Araştırma Makalesi/Research Article **Doi: 10.55009/bilisimhukukudergisi.1119881**

SİBER SUÇ, SİBER TERÖR VE SİBER SAVAŞ ÜÇGENİNDE SİBER DÜNYA

Cyber World in the Cyber Crime, Cyber Terror and Cyber War Triangle

Nurullah SANDİLAÇ*

Öz

Bu makale ile siber suç, siber terör ve siber savaş kavramları arasında bir ayrım gözeterek daha geniş bir perspektif üzerinden bu olgu ve kavramların ele alınması amaçlanmıştır. Konu ile ilgili temel araştırma sorusu: Siber suç, siber terörizm ve siber savaş kavramları farklı mıdır? Farklı ise, farklı kılan etmenler nelerdir? sorularına cevap aranmıştır. Bu çalışmada, nitel araştırma yöntemi benimsenmiş olup, araştırma desenine uygun olarak belgelere dayalı gözlem tekniği kullanılmıştır.

Anahtar kelimeler: Siber Suç, Bilişim Suçları, Siber Terör, Siber Savaş, Siber Dünya.

Abstract

With this article, it is aimed to discuss these phenomena and concepts from a wider perspective by making a distinction

* Zabıt Kâtibi, Sakarya Adliyesi, nurullah.sandilac@adalet.gov.tr, ORCID: 0000-0002-7673-2289.

Bu makale, 2021 Yılında Sakarya Üniversitesi Sosyal Bilimler Enstitüsü, Sosyoloji EABD tarafından kabul edilen "Siber Dünyada Hacker Kültürü, Hacktivizm ve Bilişim Suçları" adlı yüksek lisans tez çalışmasından üretilmiştir.

Makale Gönderim Tarihi/Received: 23.05.2022.

Makale Kabul Tarihi/Accepted: 27.06.2022.

Atıf/Citation: Sandilaç, Nurullah. "Siber Suç, Siber Savaş ve Siber Terör Üçgeninde Siber Dünya." *Bilişim Hukuku Dergisi* 4, no. 1 (2022): 141-190.

between the concepts of cyber crime, cyber war and cyber terror. Basic research question with the subject: Are the concepts of cyber crime, cyber terrorism and cyber warfare different? If different, what are the factors that make it different? answers to the questions were sought. In this study, qualitative research method was adopted and document-based observation technique was used in accordance with the research design.

Keywords: Cyber Crime, IT Crimes, Cyber War, Cyber Terrorism, Cyber World.

GİRİŞ

Bilgisayar ve internetin ortaya çıkmasından sonra suçun sanal dünyada da işlenebilme kolaylığı görülmektedir. Tek bir tıklama ile dünyanın bir ucundan diğer bir ucuna siber saldırı yapılabilecek teknolojiye kavuşulmuştur. Dolayısıyla siber suçun, elektronik bilgi işlem kayıtlarına yasadışı yollarla erişilmesi veya bu kayıtların kanuni olmayan şekilde değiştirilmesi, silinmesi veya bilginin elde edilmesi için hazırlık yapılması olarak tanımlandığı görülmektedir.[1]

Siber alanda gerçekleştirilen suçlar ve saldırılar hızlı değişim gösteren konular arasındadır. Bu anlamda devletlerin mevcut yasalarında düzenleme yapması gerekmektedir. Aksi takdirde yasadaki boşluklar, sosyal hayatta önemli problemlerin meydana gelmesine neden olacaktır. Düzenleme yapılmadan önce siber alanda yaşanan değişimlerin takip edilerek, bunlara yönelik kavramların doğru şekilde tanımlanması zorunluluğu mevcuttur. Ancak bu alanda yaşanan gelişmeleri takip etmek ve uygun tanımları ortaya koymak hukukçuların karşılaştığı zorluklar arasındadır. Çünkü bu alanda bir hukukçu kimliğinin yanında internete, bilişim sistemlerine ve buna bağlı teknolojik ürünlere ilişkin kapsamlı bilgilere sahip olunması

---

[1] Emin Doğan Aydın, *Bilişim Suçları ve Hukukuna Giriş* (İstanbul: Doruk Yayınları, 1992), 27-28.

gerekmektedir. Günümüzde bilim ve teknoloji alanında yaşanan gelişmelerden ötürü bilim ve hukuk birlikte çalışmalı ve birlikte ilişki kurmalıdır.[2]

Hukukta kavramların ne anlama geldiği önem taşımaktadır. Bu nedenle çalışmamızda, siber dünyada işlenen bilişim suçlarının tek başına sadece bir suç olarak mı değerlendirilmesinin yerinde olduğu yoksa yöntem ve kullandıkları araçlar bakımından siber suç, siber terörizm ve siber savaş kavramlarının birbirlerinden farklı olarak mı değerlendirilmesi gerektiği, farklı ise farklı kılan etmenlerin neler olduğu şeklindeki sorulara cevap aranarak, siber alanda yaşanan teknolojik gelişmelere bağlı olarak kavramların doğru bir şekilde tanımlanmasına katkı sunulması amaçlanmıştır.

Bu çalışmamızla bilişim sistemi, siber suç, siber terörizm ve siber savaş konuları etrafında birinci bölümde, bilişim sisteminin ne olduğu hangi unsurlardan oluştuğu açıklanmıştır. Bilişim sistemlerinin temelde bilgisayar ve internetten oluştuğu kabul edilmekte olduğundan bilgisayar ve internet tarihinden bahsedilmiştir. Ardından suç kavramı açıklanmış, bilişim ile suç arasındaki ilişki açıklanmaya çalışılmıştır. İkinci bölümde siber ve siber saldırı kavramları açıklanmış, siber suçun saldırı aşamaları, türleri ve kullandıkları siber silahların nelerden ibaret olduğu izah edilmiştir. Üçüncü bölümde siber tehditlerin biçimleri olan siber suç, siber terörizm ve siber savaş kavramları açıklanmıştır. Sonuç bölümünde siber tehdit biçimlerinin ve eylemlerin birbirleriyle olan ilişkisi irdelenmiş ve farkları ortaya çıkarılmıştır.

Bu çalışmada, nitel araştırma yöntemine uygun olarak, belgelere dayalı gözlem tekniği uygulanmıştır. Bu nedenle alan yazında literatür taraması yapılmış olup kitap, dergi, makale, internet belgeleri, tez vb. dokümanlar incelenmiştir.

---

[2] Mehmet Yayla, "Hukuki Bir Terim Olarak 'Siber Savaş'," *Türkiye Barolar Birliği Dergisi,* no. 104 (2013): 178-179.

I. BİLİŞİM ALANINDA KULLANILAN KAVRAMLAR

A. Bilişim

Türk Dil Kurumu Türkçe güncel sözlüğünde bilişim "*insanoğlunun teknik, ekonomik ve toplumsal alanlardaki iletişiminde kullandığı ve bilimin dayanağı olan bilginin özellikle elektronik makineler aracılığıyla düzenli ve akla uygun bir biçimde işlenmesi bilimi"* şeklinde ifade edilmiştir.[3] Ayrıca bu kavram enformasyon kelimesiyle de ifade edilmiştir. Enformasyon kavramı ise Fransızca dilinde *informatique* kelimesinden doğmaktadır. Fakat daha sonra bu yabancı kökenli olan enformasyon kavramı bırakılarak Türkçe karşılığı olan bilişim kelimesinin kullanılması yaygınlık kazanmıştır.[4]

Yazıcıoğlu'na göre bilişim "*bilgisayardan da faydalanmak suretiyle bilginin saklanması, iletilmesi ve işlenerek kullanılır hale gelmesini konu alan akademik ve mesleki disipline verilen addır*."[5] Yenidünya ve Değirmenci'ye göre bilişim, "*teknik ekonomik, sosyal, hukuk ve benzeri alanlardaki verinin saklanması, saklanan bu verinin otomatik olarak işlenmesi, organize edilmesi, değerlendirilmesi ve aktarılması ile ilgili bilim dalıdır*."[6]

Dülger'e göre "*İnsanların teknik, ekonomik, siyasal ve toplumsal alanlardaki iletişiminde kullandığı bilginin, özellikle bilgisayar aracılığıyla düzenli ve akılcı biçimde işlenmesi, her türlü düşünsel sürecin yapay olarak yeniden üretilmesi, bilginin bilgisayarlarda*

---

3 Türk Dil Kurumu Sözlükleri, erişim tarihi: Haziran 21, 2022, http://www.sozluk.gov.tr.

4 Murat Volkan Dülger, *Bilişim Suçları ve İnternet İletişim Hukuku* (Ankara: Seçkin Yayınları, 2014), 65.

5 Recep Yılmaz Yazıcıoğlu, Bilgisayar Suçları: Kriminolojik, Sosyolojik ve Hukuksal Boyutları İle (İstanbul: Alfa Yayınevi, 1997), 131.

