktır.
e. Devletler arasında sadece adli işbirliği değil, aynı zamanda polisiye işbirliği de gerçekleştirilmelidir. Polisiye işbirliği konusunda aktif rol

oynayan mekanizmalar INTERPOL, EUROPOL, ASEANAPOL ve AMERİPOL'dur.

f. Gelişmiş devletler ve gelişmekte olan veya az gelişmiş devletler arasında bilişim teknolojisi bakımından büyük bir boşluk bulunmaktadır. Dolayısıyla gelişmiş devletler az gelişmiş devletlere teknik destek ve donatım sağlamalıdır.

KAYNAKÇA

Acar, Ünal/ Ömer Urhal: **Devlet Güvenliği İstihbarat ve Terörizm,** Ankara, Adalet Yayınevi, 2007.

Agrafiotis, Ioannis / Jason R. C. Nurse/ Michael Goldsmith/ Sadie Creese/ and David Upton: "A Taxonomy of Cyber-harms: Defining The Impacts of Cyber-attacks and Understanding How They Propagate", **Journal of Cybersecurity**, Vol. 4, No.1, 2018, s. 1-15.

Ajayi, Emmanuel Femi Gbenga: "Challenges to Enforcement of Cyber-Crimes Laws and Policy", Journal of Internet and Information Systems, Vol. 6, No.1, 2016, s. 1-12.

Akarslan, Hüseyin: **Bilişim Suçları**, 2.bs., Ankara, Seçkin Hukuk, 2015.

Akbulut, Berrin: **Bilişim Alanında Suçlar**, 2.bs, Ankara, Adalet Yayınevi, 2017.

Akpek, Nusret Onur: "Siber Suçlar Sözleşmesinin Getirdikleri ve İç Hukuk Açısından Konuya Yaklaşım", **İstanbul Bilgi Üniversitesi, Sosyal Bilimler Enstitüsü, , Yayımlanmamış Yüksek Lisans Tezi**, İstanbul, 2015.

Aldesco, Albert I.: "The Demise of Anonymity: A Constitutional Challenge to the

Convention on Cybercrime", **Loyola of Los Angeles Entertainment Law Review,** Vol. 23, No.1, 2002, s. 81-123.

Aliusta, Cahit/ Recep Benzer: "Avrupa Siber Suçlar Sözleşmesi ve Türkiye'nin Dahil Olma Süreci", **Uluslararası Bilgi Güvenliği Mühendisliği Dergisi**, C.IV, No.2, 2018, s. 35-42.

Altunok, Ebru/ Ali Fatih Vural: "Bilişim Suçları", **Denetişim**, S.8, 2011, s. 74-84.

Angers, Lucie: "Combating Cyber-Crime: National Legislation as a Pre-Requisite to International Cooperation", **Crime and Technology New Frontiers for Regulation, Law Enforcement and Research**, Ed. Ernesto U. Savona, Dordrecht, Springer Science, 2004.

Aydın, Emin Doğan: **Bilişim Suçları ve Hukukuna Giriş**, Ankara, Doruk Yayınları, 1992.

Başlar,Yusuf: "Adli Bilişim Sürecinde Karşılaşan Sorunlar ve Çözüm Önerileri", **TBBD**, S. CXLVIII, 2019, s. 47-76.

Bayraktar, Gökhan: **Siber Savaş ve Ulusal Güvenlik Stratejisi**, İstanbul, Yeniyüzyıl Yayınları, 2015.

Bell, R. E.: "The Prosecution of Computer Crime", **Journal of Financial Crime** , Vol. 9, No. 4, 2002, s. 308-325.

Benzer, Recep: "Siber Suçlar ve Teorik Yaklaşımlar", **Güncel Tehdit : Siber Suçlar**, Ed.

Hüseyin Çakır , Mehmet Serkan Kılıç, İstanbul, Seçkin Yayınları, 2014.

Boister, Neil: "Transnational Criminal Law?", **EJIL**, Vol. 14, No. 5, 2003, s. 953-976.

Borko, Andrii /Vadym Nehodchenko/ **Olena Volobuieva/ Ivan Kharaberiush/ Yevheniia Lohvynenko:** "Fighting Against Cybercrime: Problems and Prospects in Ukraine and the World", **Journal of Legal, Ethical and Regulatory Issues,** Vol. 22, No.2, 2019, s. 1-5.

Brenner, Susan W./ Bert-Jaap Koops: "Approaches to Cybercrime Jurisdiction", **Journal of High Technology Law,** Vol. 4, No. 1, 2004, s. 1-46.

Brenner, Susan W./ Joseph J. Schwerha IV: "Transnational Evidence Gathering and Local Prosecution of International Cybercrime", **The John Marshall Journal of Information Technology & Privacy Law**, Vol. 20, No. 3, 2001, s. 347-396.

Brenner, Susan W./Marc D. Goodman: "In Defense of Cyberterrorism: An Argument for Anticipating Cyber-Attacks", **University of Illionis Journal of Law, Technology and Policy**, No.1, 2002, s. 1-57.

Brenner, Susan W.: **Cybercrime: Criminal Threats from Cyberspace**, California, ABC-CLIO, 2010.

Brenner, Susan W.: "Cybercrime Metrics: Old Wine, New Bottles?", **Virginia Journal of Law and Technology,** Vol. 9, No. 13, 2004, s. 1- 53.

Brenner, Susan W.: "Cybercrime jurisdiction", **Crime, Law and Social Change**, Vol.46, No.4-5, 2006, s. 189-206.

Brenner, Susan W.: "Law, Dissonance, and Remote Computer Searches", **North Carolina Journal of Law & Technology**, Vol. 14, No.1, 2012, **s**. 43-92.

Broadhurst, Roderic: "Developments in The Global Law Enforcement of Cyber-Crime", **Policing: an International Journal of Police Strategies and Management**, Vol. 29, No. 3, 2006, s. 408-433.

Brunst, Phillip W.: "Terrorism and the Internet: New Threats Posed by Cyberterrorism and Terrorist Use of the Internet", **A War on Terror? The European Stance on a New Threat, Changing Laws and Human Rights Implications,** Ed. Marianne **Wade**, Almir **Maljevic,** Berlin, Springer, 2010.

Buono, Laviero: "Fighting Cybercrime Between Legal Challenges and Practical Difficulties: EU and National Approaches", **ERA Forum,** Vol.17, No.3, 2016, s. 343–353

Çakmak, Haydar/ Cenker Korhan Demir: "Siber Dünyadaki Tehditler ve Kavramlar", "**Suç, Terör ve Savaş Üçgeninde Siber Dünya**", ed. Haydar

Çakmak, Taner Altunok, Ankara, Barı Platin Kitabevi, Platin Yayınevi, 2009.

Çakmakkaya, Baki Yiğit/ Teoman Akpınar: "Bilişim Suçları İle Mücadelede Karşılaşılan Sorunlar", **Balkan ve Yakın Doğu Sosyal Bilimler Dergisi**, C.IV, S. 3, 2018, s. 123-129.

Calderoni, Francesco: "The European legal framework on cybercrime: striving for an effective implementation", **Crime, Law and Social Change**, Vol. 54, No. 5, 2010, s. 339–357.

Cammack, Chance: "The Stuxnet Worm and Potential Prosecution by the International Criminal Court under the Newly Defined Crime of Aggression", **Tulane Journal of International & Comparative Law**, , Vol. 20, No.1, 2011, s.303-324.