6 Ahmet Caner Yenidünya ve Olgun Değirmenci, *Mukayeseli Hukukta ve Türk Hukukunda Bilişim Suçları* (İstanbul: Legal Yayıncılık, 2003), 27.

depolanması ve kullanıcıların erişimine açık bulundurulması bilimidir."[7]

Dülger bilişim kelimesi yerine bilgisayar kelimesinin kullanılmasının yanlış olduğunu belirtmiştir. Bilişim bir bilim dalıdır. Bilgisayar ise makineyi ifade etmektedir. Dülger, bu sebeple bilişim kelimesinin bilgisayara göre daha geniş ve kapsayıcı bir kelime olduğu görüşünü doğru bulmamakta olsa olsa bilişim sistemi ile bilgisayar kelimelerinin karşılaştırılmasında bu açıklamanın doğru olduğunu ifade etmektedir.[8]

B. Bilişim Sistemi

Öncelikle sistemi açıklamaya çalışırsak; ortak bir hedef için bir arada çalışan, birbirine bağlı ve birlikte hareket etme kabiliyetine sahip parçacıklardan oluştuğu bir bütündür. Örnek olarak eğitim sistemi, ulaşım sistemi vb. sayabiliriz. Bilgisayarlar kullanılmak suretiyle oluşturulan bilgi sistemleri için de *Bilişim Sistemleri* veya *Bilgisayar Tabanlı Bilgi Sistemleri* kavramı kullanılmaktadır.[9]

Bilişim sistemi, veri ya da bilgileri alan, bu bilgileri işleme tabi kılan, sonuçları veya verileri çıktı şeklinde verebilen elektronik sistemler olarak tanımlanabilir.[10] Bilişim sistemi veya bilişim alanı, verileri toparladıktan sonra bunları otomatik işlemlere tabi kılma olanağı veren sistemlerdir.[11]

Avrupa Konseyi Siber Suç Sözleşmesi'nde, bilgisayar sistemi kavramının, bir ya da birden fazlası belirli bir yazılım

---

7 Dülger, Bilişim Suçları, 67.

8 Dülger, Bilişim Suçları, 68.

9 Davut Özkul, "Bilişim Sistemi Kavramı ve Bilişim Sistemlerinin Denetimi," *Sayıştay Dergisi* 13, no. 44-45 (2002): 14.

10 Hüseyin Akarslan, *Bilişim Suçları* (Ankara: Seçkin Yayıncılık, 2012), 27.

11 İsmail Malkoç, *Açıklamalı İçtihatlı Yeni Türk Ceza Kanunu-2. Cilt* (Ankara: Malkoç Kitapevi, 2007), 1665.

etrafında otomatik olarak veri işleyebilen bir aygıtıyla da birbirine bağlı ya da birbiriyle ilişkili bir dizi aygıtı olarak tanımlandığı görülmüştür.[12]

Türk ceza hukuku sisteminde bilişim sistemi ilk kez 20.09.2011 tarihinde Resmî Gazete'de yayınlanan Ceza Muhakemesinde Ses ve Görüntü Bilişim Sisteminin Kullanılması Hakkında Yönetmelik'in tanımlar ve kısaltmalar başlıklı 3'üncü maddenin ilk fıkrasının b bendinde "*Bilişim sistemi: Bilgisayar, Çevre birimleri, iletişim altyapısı ve programlardan oluşan veri işleme saklama ve iletmeye yönelik sistemi ifa eder"* şeklinde belirtilmiştir. Yönetmelikte bilişim sisteminin bilgisayardan ibaret görülmesi olarak tanımlanmasının hatalı olduğu belirtilmiştir.[13]

C. Bilişim Sisteminin Unsurları

1. Bilgisayar

Bilgisayarı icat edenler bu aygıta İngilizce olarak *computer* adını vermişlerdir. Günümüzde İngilizce dilinin dünyada yaygın olması nedeniyle *computer* kelimesi yerleşik hale gelmiştir. Ülkemizde ise, bilgi işlemek anlamından türetilerek "*bilgi saymak, bilgi vermek*" anlamlarını taşıyan bilgisayar kelimesi, *computer* kelimesinin yerine kullanılmaktadır.[14]

Bilgisayarın birçok tanımı yapılmakla birlikte hızla gelişen bilim ve yeni yeni üretilen teknolojik ürünlerin insan hayatına sokulması sonucunda bilgisayar hakkında yapılmış olan tanımlar eksik kalmış, bilgisayarın ne olduğunu tanımlamak zorlaşmıştır. Çünkü klasik bilgisayarı oluşturan unsurların dışında (fare, kasa, monitör) günümüzde bilgisayarın işlevini gören dizüstü bilgisayar, tablet, akıllı saat gibi yeni bilgisayar

---

[12] İsmail Ergün, *Siber Suçların Cezalandırılması ve Türkiye'de Durum* (Ankara: Adalet Yayınevi, 2008), 11.

[13] Yavuz Erdoğan, *Türk Ceza Kanunu'nda Bilişim Suçları (*İstanbul: Legal Yayıncılık, 2013), 16.

[14] Dülger, Bilişim Suçları, 55.

türleri çıkmıştır. Yine de genel anlamda bilgisayarın tanımına yer verecek olursak; bilgisayarın yaptığı işler ve işlevlerine göre ve bilgisayarın fiziksel özellikleriyle yaptığı işler ve işlevlerine göre, iki ayrı yöntem izlenerek tanımı yapılmıştır.[15] İlk tanımlamaya göre bilgisayar; "*yeterince kavramsallaştırılmış ve iyi tanımlanabilmiş her türlü problem üzerinde çalışabilen bir aygıttır. Bilgisayarı elektronik hesap makineleri ile programlanabilir aygıtlardan ayıran özelliği bilgisayarın bilişim özelliğine sahip olması yani bilgisayarın genel amaçlı kullanılabilmesidir*."[16] İkinci tanımlamaya göre bilgisayar; dış ortamdan farklı yöntemlerle aldığı verileri, içeriğinde barındırdığı yazılımları depo edip, işleyen, bu verilerden yeni sonuçlar çıkaran, çıkardığı sonuçları kullanan kişiye gösteren, bu itibarla veri iletişimi sağlayan makinedir.[17]

a. Bilgisayarın Unsurları

Bilişim sisteminin ilk unsuru olan bilgisayar çeşitli kısımlardan meydana gelir. Bilgisayar somut ve soyut parçalardan oluşur. Somut anlamda, bilgisayarın tüm fiziki parçalarına donanım, soyut anlamda ise, bu donanımların nasıl çalışacağını tespit eden fiziki olmayan kısmına ise yazılım denmektedir.

Donanım; mikro- işlemci, ROM, RAM, çevre/giriş-çıkış birimleri (yazıcı, fare, monitör, klavye, disket sürücüsü, tarayıcı, cd sürücüsü vs.) dir.

Yazılım ise verilerin elektronik biçimde toplanabildiği, depolanabildiği, işlenebildiği, belli bir komutu yerine getirebilmek için bilgisayara yüklenen ya da önceden bünyesine yerleştirilen bilgisayara işlerlik kazandıran komutlar bütününe denilmektedir. Doktrinde genelde kabul edilen ayrım; işletim

---

15 Dülger, Bilişim Suçları, 55.

16 Dülger, Bilişim Suçları, 56.

17 Yenidünya ve Değirmenci, *Mukayeseli Hukukta*, 19.

yazılımı ve uygulama yazılımı şeklinde tasnif edilmektedir.[18] İşletim yazılımı, bilgisayarın işletilebilmesi için yerine getirmesi gereken yazılımdır. Uygulama yazılımı ise, mevcut olan işletim sistemine yüklenen ve belli bir amaç için kullanılan programlardır.[19]

2. İnternet

Türkçe'de ağların ağı ya da ağlar arası olarak ifade edilebilen internet, birden fazla bilgisayarın birbirlerine bağlanarak, dünyada yaygınlaşan ve sürekli gelişen bir iletişim teknolojisidir. İnternet, insanların sürekli üretilmekte olan bilgiyi, saklayabilme, paylaşabilme ve ona kolayca ulaşabilme isteklerinden dolayı meydana gelmiş bir teknoloji ürünüdür. İnsanlar bu teknoloji sayesinde birçok alandaki bilgilere kolaylıkla, hızlı bir şekilde, güvenli ve ucuz olarak ulaşabilmektedir.[20]

İnsan, internet ile herhangi bir yerden bağlanarak elde ettiği bilgiyi bilgisayarına aktarabilmektedir. Ayrıca bilimsel bilgilere, devlet belgelerine, eğlence amaçlı oluşturulmuş listelere, iş ve kişisel ilanlara ve veri tabanlarındaki her türlü alandaki bilgiye erişmeyi ve bu bilgileri kullanmayı mümkün kılabilmektedir.[21]

a. İnternetin Ortaya Çıkışı ve Gelişimi

İnternetin kökenleri 1960 yılında Amerikan Federal Hükümeti Savunma Bakanlığı'na bağlı araştırma ve geliştirme

---

[18] Levent Kurt, Açıklamalı-İçtihatlı Tüm Yönleriyle Bilişim Suçları ve Türk Ceza Kanunundaki Uygulaması (Ankara: Seçkin Yayınevi, 2005), 31-36.

[19] Yenidünya ve Değirmenci, *Mukayeseli Hukukta*, 23-24.

[20] Aslan İnan, *İnternet El Kitabı* (İstanbul: Sistem Yayıncılık, 2000), 7-9.