Çaşın, Mesut Hakkı: **Uluslararası Terörizm**, Ankara, Nobel Yayın Dağıtım, 2008.

Cerezo, Ana I./ Javier Lopez/ Ahmed Patel: "International Cooperation to Fight Transnational Cybercrime", Second International Workshop on Digital Forensics and Incident Analysis, **IEEE**, 2007, s. 13-27.

Chang, Weiping/ Wingyan Chung/Hsinchun Chen/ Shihchieh Chou: "An International Perspective on Fighting Cybercrime", **International Conference on Intelligence and Security Informatics,** ed. Hsinchun Chen, Richard Miranda, Daniel D. Zeng, Chris

Demchak, Jenny Schroeder, Berlin, Springer, 2003,

Choi, Kyung-shick/ Claire Seungeun Lee/ Robert Cadigan: "Spreading Propaganda in Cyberspace: Comparing Cyber-Resource Usage of Al Qaeda and ISIS", **International Journal of Cybersecurity Intelligence and Cybercrime**, Vol. 1, No. 1, 2018, s. 21-39.

Choo, Kim-Kwang Raymond: "Organised Crime groups in Cyberspace: A Typology", **Trends Organ Crim,** Vol.11, No. 3, 2008, s. 270-295.

Christou, George: **Cybersecurity in the European Union Resilience and Adaptability in Governance Policy,** London, Palgrave Macmillan, 2016.

Christou, George: "The Challenges of Cybercrime Governance in the European Union", **European Politics and Society**, Vol. 19, No. 3, 2018, s. 355-375.

Çifci, Hasan: **Her Yönüyle Siber Savaş**, Ankara, TÜBİTAK Popüler Bilim Kitapları, 2013.

Çitin, Erol/ İsmail Malkoç: **Uygulamada Sahtekarlık Suçları, Bilgisayar Suçları, Tebligat Suçları ve İlgili Mevzuat**, Ankara, Adalet Yayınevi, 1995.

Çitlioğlu, Ercan: **Gri Tehdit Terörizm,** Ankara, Destek Yayınları, 2008.

Clarke, Richard A./ Robert K. Knake: **Siber Savaş, Ulusal Güvenliğine Yönelik Yeni Tehdit**, Çev. Murat Erduran,

İstanbul, İstanbul Kültür Üniversitesi Yayınevi, 2010.

Clough, Jonathan: "Cybercrime", **Commonwealth Law Bulletin,** Vol.37, No.4, 2011, s. 271- 680.

Clough, Jonathan: "A World of Difference: The Budapest Convention On Cybercrime And The Challenges Of Harmonisation", **Monash University Law Review**, Vol. 40, No.1, 2014, s. 698-736,

Çolak, Haluk: "Siber Terörizmin Önlenmesinde Kurumsal Yapılanma ve Uluslararası Adli Yardımlaşma", ***Türk Hukuk Araştırmaları Dergisi***, C.I, S.1, 2016, s. 21-52.

Cottim, Armando A.: "Cybercrime, Cyberterrorism and Jurisdiction: An Analysis of Article 22 of the COE Convention on Cybercrime", **European Journal of Legal Studies**, Vol.2, No.3, 2010, s. 55-79.

Csonka, Peter: "The Council of Europe's Convention on Cyber-crime and Other European Initiatives", **Revue İnternationale de Droit Penál** , Vol.77, No.3, 2006, s. 473-501

Das, Resul Muhammet Zekeriya Gündüz, "Analysis of Cyber-attacks in IoT-based Critical Infrastructures", **International Journal of Information Security Science,** Vol.8, No.4, 2019, S.122-133.

Değirmenci, Olgun: "Bilişim Suçları", **Marmara Üniversitesi Sosyal Bilimler Enstitüsü**,

Yayımlanmamış Yüksek Lisans Tezi, 2002.

Dogrul, Murat/ Adil Aslan/ Eyyup Celik: "Developing an International Cooperation on Cyber Defense and Deterrence against Cyber Terrorism", 2011 3rd International Conference on Cyber Conflict, **IEEE**, 2011, s. 29- 43.

Downing, Richard W.: "Shoring Up the Weakest Link: What Lawmakers Around the World Need to Consider in Developing Comprehensive Laws to Combat Cybercrime", **Columbia Journal of Transnational Law**, Vol.43 No. 3, 2004, s. 705- 763.

Dülger, Murat Volkan : **Bilişim Suçları ve İnternet İletişim Hukuku**, 7. bs., Ankara, Seçkin Yayınları, 2018.

Dülger**,** Murat Volkan: **Suç Gelirlerinin Aklanmasına ilişkin Suçlar ve Yaptırımlar**, Ankara, Seçkin Yayıncılık, 2011.

Dülger, Murat Volkan: "Karşılaştırmalı Hukuk Bağlamında Birleşik krallık İngiltere Hukukunda Bilişim Suçları Mevzuatı ve Uygulaması", **Türkiye Adalet Akademisi Dergisi**, S. 31, 2017, s. 141-258.

Dülger, Murat Volkan: "Avrupa Konseyi ve Avrupa Birliği Düzenlemelerinde Çocuk Pornografisinin İnternet Aracılığıyla Yayılmasına Karşı Yapılan Düzenlemeler", **İstanbul Barosu Dergisi**, İstanbul, S.4, 2004, s.1485–1496 .

Dursun, Hasan: "Bilgisayarla İlgili Suçlar", **Yargıtay Dergisi**, C.XXIV, S.3, 1998, s. 334-339.

Easttom, Chuck/ Jeffrey Taylor: **Computer Crime, Investigation and the Law, Boston, Cengage Learning, 2011.**

Ehuan, Art: "Cybercrime and Law Enforcement Cooperation", **CyberForensic Understanding Information Security Investigations**, Ed. Jennifer Bayuk, Totowa, Humana Press, 2010.

Eker, Umut: "Türk Ceza Hukukunda Bilişim Suçları-Eski TCK Bağlamında Hukukumuzda Yer Alan İlk Düzencemeler ve 5237 Sayılı Yeni Türk Ceza Kanunu'nun İlgili Hükümlerinin Yorumu", **TBBD**, S. 62, 2006, s. 101-132.

Emine Eylem Aksoy, "Siber Suçluluğa Dair Sözleşme", **Prof. Dr. Kemal Oğuzman'a Armağan**, 2002.

Emir, Nergiz: "Uluslararası Ceza Mahkemesi'nin Yargı Yetkisi Bakımından Saldırı Suçu", **Anadolu Üniversitesi Hukuk Fakültesi Dergisi**, C.I, S.2, 2015, s. 118-143

Erdal, Selcen: "Uluslararası Ceza Mahkemesinin Ulus-Devlet Egemenliğine Etkisi", **Selçuk Üniversitesi Hukuk Fakültesi Dergisi** , C.ZVIII, S. 1, 2010, s. 147- 206.

Erdem, Merve/ Gürkan Özocak: "Siber Güvenliğin Sağlanmasında Uluslararası Hukukun ve Türk Hukukunun Rolü", **Ankara Üniversitesi Hukuk**

Fakültesi Dergisi, C. LXVI, S.1., 2019, s. 127 – 212.

Erdem, Merve/ Gürkan Özoczk: "Sınıraşan Bir Suç Olarak Siber Suçlarla Mücadelede Uluslararası İşbirliği", **19. Akademik Bilişim Konferansı Bildiri Kitabı**, Aksaray Üniversitesi, 2017.