[21] Tülay Bektaş Şeker, *İnternet ve Bilgi Açığı* (Konya: Çizgi Kitapevi Yayınları, 2005), 67.

birimi olan The Defense Advanced Research Projects Agency'e (DARPA)[22] dayandırılmaktadır.[23]

İlk önce ABD Savunma Bakanlığı, 1950 yıllarında SSCB'nin ilk yapay uydusu Sputnik'i uzaya göndermesine karşılık, ARPA isminde bir birim kurmuştur. ABD ve SSCB arasındaki soğuk savaş sırasında Amerikan ordusu, askeri verilerin ana bilgisayar kontrolünde diğer bilgisayarlarda da görünmesi ve tüm birimlerin aralarında kesintisiz iletişim sağlanabilmesi için bir ağ yapısı geliştirmeye karar vermiştir.[24]

ABD Savunma Bakanlığı 1969 yılında askeri araştırma projelerini ve çeşitli bilgisayar bilimlerini desteklemek için paket anahtarlamalı ağı yani ARPANET'i oluşturmuştur. Bu ağ daha sonra ABD'deki araştırma kuruluşlarında ve üniversitelerde kullanılarak büyümüştür. Bu ağ için 1973 yılında ise Stanford Üniversitesi,[25]Üniversite Koleji, BBN[26] ve Londra ile farklı bilgisayarların birbirlerini anlamak için protokol seti geliştirmek amacıyla internet working projesi başlatmıştır. 1978 yılına kadar farklı bilgisayarın birbirlerini anlayabileceği "*İletim Kontrol Protokolü*" (TCP) geliştirilmiştir. 1980 yılında bu protokol sabitleştirilmiştir ve ARPANET'e bağlı bilgisayarlar arasındaki iletişim kolaylaştırılmıştır. 1983 yılında ise tüm ARPANET kullanıcıları yeni bir protokol olan İletim Kontrol Protokolü/İnternet Protokolü'ne (TCP/IP) geçiş yapmıştır. Daha sonra ARPANET 1990 yılında kullanımdan kaldırılmıştır. Ancak

---

22 Savunma İleri Düzey Araştırma Projeleri Kurumu

23 Kürşat Çağıltay, *İnternet* (Ankara: METU PRESS, 1997), 5.

24 Ömer Sıddık Budak, "Bilişim Öğrencilerinin Siber Suç Farkındalığı: Erzurum İli Mesleki ve Teknik Liseler Örneği" (Yüksek lisans tezi, Atatürk Üniversitesi, 2015), 4.

25 Stanford Üniversitesi, ABD'nin Kaliforniya eyaletinde San Francisco'nun 40 km güneydoğusunda bulunan özel bir üniversitedir. Üniversite, şu anda dünyadaki en büyük bütçeye sahip 3. Üniversitedir.

26 Raytheon BBN Technologies, başlangıçta Bolt Beranek ve Newman isimli Amerikalı araştırma ve geliştirme şirketi

TCP/IP protokolünün kullanımı ve geliştirilme süreci devam etmiştir.[27] Daha sonra ARPANET askeri kolu MILNET sivil kolu NSFNET olarak ikiye ayrılmış ve kendisi INTERNET adını almıştır.

1970-1981 yılları arasında çeşitli ağlar oluşturulmaya başlanmıştır. Bunlar arasında UUCP (Unix-to-Unix Copy), bilgisayar bilimleri alanında çalışan 100'e yakın araştırmacının elektronik posta ile iletişim kurabilmesi amacıyla Wisconsin Üniversitesi'nde Larry Landweber adlı kişi tarafından THEORYNET, üniversitelerin bilgisayar bölümleri arasında araştırma gayeli bir bilgisayar ağı oluşturulması amacıyla 1979 yılında Wisconsin Üniversitesi, NSF ve DARPA arasında bir görüşme yaparak UUCP kullanılarak CSNET, BITNET, USENET kurulmuştur. 1986 yılında omurga hızı 56Kbps olan NSFNET kurulmasına müteakip NSF, ABD dahilindeki internetin belkemiği NSFNET'in ticari anlamda çalıştırılması amacıyla Michigan Üniversitesi, MCI ve IBM'nin oluşturduğu ve Merit Network Inc. ismi verilen konsorsiyum ile sözleşme imzalanmıştır. Bu şekilde bilgisayarların bir diğer bilgisayara bağlanmasına yarayan bir sistem kurulmuştur.[28]

1989 yılında internetin sivilleşme süreci başlamıştır. İsviçre'de Tim Bernard Lee adında bir araştırmacı Nükleer Araştırmalar Merkezi'nde çalışmıştır. 1992 yılında bu araştırmacı World Wide Web (WWW) adlı teknolojisini meydana getirerek interneti sivil kullanıma açmıştır. "WWW" teknolojisi ile her tür görsel/grafik unsuru barındıran sayfalar oluşturabilmeyi ve tıklamalar aracılığı ile bu sayfaların birbirlerine bağlanabilmesini sağlamıştır.[29] Daha sonra dünya genelinde kullanılan milyonlarca ağın da NSFNET'e bağlanması ile 1990 yıllarının başlangıcından günümüzde kullanılan haliyle internetin temeli kurulmuştur.

---

27 Çağıltay, *İnternet*, 5.

28 Çağıltay, *İnternet*, 7-10.

29 Bektaş Şeker, İnternet ve Bilgi Açığı, 68.

b. Türkiye'de İnternetin Gelişimi

Türkiye'de genel amaçlı kullanılan bilgisayar ağları, 1980 yılında üniversitelerin önderliğinde EARN'ın Türkiye'deki uzantısı olan, Türkiye Araştırma Kurumları Ağı (TÜVAKA) ile kurulmuştur.[30]

Türkiye'de internet hazırlıkları 1991 yılında ODTÜ ve TÜBİTAK tarafından oluşturulan TR-NET (Türkiye Internet Proje Grubu) adı altındaki proje grubu ile başlatılmıştır. İlk bağlantı Nisan 1993 yılında ODTÜ-Washington (Türkiye-ABD) arasında gerçekleştirilmiştir.[31] Sonraki bağlantı ise 1994 yılında Ege Üniversitesi'nde TUVAKA kapsamında BITNET bağlantısı amacı ile kullanılan uluslararası hat 64Kbps hız ile Bonn üzerinden internet servisi sunmaya başlanmıştır.[32] Ardından sonraki bağlantılar ise sırasıyla Bilkent Üniversitesi (1995 Eylül), Boğaziçi Üniversitesi (1995 Kasım) ve İstanbul Teknik Üniversitesi (1996 Şubat) bağlantılarını gerçekleştirmiş ve 1996 yılı ağustos ayında TURNET çalışmaya başlamıştır.[33]

TR-NET'in teknik ve idari yönetimi 1996 yılından sonra ODTÜ BİDB[34] tarafından üstlenilmiştir. İlk internet servis sağlayıcı olan TURNET servisinin devreye girmesi ile TR-NET'in de konumu değişmiş ve TR-NET akademi dışı kuruluşlara hizmet sağlayan bir internet servis sunucusu (ISS) olarak çalışmaya başlamıştır.[35]

Türkiye'de kendi omurgaları olan iki kuruluştan biri ULAKBİLİM, diğer ise TURNET'tir. Bunlardan ilki, akademik amaçlı bağlantılar amacıyla çalışmaya başlamıştır. Diğer ise ticari amaçlı faaliyetlerini sürdürmüştür. Daha sonra 1 Haziran

---

30 Çağıltay, *İnternet*, 24.

31 İnan, İnternet El Kitabı, 7

32 Çağıltay, *İnternet*, 24.

33 İnan, İnternet El Kitabı, 66

34 ODTÜ Bilgi İşlem Daire Başkanlığı

35 Çağıltay, *İnternet*, 25-26.

1996 yılında TUBİTAK çatısında Ulusal Akademik Ağ ve Bilgi Merkezi (ULAKBIM) ismiyle Yüksek Öğretim Kurulu'nun da yardımıyla yeni merkez kurulmuştur. TÜBİTAK, ULAKBİM'in yeni teknolojileri kullanarak ülke çapında bütün araştırma ve eğitim kurumlarını birbirine bağlayacak Ulusal Akademik Ağ (ULAK-NET) adıyla bir veri iletişim ağı kurmuş ve bilgi hizmetleri vermiştir. TUR-NET ise 1995 yılı içinde açtığı bir ihale ile, ilk ODTÜ-ABD bağlantısını sağlayan grubun da başlangıçta içinde olduğu bir konsorsiyum tarafından oluşturulmuştur.[36]

D. Suç Kavramı

Suç olgusu topluma, mekâna ve zamana göre farklı anlamlar barındırmaktadır. Herhangi bir zamanda veya herhangi bir yerdeki toplum tarafından suç olarak görülmeyen bir eylem farklı zamanda veya başka yerdeki toplum tarafından suç olarak kabul edilebilmektedir. Bu nedenle suç olgusunu tanımlamak kolay değildir.[37] Suç kavramının her toplumda oldukça farklı anlamları mevcut ise de bu kavramı hukuki boyutta ele almak gerekmektedir. Sözlük anlamında suç; "*toplum düzenini bozan, kanunlarca yasaklanan, hukuka aykırı davranışlardır*."[38] Başka bir tanımlamaya göre ise; "*hukuk düzeninin cezai müeyyide altına aldığı insan davranışlarıdır*."[39]

Suç dinamik ve sosyal bir olgudur. Dinamik olgudur çünkü toplumsal değişimler içerisinde farklılık göstermektedir. Sosyal olgudur çünkü birden fazla insanın olduğu yerde birine göre suç

---

36 İnan, İnternet El Kitabı, 68.

37 Senem Burkay, "Teorik Çerçevede Suç," *ETHOS: Felsefe ve Toplumsal Bilimlerde Diyaloglar* 2, no. 4 (2008): 2.

38 Fadime Dilber, "Kitle İletisim Araçları ve Suç Olgusu," *Karamanoğlu Mehmetbey Üniversitesi Sosyal ve Ekonomık Arastırmalar Dergısi* 16, no. Özel Sayı 1 (2014): 64.

39 Wilhelm Gallas, "Cezalandırılabilirliğin Temelleri ve Sınırları (Suç Kavramı Üzerine Düşünceler)," çev. İzzet Özgenç, *Selçuk Üniversitesi Hukuk Fakültesi Dergisi* 4, no. 1-2 (1994): 306.

olarak kabul gören bir davranış başka birine göre suç olarak kabul görülmeyen bir davranış ortaya çıkmaktadır. Örnek vermek gerekirse teknolojinin gelişmesiyle birlikte bilgisayar kullanımının yaygınlaşmasıyla bilgisayar aracılığıyla suçun işlenebilmesi mümkün hale gelmiş, bu şekilde bilgisayar suçları veya bilişim suçları ismi altında yeni bir suç tipi ortaya çıkmıştır. İlk olarak ABD'de işlenen bu suç tipi 1970'li tarihlerden itibaren tüm ülkelerde görülmüştür.[40]

Kanunların suç kabul ettiği cezai yaptırımlara bağladığı, hukuka aykırı eylem olarak nitelendirilen suç kavramı ve yaptırımları ancak kanunlar tarafından konulur ya da kaldırılır bu nedenden ötürü bir davranış kanunlarca suç olarak kabul edilmemiş ise hukuka aykırı bir davranış olsa dahi suç olarak kabul edilmemektedir.[41] Yani hukuki anlamda suçu ceza kuralı belirler. Eğer kural yoksa suç da yoktur. Ceza hukukunun temel ilkelerinden biri suç ve cezanın, yasada tanımlanmış olmasıdır. Özetle suç kavramını tanımlayacak olursak, ceza tehdidi altında yasaların yapılmasını yasakladığı olumlu ve olumsuz eylemler olarak ifade edebiliriz.

E. Bilişim ve Suçun Kesişimi

Bilişim ve iletişim; teknolojinin büyük hızla gelişmesine paralel olarak hayatımızın önemli bir parçası olmuştur. Gelişen teknolojinin kötüye kullanılmasıyla yeni suç alanları, araçları ve tipleri ortaya çıkmış; diğer bir ifadeyle bilişim teknolojisi, fiil ve fail tipolojisini temelden değiştirmiştir.[42]

Bilişim suçlarının hızlı evrimi ile hukukun ağır işleyen yapısı, problemlerin ortaya çıktığı noktada çatışmakta, hukukun nefesi bilişim suçlarına yetmemektedir.[43] Nitekim yasal

---

40 Burkay, "Teorik Çerçevede," 2.

41 Burkay, "Teorik Çerçevede," 3.

42 Erdoğan, Türk Ceza Kanunu'nda, 42.

43 Erdoğan, Türk Ceza Kanunu'nda, 43.

düzenlemelere ihtiyaç duyulması karşısında; mevzuat hazırlık süreci, yürürlük safhası, uygulamanın kamu ve özel sektörde sağlıklı şekilde yerleşmesi, olası eksiklik ve sorunların giderilmesi gibi süreçlerin eşzamanlı olarak etkin şekilde uygulanabilmesi her zaman mümkün olamamaktadır.[44]

Siber alanda sorumluluk bilinciyle hareket edilmemesi sonucunda bilgisayar sistemini kullanmanın etik ilkelerine aykırılık oluşturacağı gibi, bazı durumlarda hukuk kurallarını ihlale de sebebiyet verebilmektedir. Siber suçlar konusunda yapılan ve yapılacak hukuki düzenlemelerde suç politikasının evrensel nitelikteki temel ilkelerine uygun davranılması mecburiyeti vardır. Suç politikası, ceza hukukunun toplumu koruma görevini en iyi şekilde yürütmesi için hangi esaslar dahilinde düzenlenmesi gerektiği sorunuyla ilgilenmektedir. Bu sorunun çözümüyle ilgili olarak, suçun sebepleri üzerine odaklanır, ceza hukukunda uygulanan müeyyidelerin etkinliklerini araştırır, hukuku ihlal eden eylemlerin etkili biçimde önlenmesi için kanun koyucunun, ceza hukukunun kapsama alanını nereye kadar genişletebileceğini düşünür ve suç olayını en iyi belirleyen yasal unsurların neler olabileceğini inceler. Suç politikasında izlenen bu amaca ulaşmak için uyulması gereken temel ilkeler, kusur ilkesi, hukuk devleti ilkesi ve hümanizm ilkesi olarak tüm demokratik sistemlerde kabul edilmiştir. Suç politikasının evrensel nitelik kazanmış bu temel ilkelerine uyulmadan siber suçlar alanında yapılacak her normatif düzenlemede önemli yapısal problemlerin olacağı açıktır.[45] Bu nedenle bu çalışmamız ile bilişim suçları ile muhatap olan uygulayıcıların teknik terimler nezdinde; suçun oluşması ve işleniş şekillerinin anlaşılması açısından bu

---

[44] Burak Cesur Aköz, "Türk Ceza Kanunu Kapsamında Bilişim Suç ve Cezaları ile Örnek Yargısal Kararların Analizi ve Mevzuat Önerileri" (Bilişim uzmanlığı tezi, Bilgi Teknolojileri ve İletişim Kurumu, 2018), 21.

[45] Kayıhan İçel, "Avrupa Konseyi Siber Suçlar Sözleşmesi Bağlamında 'Avrupa Siber Suç Politikasının Ana İlkeleri'," *İstanbul Üniversitesi Hukuk Mecmuası* 59, no. 1-2 (2011): 3-4.

kavramların sağlıklı bir şekilde anlaşılması ehemmiyet arz etmektedir.

II. SİBER SALDIRI

A. Siber ve Siber Saldırı Kavramı

"Sibernetik" (*cybernetics*) sözcüğünün bir ön takısı olan "siber" kelimesinin, aynı zamanda sözcüğü kısaltmak amacıyla kullanıldığı görülmüştür.[46] Cyber sözcüğünden dilimize siber olarak tercüme edilmiştir. Bunun en önemli sebebi, siber kelimesinin gelişim süreci içerisinde yüklenmiş olduğu dönemsel anlam ve kültürel bütünlüğüdür. Merriam-Webster sözlüğünde "*cyber*" kavramının köken bilimsel olarak kökeninin "*cybernetic*"ten geldiği söz edilmektedir. "*Cybernetic*," otomatik hakimiyet sistemleri (sinir sistemi gibi) etrafında kontrol ve iletişim kuramının yer aldığı bilim dalı olarak tanımlanmıştır.[47] 1948 yılında sibernetik ilk defa, Norbert Weiner adlı Amerikalı bir bilim insanı tarafından "*makinelerde ve hayvanlarda iletişim ve hâkimiyet bilimi*" manasında kullanılmıştır.[48] Cyber ise, cybernetic'ten türemiş ve bilgisayar ağları için kullanıldığı belirtilmiştir. 1980 yıllarında, bilgisayar ağlarının online dünyası siber alan (*cyberspace*) olarak adlandırılmıştır. Bu dönemde "cyberpunk" akımının etkisiyle, rave/techno alt kültürü bünyesinde, teknolojiyi öğrenmeye ve etkin bir biçimde kullanmaya karşı arzulu, bağımsız kişiler "*hacker*" olarak anılmaya başlanmıştır.[49]

---

[46] Haydar Çakmak ve Cenker Korhan Demir, "Siber Dünyadaki Tehditler ve Kavramlar," iç. *Suç, Terör ve Savaş Üçgeninde Siber Dünya*, ed. Haydar Çakmak ve Taner Altunok (Ankara: Barış Platin Kitabevi, 2009), 25.

[47] Aslı Deniz Helvacıoğlu, "Avrupa Konseyi Siber Suç Sözleşmesi- Temel Hükümlerin İncelenmesi," iç. *İnternet ve Hukuk*, ed. Yeşim M. Atamer (İstanbul: İstanbul Bilgi Üniversitesi Yayınları, 2004), 277.

[48] Çakmak ve Demir, "Siber Dünyadaki," 25.

[49] Helvacıoğlu, "Siber Suç Sözleşmesi," 278.