Erdoğan, Yavuz: **Avrupa Konseyi Siber Suçlar Sözleşmesi'nde Yer Alan Koruma Tedbirleri ve Bu tedbirlerin Türk Hukukundaki Yeri**, İstanbul, Legal Yayıncılık, 2018.

Eren, Mehmet: "Avrupa Birliği'nin Siber Güvenlik Stratejisi İçin Kuramsal Çerçeve Ve Strateji Belgesi Öncesi AB'nin Eylemleri", **Cyberpolitik Journal**, Vol. 2, No. 3, 2017, s. 25-58.

Eren, Mehmet: **Avrupa Birliği'nin Siber Güvenlik Politikası**, İstanbul, Beta Yayınları, 2017.

Ersoy,Yüksel: "Genel Hukuki Koruma Çerçevesinde Bilişim Suçları", **Ankara Üniversitesi Siyasal Bilimler Dergisi**, C. XLIX, S. 3, 1994, s. 149-189.

Fafinski, Stefan: **Computer Misuse Response, Regulation and The Law**, Devon, Willan Publishing, 2009.

Foggetti, Nadina: "Transnation Cyber Crime, Differences Between National Laws and Development of European Legislation: By Repression",

Masaryk University Journal of Law and Technology, Vol.2, No. 2, 2008, s. 31-45.

Freitas, Pedro Miguel F. /Nuno Gonçalves: "Illegal Access to Information Systems and the Directive 2013/40/EU", **International Review of Law, Computers & Technology**, 2015, Vol. 29, No.1, s. 50–62.

Gabrys,Ed: "The International Dimensions of Cyber-Crime Part 1.", **Information Systems Security,** Vol.11, No. 4, 2002, s. 21-32.

Gates, Bill: **The Road Ahead**, New York, Viking, 1995.

Genderen, Rob van den Hoven van: "Cybercrime Investigation and the Protection of Personal data and Privacy", Economic Crime Division Directorate General of Human Rights and Legal Affairs, Strasbourg, 2008.

Gercke, Marco: **Understanding Cybercrime: Phenomena, Challenges and Legal Response,** Geneva, International Telecommunication Union Publication, 2014.

Gercke, Marco: "Siber Suç Sözleşmesi İle 10 Yıl: Avrupa Konseyi'nin İnternet Bağlantılı Suçlara Karşı Mücadele Belgesinin Başarları ve Kusurları", **İnternet Hukuku**, Ed. Yener Ünver, Ankara, Seçkin, 2013.

Gercke, Marco: "Europe's Legal Approaches to Cybercrime", **ERA Forum**, Vol.10, No.3, 2009, s. 409–420.

Ghernaouti, Solange: **Cyber Power Crime, Conflict and security in Cyberspace**, Switzerland, EPFT press, 2013.

Gökcen, Ahmet/ Caner Yenidünya/ Mehmet Emin Artuk: **Ceza Hukuku Genel Hükümleri**, 8.bs., Ankara, Adalet Ayayıevi, 2014.

Goodman, Marc D./ Susan W. Brenner: "The Emerging Consensus on Criminal Conduct in Cyberspace", **International Journal of Law and Information Technology**, Vol. 10, No. 2, 2002, s.139-223.

Goodman, Marc: "International Dimensions of Cybercrime", **Cybercrimes: A Multidisciplinary Analysis**, Ed.,Sumit Ghosh, Elliot Turrini, Berlin, Springer, 2010.

Gordon, Sandy: "Regionalism and Cross-border Cooperation Against Crime and Terrorism in the Asia-Pacific", **Security Challenges**, Vol.5, No.4, 2009, s. 75-102.

Gordon, Sarah/ Richard Ford: "On the Definition and Classification of Cybercrime", **Journal in Computer Virology**, Vol. 1, No. 2, 2006, s. 13-20.

Gözüşirin, Mesih: "5237 Sayılı Türk Ceza Kanununda Bilişim Suçları ve Bilişim Suçları İle Mücadeleye İlişkin Model Önerisi", **Kara Harp Okulu Savunma Bilimleri Enstitüsü**, **Yayımlanmamış Yüksek Lisans Tezi**, Ankara, 2011.

Grabosky, Peter. "Requirements of Prosecution Services to Deal with Cyber Crime", **Crime Law Soc Change**, Vol.47, No. 4-5, 2007, s. 201–223.

Greenberg, Marc H.: "A Return to Lilliput: The LICRA v. Yahoo! Case and the Regulation of Online Content in the World Market", **Berkeley Technology Law Journal** , Vol. 18, No. 4, 2003, s. 1191-1258.

Gürkaynak, Muharrem/Adem Ali İrem: "Reel Dünyada Sanal Açmaz: Siber Alanda Uluslararası İlişkiler", **Süleyman Demirel Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi,** C.XVI, S.2, 2011, s. 263-279.

Haase, Adrian: "Harmonizing Substantive Cybercrime Law Through European Union Directive 2013/40/EU – From European Legislation to International Model Law?", 2015 First International Conference on Anti-Cybercrime, **IEEE**, 2015.

Havuz, Serdar: "Avrupa Konseyi Siber Suçlar Sözleşmesi kapsamında Türkiye Güvenliği", **Harap Akademileri Komutanlığı Stratejik Araştırmalar Enstitülüsü, Yayımlanmamış Yüksek lisans Tezi**, İstanbul, 2007.

Henriksen, Anders: **International Law**, 2. bs., Oxford, Oxford Universty Press, 2019.

Hill, Richard: **The New International Telecommunication Regulations and the**

Internet A Commentary and Legislative History, Berlin, Springer, 2014.

Hosein, Ian: "Creating Conventions: Technology Policy and International Cooperation in Criminal Matters", **Governing Global Electronic Networks International Perspectives on Policy and Power,** Ed. William J. Drake, Ernest J. Wilson III, London, The MIT Press, 2008.

Hunter, Mark/ Marc Le Menestrel/ Henri-Claude de Bettignies: "Ethical Crisis on the Internet: the Case of Licra vs. Yahoo!", **Business Ethics and the Electronic Economy**, Ed. Peter Koslowski, Christoph Hubig, Peter Fischer Berlin, Springer, 2004.

İçsel, Kayhan: "Avrupa Konseyi Siber Suç Sözleşmesi Bağlamında Avrupa Siber Suç Politikasının Ana İlkeler", **İÜHFM**, C.LIX, S.1-2, 2001, s. 3-10.

Jain, Ankur: "Cyber Crime: Nature, Elements and Types", **National Journal of Cyber Security Law**, Vol. 2, No.2, 2019, s.1–5.

Karabal, Mustafa/ Bekir Peker/ Ali Sarvan: "Bilişim Suçları ve Türk Polis Teşkilatı", **Çağın Polisi Dergisi**, S.6, 2003. s. 1-4.

Karagülmez, Ali: **Bilişim Suçları ve Soruşturma-Kovuşturma Evreleri**, 5.bs, Ankara, Seçkin, 2014.

Kaya, İbrahim : **Uluslararası Hukukta Temel Belgeler**, Ankara, Seçkin Yayıncılık, 2013.

Kaya, İbrahim: **Terörle Mücadele ve Uluslararası Hukuk**, Ankara, USAK Yayını, 2005.

Keçeligl, Mutlu Dinç: "Evrensel Yargı Yetkisi: Ceza Hukuku Bağlamında Evrensellik İlkesine Bakış" **Terazi Hukuk Dergisi**, C.XIII, S.143, 2018, s. 123-141,

Keyser, Mike: "The Council of Europe Convention on Cybercrime", **Journal of Transnational Law & Policy**, Vol. 12, No.3, s. 287- 326.

Kizza, Joseph Migga: **Computer Network Security**, Boston, Springer, 2005.

Kovacich, Gerald L./ William C. Boni: **High-Technology-Crime Investigator's Handbook: Working in the Global Information Environment**, Oxford, Elsevier 2000.

Kovács, László: "Cyber Security Policy and Strategy in the European Union and Nato", **Land Forces Academy Review**, Vol. XXIII, No. 1, 2018, s. 16-24.

Kreb, Claus/ Leonie Von Holtzendorff: "The Kampala Compromise on the Crime of Aggression", **Journal of International Criminal Justice**, Vol.8, No. 5, 2010, s. 1179–1217.

Kshetri, Nir: "Cybercrime and Cybersecurity in Africa", **Journal of Global Information Technology Management,** Vol. 22, No. 2, 2019, s. 77–81.

Kurt, Levent: **Açıklamalı -İctihatlı Tüm Yönleriyle Bilişim Suçları ve Türk Ceza**

Kanunundaki Uygulama, Ankara, Seçkin Yayıncılık , 2005.

Lachow, Irving/ Courtney Richardson: "Terrosit Use of the Internet: The Real Story", **Joint Force Quarterly National Defense University**, Vol.45, No.2, 2007.

Laksana, Andri Winjaya: "Cybercrime Comparison Under Criminal Law In Some Countries", **Jurnal Pembaharuan Hukum** Vol. 5, No. 2, 2018, s. 217-226.

Li, Jun/ Jidong Jia: "Confusion and Relief of Criminal Jurisdiction of Cybercrimes", **Advances in Computer Science Research, Volume 65,** 2018 3rd International Conference on Communications, Information Management and Network Security (CIMNS 2018), Atlantis Press, 2018.

Li, Xingan: "International Actions against Cybercrime: Networking Legal Systems in the Networked Crime Scene" **Webology**, Vol. 4, No. 3, 2007, s. 1-24.

Liggett, Roberta/ Jin R. Lee/ Ariel L. Roddy/ Mikaela A. Wallin: "The Dark Web as a Platform for Crime: An Exploration of Illicit Drug, Firearm, CSAM, and Cybercrime Markets", **The Palgrave Handbook of International Cybercrime and Cyberdeviance**, Ed., Thomas J. Holt, Adam M. Bossler, Cham, Palgrave Macmillan, 2020.

Lin, Herbert S.: "Offensive Cyber Operations and the Use of Force", **Journal of National Security**

Law & Policy, Vol.4, No.63, 2010, s. 63-86.

Lin, Leo S. F. / John Nomikos: "Cybercrime in East and Southeast Asia: The Case of Taiwan", **Asia-Pacific Security Challenges Managing Black Swans and Persistent Threats**, Ed. Anthony J. Masys, Leo S. F. Lin, Switzerland, Springer, 2018.

Maclean, Don: "Sovereign Right and the Dynamics of Power in the ITU: Lessons in the Quest for Inclusive Global Governance", **Governing Global Electronic Networks International Perspectives on Policy and Power,** Ed., William J. Drake, Ernest J. Wilson III, London, The MIT Press, 2008.

Maillart, Jean-Baptiste: "The limits of Subjective Territorial Jurisdiction in the Context of Cybercrime", **ERA Forum**, Vol. 19, No. 3, 2019, s. 375- 390.

Malby, Steven/ Robyn Mace/ Anika Holterhof/ Cameron Brown/ Stefan Kascherus/ Eva Ignatuschtschenko: **Comprehensive Study on Cybercrime**, New York, United Nations Office on Drugs and Crime, 2013.

Maxwell, Winston J./ Marc Bourreau: "Technology Neutrality in Internet, Telecoms and Data Protection Regulation", **Computer and Telecommunications Law Review**, Vol. 31, 2014, s. 1-8.

Mcguire, Mike: **Into The Web of Profit An In-Depth Study of Cybercrime, Criminals and Money**, California, Bromium, Inc., 2018.

Mosıu, Ovidiu/ Ion Balaceanu/ Eduard Mihai, "Cyber Terroism and the Eeffects of the Russian Attacks on Democratic States in East Europe", **Scientific Journal of Silesian University of Technology. Series Transport,** Vol. 106, No.11, 2020, s. 131-139.

Mumcu, Şinasi Özgür: "Siber Saldırıları ve Uluslararası Hukuk Hakkında Genel Bir Değerlendirme", **Galatasaray Üniversitesi Hukuk Fakültesi Dergisi**, S.1, 2012, s. 211-228.

Nain, Delphine/ Neal Donaghy/ Seymour Goodman: "The International Landscape of Cyber Security", **Information Security: Policy, Processes, and Practices**, Ed. Detmar W. Straub, Seymour Goodman, Richard Baskerville, New York, M.E. Sharpe, 2008.

Nasheri, Hedieh: **Economic Espionage and Industrial Spying**, Cambridge, Cambridge University Press, 2005.

Oerlemans, Jan-Jaap: **Investigating Cybercrime**, Amsterdam, Amsterdam University Press, 2017.

Okoniewski, Elissa A.: "Yahoo!, Inc. v. LICRA: The French Challenge to Free Expression on the Internet", **American University International Law Review,** Vol. 18., No.1, 2002, s. 295-239.

Önok, Murat: "Avrupa Siber Suç Sözleşmesi Işığında Siber Suçlarla Mücadelede Uluslararası İşbirliği", **Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi**, C.IX S.2, 2013, s. 1229-1270.

Oraegbunam, Ikenga K.E.: "Jurisdictional Challenges in Fighting Cybercrimes: Any Panacea From International Law?", **Nnamdi Azikiwe University Journal of International Law and Jurisprudence,** Vol. 6. 2015, s.57-65.

Orji, Uchenna Jerome: "The African Union Convention on Cybersecurity: A Regional Response Towards Cyber Stability?", **Masaryk University Journal of Law and Technology**, Vol. 12, No. 2, 2018, s. 91-130.

Osula, Anna-Maria: "Mutual Legal Assistance & Other Mechanisms for Accessing Extraterritorially Located Data", **Masaryk University Journal of Law and Technology**, Vol. 9, No. 1, 2015, s. 43-64.

Özbek, Mücahid: "The Impacts of European Cybercrime Convention on Turkish Criminal Law", **GSI Articletter**, S. 13, 2015, s. 73-88.

Özbek, Mücahid: "Avrupa Siber Suçlar Sözleşmesi Çerçevesinde Adli Yardımlaşma", **Galatasaray Üniversitesi Sosyal Bilimler Enstitüsü Yayımlanmamış Yüksek Lisans Tezi,** İstanbul, 2015.

Özbek, Veli Özer: "İnternet Kullanımında Ortaya Çıkabilecek Bazı Ceza Hukuku Sorunları", **DEÜHFD,** C.IV, S.1., 2002, s. 101-185.

Özüdoğru, Uğur: "Siber Suçlar ve Mücadele Yöntemleri : Dünya Uygulamaları ve Türkiye İçin Çözüm Önerileri" **Bilgi Teknolojileri ve İletişim Kurumu, Yayımlanmamış Bilişim Uzmanlığı Tezi,** 2011.

Painter, Christopher: "Threats to the Net: Trends and Law Enforcement Responses", **Crime and Technology New Frontiers for Regulation, Law Enforcement and Research**, Ed. Ernesto U. Savona, Netherlands, Springer, 2004.