Tekrardan bahsedecek olursak bilişim kelimesi, siber sözcüğünün ilerisinde bir manayı hedef göstermektedir. Bilişim ve siber kelimeleri ara sıra birbirinin yerlerine kullanılmış olsa da siber, elektronik sistemlerin bulunduğu alan, bilişim ise bu alandan aktif bir şekilde yararlanma ve bu ortam aracılığıyla bilgi işlenmesi/üretilmesi anlamlarını taşımaktadır.[50] Çalışmamızın ilerleyen bölümlerinde siber suç ve bilişim suçu kavramlarının durumu tartışılmıştır.

Siber saldırılar, devletler, kuruluşlar, teröristler, işletmeler veya kişilerin belli bir amaç doğrultusunda siber alanda gerçekleştirmiş oldukları saldırı faaliyetlerini ifade etmektedir. Siber saldırılar, altyapıyı, yazılımı ve donanımı hedef almaktadır.[51]

B. Siber Saldırı Aşamaları

Siber saldırıların genellikle 6 aşamada gerçekleştiği ifade edilmektedir. Bu anlamda sistemle ilgili bilgi toplama; sisteme sızma; sıradan kullanıcı girişi; ayrıcalıklı kullanıcı girişi; sistem kaynaklarının ele geçirilmesi; sistem kaynaklarının etkilenmesi aşamalarından oluşur. Birinci aşamada, bir sisteme saldırıda bulunmadan önce, o sistemle ilgili maksimum düzeyde bilgi toplamak gerekir. Bu bilgiler, internet üzerinden toplanabileceği gibi, istihbarat örgütleri aracılığıyla ya da sosyal mühendislik metotlarıyla da toplanabilmektedir. İkinci aşamada, toplanan temel bilgilerden sonra otomatik yazılım araçları (NMap, Nessus gibi) kullanılarak sistemin zafiyetleri araştırılır. Yani bilişim sistemine kolay şifre testi, önceki bilgileri kullanarak daha karmaşık şekilde tahmin yürütme ya da daha önce tespit edilen şifreler aracılığıyla girilmeye çalışılır. Üçüncü aşamada öncelikle sıradan kullanıcı yetkileriyle giriş sağlanarak sistemin kaynakları keşfedilmeye çalışılır (kullanıcı adları, servisler, ağ yapısı gibi). Bu aşamada ele geçirilen bilgiler ve sistemdeki

---

50 Çakmak ve Demir, "Siber Dünyadaki," 26.

51 Hasan Çiftçi, *Her Yönüyle Siber Savaş (*Ankara: TÜBİTAK Popüler Bilim Kitapları, 2013), 133.

güvenlik zaafları sayesinde, ayrıcalıklı kullanıcı yetkileri alınır. Dördüncü aşamada, sisteme ayrıcalıklı yetkileri elde ettikten sonra (*root*, *superuser*, *administrator*) kötü niyetli eylemleri gerçekleştireceği yetkilere sahip olunur. Beşinci aşamada ise saldırgan, sistemdeki bilgileri ileride birtakım bir bileşene (dosya sunucusu, web sunucusu, etki alanı sunucusu, veri tabanı sunucusu, güvenlik sunucusu vb.) saldırmak için kullanır. Ele geçirilen veriler de FTP (File Transfer Protocol) kullanılarak sistem dışına aktarılabilir ya da gelecek bir zamanda aktarılmak üzere saklanabilir. Son aşamada ise saldırgan, sistemdeki bilgi veya işlemleri, değiştirmek, bozmak veya yok etmek için zararlı programlar yükleyebilir ya da bu eylemleri bizzat kendisi yapabilir.[52]

C. Siber Saldırı Türleri

a. Kabloya Saplama Yapma (Wire Tapping)

Emniyete alınmamış iletişim ağ kablolarına, özel teçhizat kullanılarak fiziki anlamda saplama yapılması ve iletişim kurulmasıdır. Bu yöntem ile tüm trafiğin ele geçirilmesi mümkündür. Telefon trafiği de bu yöntemle dinlenebilmektedir.[53]

b. Tuzak Kapı (Backdoor)

İşletim sistemleri normal şartlar altında yetkisiz şekilde girişe veya herhangi bir program ya da kod çalıştırmasına ve değiştirilmesine izin vermeyecek şekilde tasarlanmaktadır. İşletim sistemlerini ve programları hazırlayan programcılar, ilerde ortaya çıkabilecek durumlara karşı hatta bulma amacıyla kod ekleyebilmek veya ara program çıktısı alabilmek amacıyla programa istediğinde "trap doors" adı verilen durma mekanizmaları eklerler. Bu gizli kapıların program ve işletim sistemi tamamlandığında temizlenmesi gerekir. Ancak bazı

---

52 Çiftçi, Her Yönüyle Siber Savaş, 135-138.

53 Çiftçi, Her Yönüyle Siber Savaş, 139.

durumlarda hata sonucu olarak ya da ileride kullanılmak amacıyla gizli kapılar kapatılmaz. Bu durumlarda gizli kötü niyetli kişiler tarafından kullanılabilmektedir.[54]

c. Hizmet Dışı Bırakma (Denial of Service, Dos)

Bilgisayarı veya bilgisayar sistemlerini hedef kullanıcı topluluğunun taleplerine cevap veremez hale getirmektir.[55] Hizmet dışı bırakmak için kullanılan yöntemler şunlardır:

- İletişim ağı bant genişliği, işlemci zamanı ya da disk alanı gibi kaynakların tüketilmesi,
- Konfigürasyon verilerinin bozulması,
- Sistem durum bilgilerinin bozulması,
- Sistem bileşenlerinin fiziksel olarak bozulması,
- Kullanıcı ve sistem arasındaki iletişimin kanalının kesilmesi[56]

d. Kriptografik Saldırılar

Şifrelenmiş mesaj veya verilerin şifresinin çözülmesi maksadıyla uygulanan saldırılardır. Temel prensibi güçlü bir algoritmanın güvenliği bütünüyle anahtarın içindedir; algoritmanın tasarım detaylarında değildir.[57]

e. Zamanlama Saldırıları

Kriptografik saldırıların özel bir türüdür. Kriptografi de kripto algoritmasının çalışması için geçen sürenin analiz edilerek kripto sisteme nüfuz edilmesi amacıyla yan kanal saldırısı yapılmasına "zamanlama saldırısı" adı verilmektedir. Bilgisayarda yapılan her işlem bir süre gerektirmektedir. Bu süre sisteme verilen girdiye bağlı olarak değişir. Hassas süre ölçümü

---

54 Ebru Altunok ve Ali Fatih Vural, "Bilişim Suçları," *Denetişim*, no. 8 (2011): 79.

55 Alper Başaran, *Siber Savaş Cephesinden Notlar (*İstanbul: Arion Yayınevi, 2016), 29.

56 Çiftçi, Her Yönüyle Siber Savaş, 140.

57 Çiftçi, Her Yönüyle Siber Savaş, 141.

yapılmak suretiyle kripto sistemin özelliklerine ve girdiye ulaşılması çalışılır.[58]

f. İnternet Servis Saldırıları

Bilgisayarlar birbirleriyle iletişim ağı aracılığıyla, internet protokol ve servisleriyle bağlanmakla ve iletişim kurmaktadır. İnternette kullanılan protokollerin (TCP/IP, FTP, Telnet, POP3, HTTP, SMTP, DNS, DHCP BGP gibi) zayıf noktaları veya bu protokolleri gerçekleştiren yazılımlardaki açıklıklar kullanılarak bilgisayarlara saldırı yapılabilmektedir.[59]

g. Trafik Analizi

İletişimin yakalanıp analiz edilerek iletişim örüntülerinden (*pattern*) bilgi çıkarma eylemidir. Burada, giden ve gelen verinin içeriğinden ziyade, verinin örüntüsü veya üst bilgisine bakarak sonuca varılır. Trafik analizi, mesajlar şifreli veya çok fazla miktarda olduğunda da uygulanabildiği için etkilidir. Mesajların deşifre edilmesine gerek duyulmaz. Özellikle askeri istihbarat birimleri tarafından uygulanarak düşmanın eylemleri ile ilgili veri toplanması amaçlanır. Örneğin çok fazla trafik, planlama yapıldığında, trafik olmayışı, planın sonuçlandırıldığına veya bir şeylerin beklendiğine, belirli noktalar arası trafiğin fazla olması, o noktalar arası organizasyonel bir ilişkinin olması anlamına gelebilir.[60]

h. IP Aldatmacası

Kullanılan bilgisayarın gerçek IP adresinin farklıymış gibi gösterilerek gerçek IP adresini gizlemek ya da başkasının yerine geçmek amacıyla kullanılan saldırı yöntemidir. IP aldatmacası, saldırganın kimliğini gizlemek için kullandığı yöntemlerden biri olduğundan, çok önemli bir yöntemdir. Hizmet dışı bırakma saldırılarında sıklıkla kullanılır.[61]

---

58 Çiftçi, Her Yönüyle Siber Savaş, 143.

59 Çiftçi, Her Yönüyle Siber Savaş, 144.

60 Çiftçi, Her Yönüyle Siber Savaş, 145.