Painter, Christopher: "Threats to the Net: Trends and Law Enforcement Responses", **Crime and Technology New Frontiers for Regulation, Law Enforcement and Research**, Ed. Ernesto U. Savona, Dordrecht, Springer, 2004.

Palmer, Adam: "Mutual Legal Assistance: Understanding the Challenges for Law Enforcement in Global Cybercrime Cases Issue Brief", **Center for Cyber and Homeland Security at Auburn University**, 2018, s. 1-17.

Palustre, Adonis/ David Croasdell: "The Role of Transnational Cooperation in Cybersecurity Law Enforcement**", Proceeding Softhe 52nd Hawaii**

International Conference on System Sciences, 2019, s. 5607- 5598.

Payne, Brian K.: "Defining Cybercrime", **The Palgrave Handbook of International Cybercrime and Cyberdeviance**, Ed. Thomas J. Holt, Adam M. Bossler, Palgrave Macmillan, Switzerland, 2020, s. 3- 26.

Peker, Bekir: "Bilişim Suçları ve Bilişim Güvenliğinin Ulusal ve Uluslararası Boyutu" **Selçuk Üniversitesi Sosyal Bilimler Enstitüsü, Yayımlanmamış Yüksek Lisans Tezi**, Konya, 2010.

Perloff-Giles, Alexandra: "Transnational Cyber Offenses: Overcoming Jurisdictional Challenges", **The Yale Journal of International Law**, Vol. 43, No. 1, 2018, s.191-227.

Pocar, Fausto: "New Challenges for International Rules Against Cyber-Crime", **European Journal on Criminal Policy and Research**, 2004, Vol. 10, No.1, s. 27–37

Podgor, Ellen S.: "Cybercrime: National, Transnational, or International?", **Wayne Law Review**, Vol. 50, No.1, 2004 s. 97-108.

Portnoy, Michael/ Seymour Goodman: **Global Initiatives to Secure Cyberspace An Emerging Landscape**, Ed. Michael Portnoy, Seymour Goodman, New York, Springer Science, 2009.

Roosendaal, Arnold/ Mari Kert/ Alison Lyle/ Ulrich Gasper:

"Data Protection Law Compliance for Cybercrime and Cyberterrorism Research" **Combatting Cybercrime and Cyberterrorism Challenges, Trends and Priorities**, Ed., Babak Akhgar , Ben Brewster, Cham, Springer, 2016.

Roscini, Marco: "Gravity in the Statute of the International Criminal Court and Cyber Conduct That Constitutes, Instigates or Facilitates International Crimes", **Criminal Law Forum**. Vol. 30, No. 3, 2019, s. 247–272

Şafak, Erdi: "Uluslararası Hukukta Değişen Güvenlik Algısı ve Saldırı Suçu Bağlamında Siber Saldırılar", **Selçuk Üniversitesi Hukuk Fakültesi Dergisi**, C.XXVIII, S.1, 2020, s.127-160,

Sağsan, Mustafa: "Bilgi Savaş: Siperlerden Klavyelere Taşınan Hareketin Anatomisi", **Avrasya Dosyası,** C.VIII, S. 2, 2002, s. 213-232.

Şamlı, Rüya: "Türk ve Dünya Hukukunda Bilişim Suçları", Akademik Bilişim'10 - XII. Akademik Bilişim Konferansı Bildirileri 10 - 12 Şubat 2010 Muğla Üniversitesi.

Saraçlı, Murat: "Uluslararası Hukukta Terörizm", **Gazi Üniversitesi Hukuk Fakültesi Dergisi,** C. XI, S.1, 2007, s. 1049- 1087.

Sayapin, Sergey: **The Crime of Aggression in International Criminal Law**, Netherlands, Asser Press, 2014.

Schaap, Major Arıe J.: "Cyber Warfare Operations: Development and Use under International Law", **Air Force Law Review**, Vol.64, 2009, s. 121-142.

Schell,Berandette H./ Clemens Martin: **Cybercrime A Reference Handbook**, California, ABC-CLIO, 2004.

Scherrer, Amandine: **G8 against Transnational Organized Crime,** London, Routledge, 2009.

Schjolberg, Stein /Amanda B. Hubbard: "Harmonizing National Legal Approaches on Cybercrime", International Telecommunication Union, **WSIS Thematic Meeting on Cybersecurity**, 2005.

Schjolberg, Stein: **The History of Cybercrime: 1976-2014**, Germany, Cybercrime Research Institute, 2014.

Schjolberg, Stein: "The History of Global Harmonization on Cybercrime Legislation–The Road to Geneva", **Journal of International Commercial Law and Technology**, Vol.1, No.12, 2008, s 1-19.

Şen, Bilal/ Mahmut Çengiz: "Bir Sınıraşan Suç Türü Olarak Bilişim Suçları", **Sınıraşan Organize Suçlar, Kavramlar, Yöntemler, Eğilimler**, ed, Oğuzhan Ömer Demir, Bahadır Küçükuysal, 3.bs., Ankara, Adalet Yayınevi, 2013.

Servent, Ariadna Ripoll: "Protecting or Processing? Recasting EU Data Protection Norms", **Privacy, Data Protection and Cybersecurity in Europ,**

Ed., Wolf J. Schünemann, Max-Otto Baumann, Cham, Springer, 2017.

Shackelford, Scott J.: "Toward Cyberpeace: Managing Cyberattacks through Polycentric Governance", **American University Law Review**, Vol. 62, No. 5, 2013, s. 1273-1364.

Shakarian, Jana/ Paulo Shakarian,/ Andrew Ruef: **Introduction to Cyber-Warfare: A Multidisciplinary Approach**, Syngress, Waltham, 2013.

Shaw, Malcolm N.: **International Law**, 8.bs., Cambridge, Cambridge University Press, 2017.

Shinder, Debra Littlejohn/ Ed Tittel: **Scene of The Cybercrime Computer Forensics Handbook,** Massachusetts, Syngress Publishing, 2002.

Sieber, Ulrich: **Legel Aspects of Computer - Related Crime in The Information Society** (Comcrime Study), European Commissio, Würburg Üniversitesi y.y., 1998.

Sieber, Ulrich: "Instruments of international law: against terrorist use of the Internet", **A War on Terror?**, New York, Springer, 2010.

Şimşek, Kemal: "Uluslararası Adli Yardımlaşma Konusunda Uygulamada Karşılaşılan Sorunlar ve Çözüm Önerileri Üzerine", **Adalet Dergisi**, S.45, 2013, s. 145-160.

Sınar, Hasan: **İnternet ve Ceza Hukuku**, İstanbul, Beta Basım, 2001.

Sınar, Hasan: "Avrupa Konseyi Siber Suç Sözleşmesi Üzerine Bir Deneme", **Prof. Dr. Çetin Özek Armağanı**, İstanbul, Şan Ofset, 2004.

Singh, Subhash Chandra: "High-Tech and Computer Crimes: Global Challenges, Global Responses", **Contemporary Issues in International Law Environment, International Trade, Information Technology and Legal Education,** Ed., B.C. Nirmal, Rajnish Kumar Singh, New Delhi, Springer Singapore, 2018.

Smith, Russell G./ Peter Grabosky/ Gregor Urbas: **Cyber Criminal on Trial**, Cambridge University Press, Cambridge, 2004.

Speer, David L.: "Redefining Borders: The Challenges of Cybercrime", **Crime, Law and Social Change**, Vol. 34, No. 3, 2000, s. 259–273.