61 Çiftçi, Her Yönüyle Siber Savaş, 145.

i. Zararlı Yazılım Kullanımı

Bilgisayar virüsleri işletim sisteminin ve makine dilinin verdiği olanaklar kullanılarak yazılan, kendi kendisini çoğaltabilen, kopyalarını çeşitli yöntemlerle başka bilişim sistemlerine ulaştırarak bu sistemleri de etkileyebilen zararlı yazılım (virüs, solucan, Truva atı vb.) yüklemek veya yüklenmesini sağlamaktır.[62]

j. Oturum Çalma

İki bilgisayar arasındaki oturumun çeşitli yöntemlerle ele geçirilerek karşıdaki bilgisayara yetkisiz giriş yapma hakkının kazanılmasıdır. Bu saldırıda saldırgan mağdur ve sunucu arasına da girip ikisi arasındaki tüm trafiği dinleyebilir.[63]

k. Yığın E-Posta (Spam) Gönderme

Yığın e-posta, benzer içerikli e-postaların çok sayıda kullanıcılara gönderilmesidir. Yığın e-posta göndericiler, internet sitelerinden, haber gruplarından, müşteri listelerinden, sosyal medya sitelerinden vb. e-posta adresi toplar. Adresler, genellikle reklam mesajları göndermek için kullanılır. Çeşitli kaynaklarda farklı sayılar olsa da yığın e-posta miktarının toplam e-postalarının %75 ile %86'sını oluşturduğu görülmektedir.[64]

l. Açık Mikrofon Dinleme

Açık mikrofon dinleme, casus bir yazılım aracılığıyla, bilgisayara sahibinin haberi olmadan, bilgisayarın mikrofonunu açarak ortam dinlenmesinin yapılmasıdır. Ayrıca benzer şekilde bilgisayarın kamerası da açılabilmekte ve görüntü alınabilmektedir.[65]

---

62 Altunok ve Vural, "Bilişim Suçları," 79.

63 Çiftçi, Her Yönüyle Siber Savaş, 146.

64 Çiftçi, Her Yönüyle Siber Savaş, 147.

65 Çiftçi, Her Yönüyle Siber Savaş, 147.

m. Sosyal Mühendislik

İnsanlar arasındaki iletişimdeki ve insan hareketlerindeki modelleri zaaflıklar olarak tanıyıp, bunlardan yarar sağlamak suretiyle güvenlik aşamalarını atlatma yöntemine dayanan müdahaleleri içermektedir. En fazla kullanılan sosyal mühendislik metotları şunlardır:

- Karşı taraftakini güvenilir bir kaynak olduğuna inandırmak,
- Hedef sistemin atıklarını karıştırmak,
- Ortak tanıdıklar üzerinden yakınlık kurmak,
- Başkasını taklit etmek,
- Gizlice zor bir durum meydana getirerek yardım ediyormuş görünümü vermek[66]

n. Ağ Tarama (Network Scanning)

İletişim ağından akan verilerin gözlenmesi veya iletişim ağına bağlı donanımların zafiyetlerinin araştırılması eylemidir. Saldırı maksatlı olarak yapılabileceği gibi sistemin güvenlik ve performansını test etmek için de yapılabilir.[67]

o. Yerine Geçme (Masquerading)

Bilişim sistemleri erişim imkanları bakımından sınıflara ayrılmaktadır. Bazı bilişim sistemleri erişim yetkisi bakımından geniş yetkilere sahipken, bazıları da sınırlı yetkiye sahiptirler. Sistem işleyişinde bu yetkiyi tanımlayabilmek için parola veya erişim kodu ister. Ancak bazı durumlarda ufak hileler sonucunda sınırlı erişim yetkisi olan kişilere erişim hakkı tanınabilmektedir. Yetkisi olmayan veya sınırlı erişim yetkisi olan bir kişinin, parola veya erişim kodunun yazılması veya ona özgü niteliklerin taklit edilmesi şeklinde yapılıyor ise yerine geçme olarak isimlendirilir.[68]

---

66 Çiftçi, Her Yönüyle Siber Savaş, 147.

67 Çiftçi, Her Yönüyle Siber Savaş, 148.

68 Olgun Değirmenci, "Bilişim Suçları" (Yüksek lisans tezi, Marmara Üniversitesi, 2002), 65.

p. Yemleme (Phishing)

İnternette bulunan web sayfalarının tıpatıp benzerini yaparak yani onun yerine geçerek kişilerin burada gizli bilgilerini ve şifre bilgilerini girmek suretiyle bu özel bilgileri elde etme eylemidir. Bu yolla kullanıcıları kandırmak için popüler sosyal web siteleri, açık artırma siteleri, çevrim içi alışveriş siteleri, bankacılık siteleri vb. taklit edilmekte ve kullanıcılar dolandırılmaktadır. Genelde kullanıcıların e-postalarına sanki bankadan veya kullanılan başka bir siteden geliyormuş gibi mesajlar yazılmakta, kullanıcının e–postada verilen bağlantıyı yani linke tıklaması sağlanmaktadır. Açılan internet sayfası da aynen taklit edilen siteninkine benzemektedir. Ancak gerçekte bağlanılan, erişilen yer farklıdır. Kullanıcının gözünden kaçması ihtimali çok yüksektir. Örneğin "www.Facebook.com" adresi yerine www.facebooki.com adresine bağlanılmaktadır. Kullanıcı burada kullanıcı adı ve şifresini girmekte hata mesajı almakta ve gerçek facebook sitesine yönlendirilmektedir. Bu şekilde kişilerin kullanıcı adı ve parolaları toplanmaktadır.[69]

D. Siber Silahlar

Siber tehditler amacıyla kullanılan araçlara siber silahlar denilmektedir. En çok kullanılan siber silahlar şunlardır:[70]

- **Adware:** Kullanıcıların istekleri dışında reklam amaçlı açılan internet sitelerine tıklandığında ana sayfayı değiştiren programlardır.
- **DoS (Denial Of Service):** Bir sistemin ya da bir yazılımın geçici olarak durdurulması veya tümüyle kilitlenmesini amaçlayan bir exploiterdir (sömürücü).
- **Fake Mail:** Kamu kuruluşların, alışveriş sitelerinin, şirketlerin, bankaların sayfalarına benzer sahte bir sayfa

---

69 Çiftçi, Her Yönüyle Siber Savaş, 149.

70 Çetin Gümüş, "Bilişim Suçlarıyla Mücadelede Polisin Eğitimi" (Doktora tezi, Fırat Üniversitesi, 2008), 16-19.

üretilerek kullanıcıların şifre ve bilgilerini elde etmeye yönelik bir formdur.

- **Keylogger:** Kullanıcıların şifrelerini takip etmek için klavye üzerinde basılan tuşların izlerini süren programlardır.
- **Sniffer**: Koklayıcı anlamında olup yerel ağdan şifrelenmemiş paketlerin kopyalanmasında ve bilgilerin elde edilmesinde kullanılır.
- **Spam Tool:** Bilgisayar kullanıcısının isteği dışında gönderilen reklam ya da e-postaların gönderildiği program çeşididir.
- **Spoofer:** Bilgisayar korsanlarının bilişim sistemlerine yetkili biriymiş gibi kendilerini göstermelerini sağlayan bir programdır.
- **Telnet:** Uzaktaki bilgisayara erişim sağlanırken yerel sunucuya bağlanıyormuş gibi kontak kuran terminal yazılımıdır.
- **Truva Atları (Trojan):** İlk bakışta zararsız gibi gözüken ancak içinde barındırdığı zararlı kodlarla bilişim sisteminin bozulmasına neden olan programlardır.
- **Virüs:** Bilgisayar verilerinin bozulmasına, silinmesine, çalışmasının engellenmesine, yavaşlatılmasına ya da başka problemlere sebep olacak şekilde oluşturulan programlardır.
- **Worm:** Worm aslında bir solucandır ve virüslere benzer. Bilgisayar korsanının açık bulduğunda bu zaafa odaklanıp kodları yayar ve makinelere kendi kendine kopyalar. Bunlar da verileri silebilir, şifreleri wormu yazana ulaştırabilir.

III. SİBER TEHDİTLER

Siber tehditler, siber suç, siber terörizm ve siber savaş terimlerinden oluşmaktadır. Şimdi bu kavramları açıklamaya çalışıp, farklarını ortaya koymaya çalışacağız.