Sunde, Inger Marie: "Cybercrime Law", **Digital Forensics**, Ed. André Årnes, Hoboken John Wiley & Sons, 2018.

Tezcan, Durmuş/ Mustafa Ruhan Erdem/ R. Murat Önok: **Uluslararası Ceza Hukuku,** 4.bs, Ankara, Seçkin Yayıncılık, 2019.

Tınılır, Mehmet Niyazi: **İnternet Suçları ve Bireysel Mahremiyet,** Ankara, Liberte Yayınları, 2002.

Turrini, Elliot/ Sumit Ghosh: "A Pragmatic, Experiential Definition of Computer Crimes", **Cybercrimes: A Multidisciplinary Analysis**, Ed. Elliot

Turrini, Sumit Ghosh, Berlin, Springer, 2010.

Ulusoy, Orçun: **Uluslararası Ceza Mahkemesi**, Ed. Utku Kılınç, İzmir, Etki Matbaacılık Yayıncılık, 2008.

Ünver, Mustafa/ Cafer Canbay/ Ayşe Gül Mirzaoğlu: **Uluslararası Kuruluşların Siber Güvenlik Faaliyetleri**, Ankara, Bilgi Teknolojileri ve İletişim Kurumu, 2011.

Vatis, Michael A.: "The Council of Europe Convention on Cybercrime", National Research Council, **Proceedings of a Workshop on Deterring Cyberattacks : Informing Strategies and Developing Options for U.S. Policy,** Washington, D.C., National Academies Press, 2010.

Velasco, Cristos: "Cybercrime Jurisdiction: Past, Present and Future", **ERA Forum,** Vol. 16., No. 3, 2015, s. 331-347.

Wall, David S.: **Cybercrime: The Transformation of Crime in the Information Age**, Cambridge, Polity Press, 2007.

Wang, Shiuh-Jeng: "Measures of Retaining Digital Evidence to Prosecute Computer-based Cyber-Crimes" , **Computer Standards & Interfaces,** Vol.29, No.2, 2007,s. 216–223.

Weber, Amalie M.: "The Council of Europe's Convention on Cybercrime", **Berkeley Technology Law Journal**, Vol. 18, No.1, 2003, s.425-446.

Weber, Rolf H./ Ulrike I. Heinric: **Anonymization,** London, Springer, 2012.

Weber, Rolf H.: **Shaping Internet Governance: Regulatory Challenges**, Berlin, Springer, 2010.

Weimann, Gabriel: "Cyberterrorism: The Sum of All Fears?", **Studies in Conflict & Terrorism**, Vol. 28, No. 2, 2005, s. 129-149.

Wells, Donald A.: **The United Nation: States vs International Laws,** New York, Algora Publishing, 2005.

Westby, Jody R.: **International Guide to Combating Cybercrime**, Chicago, American Bar Association, 2003.

Wu, Yanbo / Dawei Xiang/ JiangMing Gao/ Yun Wu: "Research on Investigation and Evidence Collection of Cybercrime Cases", **Journal of Physics: Conference Series**, Vol. 1176, No. 4, 2019, s. 1-7.

Yayla, Mehmet: "Hukuki Bir Terim Olarak Siber Savaş", **TBBD**, S.104, 2013, s. 177-202.

Yayla, Mehmet: "Siber Savaş ve Siber Ortamdaki Kötü Niyetli Hareketlerden Farkı", **Hacettepe Hukuk Fakültesi Dergisi**, C.IV, S.2, 2014, s. 181–200.

Yazıcıoğlu, Yılmaz: "Bilgisayar Ağlarıyla İlgili Suçlar Konusunda Türk Ceza Kanunu 2000 Tasarısı" **Uluslararası İnternet hukuku sempozyumu 21-22 mayıs 2001, İzmir,** Dokuz Eylül Üniversitesi Yayını, 2002.

Yazıcıoğlu,Yılmaz: **Bilgisayar Suçları Kriminolojik, Sosyolojik ve Hukuki Boyutları İle**, İstanbul, ALFA, 1997.

Yenidünya, Caner/ Olgun Değirmenci: **Mukayeseli Hukukta ve Türk Hukukunda Bilişim Suçları,** İstanbul, Legal Yayıncılık, 2003.

Yenisy, Feridum: "İnternet Suçlarının Yeni İşleniş Biçimleri", **Uluslararası İnternet Hukuku Sempozyumu 21-22 Mayıs 2001, İzmir,** Dokuz Eylül Üniversitesi Yayını, 2002.

Yetim, Servet: "Bilişim Suçları ve Etkin Mücadele Yöntemleri", **Terazi Hukuk Dergisi**, C.IX, S.95, 2014, s. 80-86.

Yılmaz, Hatice Kübra Ecemiş: "Birleşmiş Milletler Antlaşması, Kuzey Atlantik Antlaşması ve Uluslararası Hukuk Açısından Siber Saldırının Tanımlanması Sorunu", **Journal of Social And Humanities Sciences Research,** Vol.6, No.38, 2019, s. 1641-1655.

Yılmaz, Sacit: **Türk Ceza Hukuku Sisteminde Siber Suçlar**, Ankara, Adalet Yayınevi, 2016.

Yılmaz, Sait: **21. Yüzyılda Güvenlik ve İstihbarat**, İstanbul, Alfa Yayınları, 2006.

Zakaras, Matthew R.: "International Computer Crimes, General Report", **Revue Internationale de droit pénal,** Vol. 72, No. 3, 2001, s. 813 – 829.

Arapça Kaynaklar

Yusuf, Hasan Yusuf: **El Ceraim el Duveliye li İnternet,** Kahire, El merkez el Kavumi li el İsdarat el Kanuniye, 2011.

Elşehri, Faiz Bin Abdullah: "EL Tahdiyat el Emniye el Musahibe li Vesail el İtisal el Cedide", **El mecele el Arabiye li Dirasat ve el Tedrib**, C.XX, S.39, 2003, s. 133-182.

Elmenaase, Osama Ahmet/ Jelal Muhamet Elzubi: **Ceraim Tekeniyet Nuzum el-Melumat el-Elektroniye**, Umman, Dar el Sekafe li Neşir ve Tevzii, 2010.

Hemi, Ahmet/ Zühera Keisi: "Suar Creaim Tekneiyet el Melumat Wifke li İtifakiye el Arabiye li Senet 2014", **Mecelet el Ulum el Siyasiye ve el Knuniye**, C.X, S.1, 2019, s. 776-795.

Hesenin, İmam/ Ata Alla: **Ceraim Tekeniyet el Malumat fi el Teştiaat ve el Sukuk el Arabiye**, Riyad, Dar Camiat Naif li Neşir, 2017.

Cebur, Muna Eleşker: **El-sibraniye Hacis el-Asır**, Beirut, El-mekez El-Arabi li-albuhus el-Kanunniye ve el- Kazaye, Cami'at el- düvel El Arabiye, 2016.

Alredaide, Abdulkerim. **El ceraim el Müstahdese ve İstiratijiyet Müvacehetiha**, Umman, Dar ve Mektebet Hamid li Neşir ve el Tavzii, 2013.

Sadat, Diya Yahya el: **Mebadi İstihdam el Hasib el Ali ve el İnternet ve Cühud Mükafehet el**

Ceraim el Naşie, İskenderiye, Menşe el Mearif, 2012.

Sultan, Kawther Hazim: "Mekuf el Kanun ve el Kada'a min el Cerime El'elektroniye", **Mecelet Küliyet el terbiye el Esasiye**, C.XXII, S. 96, s. 969- 988.

Eldusuky, Tarık İbrahi: **EL'emin Elmalumaty**, İskenderiye, Dar Elcamiaa Elarabiye, 2009.

Afiefe, Talal Ebu: **Usul İlmi el İcarm ve el İkap ve Ahir el Cühüd el Düveliye ve el Arabiye li Mükafehet el Cerime el Münezeme Aber el Vataniye**, Kudüs, Dar el Cündi li Neşir ve el Tavzii, 2013.

ULUSLARARASI BELGELR

I. BİRLEŞMİŞ MİLLETLER KARARLARI

Birleşmiş Milletler Genel Kurul Kararı, (A/ RES/60/177), Follow-up to the Eleventh United Nations Congress on Crime Prevention and Criminal Justice, 2005.

Birleşmiş Milletler Genel Kurul Kararı, (A/RES/57/239), Creation of a Global Culture of Cybersecurity, 2003.

Birleşmiş Milletler Genel Kurul Kararı, (A/RES/58/199), Creation of a Global Culture of Cybersecurity and the Protection of Critical Information Infrastructures, 2004.

Birleşmiş Milletler Genel Kurul Kararı, (A/RES/64/211), Creation of a Global Culture of Cybersecurity and Taking Stock of National Efforts to Protect Critical Information Infrastructures, 2010.

Birleşmiş Milletler Genel Kurul Kararı, (A/RES/68/167), The Right to Privacy in the Digital Age, 2014,

Birleşmiş Milletler Genel Kurul Kararı, (A/RES/69/166), The Right to Privacy in the Digital Age, 2015.

Birleşmiş Milletler Genel Kurul Kararı, (A/RES/71/199), The right to privacy in the digital age, 2017.

Birleşmiş Milletler Genel Kurul Kararı, (A/RES/71/209), Strengthening the United Nations Crime Prevention and Criminal Justice Programme, in Particular Its Technical Cooperation Capacity, 2017.

Birleşmiş Milletler Genel Kurul Kararı, (A/ERES/56/121), Combating the Criminal Misuse of Information Technologies**,** 2002.

Birleşmiş Milletler Genel Kurul Kararı, (A/RES/45/121), 1990.

Birleşmiş Milletler Genel Kurul Kararı, (A/RES/55/63), Combating the Criminal Misuse of Information Technologies, 2001.

Birleşmiş Milletler Genel Kurul Kararı, (A/RES/65/230), Twelfth United Nations Congress on Crime Prevention and Criminal Justice, 2011.

Birleşmiş Milletler, (A/CONF.213/18), Report of the Twelfth United Nations Congress on Crime Prevention and Criminal Justice, Salvador, Brazil, 12-19 April 2010.

Birleşmiş Milletler, (A/CONF.222/12), Thirteenth United Nations Congress on Crime Prevention and Criminal Justice, Doha, 12-19 April 2015.

II. AVRUPA BİRLİĞİ KARARLARI

Council Framework Decision (2004/68/JHA) on combating the sexual exploitation of children and child pornography.

Council Framework Decision (2005/222/JHA) on Attacks Against Information Systems.

Council Framework Decision (2002/475/JHA) on Combating Terrorism.

Council Framework Decision 2008/919/JHA of Amending Framework Decision 2002/475/JHA on Combating Terrorism.

Directive (2002/58/EC), Concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector (Directive on Privacy and Electronic Communications).

Regulation (EU: 2016/679) on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation).

Directive (2006/24/EC) on the Retention of Data Generated or Processed in Connection with the Provision of Publicly Available Electronic Communications Services or of Public Communications Networks and Amending Directive (2002/58/EC).

Directive 2011/92/EU of the European Parliament and of the Council on Combating the Sexual Abuse and Sexual Exploitation of Children and Child Pornography, and Replacing Council Framework Decision 2004/68/JHA.

Directive 2013/40/EU of the European Parliament and of the Council, on Attacks Against Information Systems and Replacing Council Framework Decision 2005/222/JHA.

III. DİĞER BELGELER VE ANTLAŞMALAR

European Commission, Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace, Brussels, 2013.

Court of Justice of the European Union, Judgment of the Court (Grand Chamber), 8 April 2014, Joined Cases C-293/12 and C-594/12 Digital Rights Ireland and Others.

Arap Adalet Baklanları Konseyi, 19/ 495/2003 numaralı kararı.
Arap İçişler Baklanları Konseyi, 21/417/2004 numaralı kararı.

European Parliamant, Dirctorate General for Internal Policies, Policy Deparment C: Citizens' Right and Constitutional Affairs Civil Liberties, Justice and Home Affairs, The law enforcement challenges of cybercrime: are we really playing catch-up ?, 2015.

Commonwealth Secretariat, "Report of the Commonwealth Working Group of Experts on Cybercrime", **Commonwealth Law Bulletin**, Vol.40, No. 3, 2014.

Avrupa Konseyi Siber Suç sözleşmesi, 2001.

Birleşik Arap Emirlikleri Bilgi Teknolojisi Suçlarıyla Mücadelede Model (Yol Gösterici) Kanunu, 2003.

Bilgi Teknolojisi Suçlarına İlişkin Arap Sözleşmesi, 2010.

Körfez Arap Ülkeleri İşbirliği Konseyi Bilgi Teknolojisi Suçlarıyla Mücadelede Yeknesak Yasa için Riyad Antlaşması, 2012.

Council of Europe, Project on Cybercrime, International Co-operation under the Convention on Cybercrime, 2009.

African Union Convention on Cyber Security and Personal Data Protection, 2014.

Council of Europe, Explanatory Report to the Convention on Cybercrime, Budapest, 2001.

ÇEVRİMİÇİ KAYNAKLAR

Chair's Report of the Meeting of the G7 Ise-Shima Cyber Group, (Çevrimiçi), https://ccdcoe.org/uploads/2018/11/G7-180423-IseShimaChairsReport.pdf, Erişim Tarihi: 15.12.2019.

Commander Barbara, "Etter The Challenge of the Forensic Investigation of Computer Crime", (Çevrimiçi), http://www.austlii.edu.au/au/journals/AUFPPlatypus/2001/19.pdf, Erişim Tarihi: 07.10.2019.

David S. Wall, "Policing Cybercrimes: Situating The Public Police in Networks of Security Within Cyberspace", (Çevrimiçi), https://cyberdialogue.ca/wp-content/uploads/2011/03/David-Wall-Policing-CyberCrimes.pdf, Erişim Tarihi: 17.10.2019.

Dorothy D. Denning, "Is The Cyber Terror Next?" , (Çevrimiçi) http://essays.ssrc.org/sept11/essays/denning.htm, Erişim Tarihi, 25.10.2019.

Draft International Convention To Enhance Protection from Cyber Crime and Terrorism, (Çevrimiçi), https://media.hoover.org/sites/default/files/documents/0817999825_249.pdf, Erişim Tarihi: 08.12.2019.

G7 Principles and Actions on Cyber, (Çevrimiçi), https://www.mofa.go.jp/files/000160279.pdf, Erişim Tarihi: 15.12.2019.

HIPCAR Harmonization of ICT Policies, Legislation and Regulatory Procedures in the Caribbean , (Çevrimiçi), http://caricom.org/documents/16583-universal_service_and_access_mpg.pdf, Erişim Tarihi: 20.12.2019.

https://edition.cnn.com/2019/05/01/europe/vladimir-putinindependent-russian--internet-intl/index.html, Erişim Tarihi: 25.10.2019.