A. Siber Suç veya Bilişim Suçu

1960 tarihinden itibaren Amerika'da siber suç eylemlerinin ortaya çıkmasının neticesi olarak Amerikan öğretisinde yaygın bir şekilde "bilgisayar suçları" (*computer crimes*) terimi kullanılmıştır. Diğer devletlerin hukukçularınca da benimsenmiş olup, Amerika'da bilişim suçları yerine bilgisayara karşı suçlar, bilgisayar suçu, bilgisayar ilişkili suç ya da bilgisayar yardımlı suç kavramlarının kullanıldığı görülmektedir.[71]

Siber suçlar, devletlerin mevzuatlarında tanımlanmış bir suç şekli değildir.[72] Bilişim teknolojilerinin kullanımı, yaygınlığı ve gelişmişliği ülkeden ülkeye değiştiğinden ve bilişim teknolojileri alanında sınır çizmek zor olduğundan bilişim suçu ile ilgili ortak tanımlama yapılamadığı görülmüştür.[73]

Ülkemizde de bu konuda bir kavram kargaşası mevcuttur. Bilgisayar suçu, internet suçu, siber suç, bilişim sistemi aracılığıyla işlenen suç, bilgisayar ile ilgili suç, bilgisayarlara karşı işlenen suç, bilişim suçu ve bilgisayarlar aracılığı ile işlenen suç vb. şeklindeki kavramların, bu alanı tanımlamak için kullanıldığı görülmektedir.[74]

Yukarıda bahsettiğimiz kavramların bazılarına yönelik söz konusu alanda eleştiriler mevcuttur. Örneğin ilk olarak internet suçu kavramından bahsetmek gerekirse; internetin bilişim suçları için zemin hazırlayan bir ağ olduğu, her ne kadar kullanımı kapsamlı olan bir ağ olsa da internet haricinde başka ağlardan da (intranet ve eksranet gibi) bilişim suçlarının işlenmesinin mümkün olduğu belirtilmiştir. Bu nedenle bilişim suçlarının işlenme ortamına göre farklı şekillerde isimlendirilmelerinin doğru olmadığı; örneğin kasten öldürme

---

71 Yenidünya ve Değirmenci, *Mukayeseli Hukukta*, 30.

72 Ergün, Siber Suçların Cezalandırılması, 12.

73 Akarslan, *Bilişim Suçları*, 33.

74 Dülger, *Bilişim Suçları*, 69-70.

suçunu işlendiği ortama göre adam öldürme, bina içinde işlenirse bina suçu, otobanda işlenirse otoban suçu, açık alanda işlenirse açık alan suçu gibi adlandıramıyorsak, bilişim suçlarının da işlendikleri ağa göre isimlendirmenin doğru olmadığı, olsa olsa internet aracılığı ile işlenen suçlar kavramının kullanılmasının daha uygun olduğu yönünde eleştiriler getirilmiştir.[75]

Siber suç kavramından bahsedildiğinde aslında bilişim suçundan söz edildiği anlaşılmaktadır. Bilişim suçları, aslında sadece bir bilişim sisteminde işlendiği anlamı taşımamaktadır. Ayrıca bu suçun, bilişim sistemi ağları aracılığıyla da (özellikle internet) işlenebildiği anlaşılması gerekmektedir. Bilişim suçu kavramının, siber suç kavramına göre bir üst kelime olduğu ve siber suçu da ihtiva ettiği eleştirisi mevcuttur.[76]

Ancak her ne kadar bilişim suçunun, siber suç kavramına göre bir üst kavram olsa da Avrupa Birliği ile müzakere sürecinde AB müktesebatına uyum adı altında yedi paket halinde yüzlerce yasada değişiklik yapılmıştır. Türk Ceza Kanunu, Ceza Muhakemeleri Usulü Kanunu, Medeni Kanun, Hukuk Usulü Muhakemeleri Kanunu gibi 80 yıllık temel kanunlar değiştirilmiştir. En önemlisi Avrupa Birliği'ne uyum sağlamak için Anayasa'nın değiştirildiği, 1949 yılından beri Türkiye'nin kurucu üyesi sayılmakta olduğu Avrupa Konseyi'nin "Siber Suç" kavramını kullanması ve özellikle son zamanlarda yapılan çalışmalarda siber suç kavramının tercih edildiği görülmektedir.[77]

Biz de bu görüşe katılmaktayız. Bu nedenle çalışmamızda dünyadaki gelişmeleri de kapsayan ve ifade eden "siber suç" kavramı kullanılmıştır. Ancak bilişim suçu kavramına yüklenen kültürel ve dönemsel anlam bütünlüğü de göz önüne alındığında geçmiş ve mevcut yasal düzenlemeler ışında Türk

---

75 Yenidünya ve Değirmenci, *Mukayeseli Hukukta*, 31-32.

76 Yenidünya ve Değirmenci, *Mukayeseli Hukukta*, 32-33.

77 Ergün, Siber Suçların Cezalandırılması, 14.

Ceza Kanunu'nda "bilişim alanında suçlar" kavramı hem öğreti de hem uygulamada görüş birliği halinde yerleşmiş olduğu ve tercih edildiği görülmektedir. Bu itibarla ülkemizdeki gelişmeleri ifade ederken siber suç kavramı yerine bilişim suçu kavramının kullanılması daha uygun olduğu görülmüştür.

Literatürde bilişim suçu kavramının tanımı incelendiğinde birçok tanım mevcuttur. Bilişim suçları izah edilmeye gayret edilmiş ise de üzerinde uzlaşılmış ortak bir tanım mevcut değildir.[78] Çünkü bir tanımlama yapılırken ne tür bir eylemin bilişim suçu olarak değerlendirilip hangilerinin bu eylem dışında bırakılacağı açıklığa kavuşmuş görünmemektedir.[79] Bilişim suçları altı farklı ölçüt dikkate alınarak tanımlanmaktadır. Bunlar: bilgisayarın amaç veya araç olmasını arayan tanım, bilişim suçlarını malvarlığı ihlalleriyle sınırlayan tanım, bilişim sistemleriyle herhangi bir şekilde ilişkili olan suçları esas alan tanım, bilgisayar kullanımını esas alan tanım, suçu işleyen faili esas alan tanım ve sınıflandırmaya tabi tutulamayan tanımlardır.[80] Yine de hukuk doktrinindeki tanımlardan birkaçına değinecek olursak; Aydın, *"elektronik bilgi işlem kayıtlarına yasadışı yollarla erişilmesi veya bu kayıtların kanuni olmayan şekilde değiştirilmesi, silinmesi veya bu tür kayıtlara girilmesi veyahut bilgi hırsızlığı için hazırlık yapılmasıdır."*[81] Ergün; *Bilişim "sistemleri ve bilişim teknolojileri kullanılarak bu sistemlerde ve bilişim ağlarında işlenen suçlardır"* şeklinde tanımlama yapmıştır.[82] Dülger; "*verilere ve/veya veri işlemle bağlantısı olan sistemlere veya sistemin düzgün ve işlevsel işleyişine karşı, bilişim sistemleri aracılığı ile işlenen suçlar"* şeklinde tarif yapmıştır.[83]

---

78 Berrin Bozdoğan Akbulut, "Bilişim Suçları," *Selçuk Üniversitesi Hukuk Fakültesi Dergisi* 8, no. 1-2 (2000): 549.

79 Dülger, *Bilişim Suçları*, 72.

80 Dülger, *Bilişim Suçları*, 72.

81 Aydın, *Bilişim Suçları*, 27-28.

82 Ergün, Siber Suçların Cezalandırılması, 16.

83 Dülger, *Bilişim Suçları*, 73.

Bu tanımlamalardan hareketle sonuç olarak bilişim suçu; veri işleyebilen, depolayan tüm elektronik cihazlara, yine bu sistemlerin aracı kılınması suretiyle doğrudan veya dolaylı biçimde yasa dışı yollarla erişilerek sistemi bozma, içindeki kayıtları silme veya bu kayıtları elde etme eylemi olarak görülmektedir.

1. Bilişim Suçlarının Yapısı ve Özellikleri

Bilişim suçunun işlenebilmesi için gerekli olan bilişim ortamının temel unsurları üçe ayrılmaktadır. Bilişim suçunun unsurlarından birincisi, bilgisayar ve bilgisayar benzeri akıllı cihazlardır. İkincisi, bilgisayar ve bilgisayar benzeri akıllı cihazlar arasında veri iletişimin sağlanabilmesi için gerekli bir iletişim ortamıdır. Üçüncüsü ise, bu bilgisayar ve benzeri cihazların çalışması için gerekli olan enerjinin (elektrik) sağlanmasıdır.[84] Bilişim suçunun en temel özelliklerinden bahsetmek gerekirse bu suçun işlenmesi oldukça kolay bir o kadar da tespit edilmesi ve cezalandırılması açısından zor olmasıdır.

2. Uluslararası Alanda Siber Suçların Sınıflandırılması

Siber suçların sınıflandırılmasında ortak bir ayırım yapılamamıştır. Birçok tasnifi mevcuttur. Strasbourg'daki 21 Kasım 2000 tarihinde Avrupa Topluluğu'nun 24 sayılı proje çalışmalarında siber suçların dört bölüm olarak tasnif edildiği görülmektedir. Bunlar; verilerin ve bilişim sistemlerinin kullanımına, bütünlüğüne ve güvenliğine ilişkin suçlar, manevi varlığa ve bununla alakalı haklara ait suçlar, bilişim suçları, muhteviyatı itibariyle suçlardır.[85]

---

[84] Akarslan, *Bilişim Suçları*, 37.

[85] Tezcan Özkan,"Siber Terörizm Bağlamında Türkiye'ye Yönelik Faaliyet Yürüten Terör Örgütlerinin İnternet Sitelerine Yönelik Bir İçerik Analizi" (Yüksek lisans tezi, Anadolu Üniversitesi, 2006), 69.