Interpol, Global Cybercrime Strategy , (Çevrimiçi), https://www.interpol.int/content/download/5586/file/Summary_CYBER_Strategy_2017_01_EN%20LR.pdf?inLanguage=eng-GB, Erişim Tarihi: 25.12.2019.

ITU Global Cybersecurity Agenda (GCA), High-Level Experts Group (HLEG), (Çevrimiçi), https://www.itu.int/en/action/cybersecurity/Documents/gca-chairman-report.pdf, Erişim Tarihi: 21.12.2019.

ITU-EC-ACP Project, Support for the Establishment of Harmonized Policies for the ICT Market in the (ACP) States,, (Çevrimiçi), https://www.itu.int/en/ITU-D/Projects/ITU-EC-ACP/Pages/default.aspx, Erişim Tarihi: 20.12.2019.

Joachim Vogel, "Towards a Global Convention against Cybercrime", First World Conference of Penal Law. Penal Law in the XXIst Century, Guadalajara (Mexico), 2007, (çevrimiçi), http://www.penal.org/sites/default/files/files/Guadalajara-Vogel.pdf, Erişim Tarihi: 11.02.2020.

Körfez Arap Ülkeleri İşbirliği Konseyi, "Bilgi Teknolojisi Suçlarıyla Mücadelede Yeknesak Yasa için Riyad Antlaşması", (Çevrimiçi), https://cutt.ly/jaYImom, Erişim Tarihi: 09.04.2020.

Kristin Finklea, Catherine A. Theohary, "Cybercrime: Conceptual Issues for Congress and U.S. Law Enforcement", (Çevrimiçi), https://fas.org/sgp/crs/misc/R42547.pdf, Erişim Tarihi: 25.08.2019.

McConnell International, "Cyber Crime . . . and Punishment?", (Çeveimiçi), http://www.iwar.org.uk/law/resources/cybercrime/mcconnell/CyberCrime.pdf,Erişim , Erişim Tarihi 15.10.2019.

Meeting of Justice and Interior Ministers of The Eight December 9-10, 1997, (Çevrimiçi), https://www.justice.gov/sites/default/files/ag/legacy/2004/06/08/97Communique.pdf, Erişim Tarihi: 20.12.2019.

Mehmet Emin Arslan, "Siber Güvenlik ve Siber Saldırı Türleri", (Çevrimiçi), https://cutt.ly/WeEY9LE, Erişim Tarihi: 03.11.2019.

Mehmet Özcan "Siber Terörizm ve Ulusal Güvenliğe Tehdit Boyutu", (Çevrimiçi), https://docplayer.biz.tr/29878985-Siber-terorizm-ve-ulusal-guvenlige-tehdit-olusturma-boyutu.html, Erişim Tarihi: 24.10.2019.

OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security, https://www.oecd.org/internet/ieconomy/15582260.pdf, Erişim Tarihi: 20.12.2019.

OECD, Policy Guidance on Online Identity Theft, (Çevrimiçi), https://www.oecd.org/sti/consumer/40879136.pdf, Erişim Tarihi: 20.12.2019.

OECE (IPPC), (Çevrimiçi), http://www.oecd.org/internet/ieconomy/37328586.pdf, Erişim Tarihi: 20.12.2019.

Oğuz Kara, Üzeyir Aydın, Ahmet Oğuz, "Ağ Ekonomisin Karanlık Yüzü: Siber Terör", (Çevrimiçi),http://kisi.deu.edu.tr/oguz.kara/Ag%20Ekonomisinin%20karanlik%20yuzu%20siber%20teror.pdf, s.2. Erişim Tarihi: 25.10.2019.

Patrick Nohe, "Cybercrime Pays: New Study Finds Cybercriminal Revenues Hit $1.5 Trilyon Annually", (Çevrimiçi), https://www.thesslstore.com/blog/cybercrime-pays-new-study-finds-cybercriminal-revenues-hit-1-5-trillion-annually/, Erişim Tarihi: 10.11.2019.

Patrick Nohe, "Cybercrime Pays: New Study Finds Cybercriminal Revenues Hit $1.5 Trilyon Annually", (Çevrimiçi), https://www.thesslstore.com/blog/cybercrime-pays-new-study-finds-cybercriminal-revenues-hit-1-5-trillion-annually/, Erişim Tarihi: 10.11.2019.

Ready... or not? Balancing future opportunities with future risks, A Global Survey into Attitudes and Opinions on IT Security (Çevrimiçi), https://bit.ly/2Z5oF9M, Erişim Tarihi: 21.07.2019.

Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, (Çevrimiçi), https://undocs.org/pdf?symbol=en/A/70/174, Erişim Tarihi: 15.12.2019.

Telwant Singh Addl.Distt, Sessiens Judge .Delhi, "Cyber Law and Information Technology", (Çevrimiçi), https://www.slideshare.net/talwant/cyber-law-information-technology, Erişim Tarihi: 18.10.2019.

The Cost of Cybercrime, Ninth Annual Cost of Cybercrime Study Unlocking the Value of Improved Cybersecurity Portection, (Çevrimiçi), https://accntu.re/30PiK9a, Erişim Tarihi: 19.2019.

UNODC, Doha Declaration on Integrating Crime Prevention and Criminal Justice into the Wider United Nations Agenda to Address Social and Economic Challenges and to Promote the Rule of Law at the National and International Levels, and Public Participation, New York, 2015, (Çevrimiçi), https://www.unodc.org/documents/congress/Declaration/V1504151_English.pdf, Eeişim Tarihi: 15.12.2019.

World Economic Forum, The Global Risks Report 2019 14th Edition, (Çevrimiçi) http://www3.weforum.org/docs/WEF_Global_Risks_Report_2019.pdf, Erişim Tarihi: 21.11.2019.

Yılmaz Yazıcıoğlu, "Konuşma AB Uyum Komisyonu Çalışması Türk Mevzuatında Bilişim Suçları", (Çevrimiçi), http://docplayer.biz.tr/8186275-Konusma-ab-uyum-komisyonu-calismasi-turk-mevzuatinda-bilisim-suclari.html, Erişim Tarihi: 17.10.2019.

(Çevrimiçi), https://disiliskiler.ktb.gov.tr/TR-22153/ekonomik-isbirligi-ve-kalkinma-orgutu-oecd.html, Erişim Tarihi: 17.12.2019.

(Çevrimiçi), https://www.aydinpost.com/ekonomi/g7-nedir-g7-ulkeleri-hangileridir-h749844.html, Eeişim Tarihi: 13.12.2019.

2011 Deauville G8 Summit Final Compliance Report, (Çevrimiçi), http://www.g7.utoronto.ca/evaluations/2011compliance-final/2011g8finalcompliance.pdf, Erişim Tarihi: 15.12.2019.

Adam Palmer ,"Mutual Legal Assistance: Understanding the Challenges for Law Enforcement in Global Cybercrime Cases Issue Brief", Center for Cyber and Homeland Security at Auburn

University,2018,(Çevrimiçi),https://www.jstor.org/stable/resrep20738?seq=1#metadata_info_tab_contents, Erişim Tarihi: 12.02.2020.

Birleşik Arap Emirlikleri Bilgi Teknolojisi Suçlarıyla Mücadelede Model (Yol Gösterici) Kanunu'nun tam metni, (Çevrimiçi), https://carjj.org/sites/default/files/qnwn_lmrt_lrby_lstrshdy_lmkfh_jrym_tqny_lmlwmt.pdf. Erişim Tarihi, 11.12.2019.