Avrupa Komisyonu'nun 2007 yılındaki tebliğinde; elektronik ağlara ilişkin suçlar, elektronik basın üzerinde yayınlanan yasa dışı muhteviyata ilişkin suçlar ve elektronik ağlar aracılığı ile işlenen klasik suçlar biçiminde de sınıflandırma yapılmıştır.[86]

Özcan'a göre bilişim suçları üç ana başlık altında toplanmaktadır. Bunun yanında teknolojiye paralel olarak sürekli artmaktadır. Birincisi, saldırı bir bilgisayarın kendisi hedefi olabilir. Bu şekilde bir bilgisayarın sunmuş olduğu hizmetler, bilgisayarın bütünlüğü ve gizliliği tehdit altındadır. Bu durumda bir saldırı gerçekleşirse bilgisayar maddi zarar görmektedir. İkincisi, suç işlemek amacıyla bilgisayar aracı kılınabilir. Üçüncüsü ise bilgisayarın hardiskinde depolanmaması gereken bilgilerin saklanması ile suça karışılabilir (pornografik videolar, resimler vb.).[87] Bir başka tasnife göre ise; kişilere karşı işlenen bilgisayar suçları, malvarlığına karşı işlenen bilgisayar suçları ve devlete karşı işlenen bilgisayar suçları şeklindedir.[88]

3. Siber Suç Türleri

Özcan siber suç türlerini belirtirken İnterpol'ün hazırladığı "İnterpol Bilgisayar Suçları Kılavuzu", Birleşmiş Milletler'in "Bilgisayar Bağlantılı Suçların Önlenmesi ve Kontrolüne İlişkin Birleşmiş Milletler El Kitabı" ve Avustralya Polis Teşkilatı'nın "Bilgisayar Temelli Suçların Soruşturulması için Asgari

---

86 Hakan Hekim ve Oğuzhan Başıbüyük, "Siber Suçlar ve Türkiye'nin Siber Güvenlik Politikaları," *Uluslararası Güvenlik ve Terörizm Dergisi* 4, no. 2 (2013): 137.

87 Mehmet Özcan, "Siber Terörizm ve Ulusal Güvenlik," iç. *İnternet ve Hukuk*, ed. Yeşim M. Atamer (İstanbul: İstanbul Bilgi Üniversitesi Yayınları, 2004), 305-307.

88 İbrahim Balcıoğlu, "İnternet Kullanımı ve Getirip Götürdükleri," *Somuncubaba Dergisi*, (2014): 66-67.

Hükümler" kitapçıklarından yararlanarak suç tiplerini belirtmiştir:[89]

a) Bilgisayar Sistemlerine ve Servislerine Yetkisiz Erişim

i. *Yetkisiz Erişim:* Bilgisayarın sisteminin bütününe ya da bir bölümüne, programlara, içerdiği bilgilere izinsiz ve yetkisiz olarak erişilen suçlardır.

ii. *Yetkisiz Dinleme:* Yetkisiz olarak bir ağ sisteminin ya da bilgisayarın teknik anlamda dinlenilmesidir. Teknik dinleme, iletişimin izlenerek verilerin dolaylı olarak ya da doğrudan elde edilmesi ile bağlantılıdır.

iii. *Hesap İhlali:* Başkasının hesabını kullanarak bilişim sistemlerine yetkisiz erişim sağlanarak yararlanmaktır.

b) Bilgisayar Sabotajı

i. *Mantıksal:* Bilgisayar veya iletişim sisteminin, işlevinin çalışmasını engellemek için bilgisayar verileri ya da programlarının bir kısım zararlı yazılımlar kullanılarak çalışamaz hale getirilmesi, ele geçirilmesi veya değiştirilmesidir.

ii. *Fiziksel:* Bilgisayar sisteminin çalışmaması için bilgisayarı oluşturan unsurlardan birine veya tamamına fiziki müdahalede bulunarak zarar verilmesini kapsamaktadır.

c) Bilgisayar Yoluyla Dolandırıcılık: İşlenen klasik suçların siber ortamda bilgisayar ve iletişim teknolojileri kullanılarak işlenme biçimidir. Bu durum kullanıcıya maddi ve manevi zarara uğratacak şekilde zarar vermektedir.

i. *Banka Kartlarını Kullanma:* ATM cihazlarına yönelik hırsızlık ve dolandırıcılık suçlarını kapsamaktadır. ATM'ye koyulan kopyalama cihazları, kamera gibi araçlar ile banka kartları çoğaltılır veya şifresi ele geçirilir.

ii. *Girdi/Çıktı/Program Hileleri Yapma:* Bilişim sistemindeki mevcut olan verilerin kasıtlı değiştirilmesi ya da sistemden sahte çıktı alınması veya mevcut programların değiştirilmesiyle yapılan hırsızlık ve dolandırıcılıktır.

---

[89] Özkan, "Siber Terörizm," 71-75.

iii. *İletişim Servislerini Haksız ve Yetkisiz Kullanma:* Kişinin kendisine maddi çıkar sağlamak için iletişim protokol servislerine ya da bilgisayar sistemlerine izinsiz şekilde girmektir.

d) Bilgisayar Yoluyla Sahtecilik: Bilişim sistemleri aracılığıyla sahte kâğıt para, senet, kredi kartı vb. materyaller üreterek ya da dijital belgeler üzerinde değişiklik yapılmasıdır.

e) Yasalar ile Korunmuş Bir Programın/Yazılımın İzinsiz Kullanımı: Yasalar ile hakları korunmuş olan programların izinsiz olarak kopyalanması, çoğaltılması ve dağıtılması ve kullanılmasını içerir.

i. Lisanssız Sözleşme İhlali

1) *Lisans Sözleşmesine Aykırı Kullanım:* Normalde bir bilgisayar için kurulması gereken programın birden çok bilgisayara yüklenmesi ve kullanılmasıdır.

2) *Lisans Haklarına Aykırı Çoğaltma:* Yazılımın lisans haklarına aykırı davranarak kopyalanmasıdır.

3) *Lisans Haklarına Aykırı Kiralama:* Yazılımların, oyunların ya da filmlerin lisans sözleşmesine aykırı bir şekilde kiralanmasıdır.

ii. *Taklitçilik:* Lisanslı yazılımın, yasalmış izlenimi verilerek kopyalanması ve satılmasıdır.

iii. *İzinsiz İthalat:* Lisanslı bir yazılımın ilgili kişilerden izin alınmadan ticaretinin yapılmasıdır.

f) Yasadışı Yayınlar: Kanunlar tarafından yasaklanan ve suç teşkil eden her türlü yayın, internet siteleri, e-postalar, haber grupları, dijital kayıtların muhafaza edilmesi, yayınlanması ve dağıtılmasıdır.

g) Diğerleri

i. *Ticari Sırların Çalınması:* Ekonomik menfaat sağlamak veya zarar vermek kastıyla yetkisi veya yasal izni olmadan yasa dışı yollarla bir ticari sırrın kullanılması, açıklanması veya elde edilmesidir.

ii. *Verilerin Suistimal Edilmesi:* Gizli bilgilerin, sırların kişilerin rızası alınmadan çıkar temin etmek veya zarar vermek kastıyla kullanılması, dağıtılması ve satılmasıdır.

iii. *Sahte Kişilik Oluşturma ve Kişilik Taklit Etme:* Kendisine menfaat sağlamak veya karşısındakine zarar vermek kastıyla hayali bir kişilik oluşturmak ya da başkasının bilgilerini kullanarak taklit etmektir.

4. Siber Suçları Geleneksel Suçlardan Ayıran Özellikler

Siber suçların, geleneksel suçlardan ayrıştığı noktalardan biri, işlenen suçların bilişim teknolojilerinin araç olarak kullanılmasıdır. Bilişim suçlarının, geleneksel suçlar ile benzerlik gösterdiği gibi ayrılıkları da mevcuttur:[90]

a. Siber suç olarak nitelendirilen eylemin sonuçları, başka bir devletin sınırları içerisinde görülebilmektedir. Uluslararası alanda suç işlendiğinde ise delil toplama çalışması zorlaşmaktadır.

b. Siber alanda işlenen suçlarda risk geleneksel suçlardaki gibi fazla değildir. Ayrıca birtakım devletlerde kanunda mevcut boşluklar nedeniyle suçun daha kolay işlenmesinde zemin oluşturmaktadır.

c. Siber alanda gizli kalma unsuru, suç işlemeye özgün bir ortam hazırlamaktadır.

d. Siber suçları işleyen kişiler incelendiğinde, bu kişilerin önceden birbirlerini tanımadıkları görülmektedir. Farklı ülkelerde yaşasalar dahi ortak iş yaparak siber suç eylemine iştirak etmektedirler. Hatta siber suçları iş birliği içerisinde yapanların aynı dili dahi kullanmadıkları anlaşılmaktadır.

e. Siber suç eylemine karşı alınan önlemler neticesinde, daha gelişmiş yöntemlerin ortaya çıktığı görülmektedir. Bu yöntemlerin sürekli gelişmesi ve çeşitlenmesinin temel nedeni ise teknolojinin hızlı bir biçimde gelişmesinden kaynaklanmaktadır.

---

[90] Ufuk Taşçı ve Ali Can, "Türkiye'de Polisin Siber Suçlarla Mücadele Politikası: 1997-2014," *Fırat Üniversitesi Sosyal Bilimler Dergisi* 25, no. 2 (2016): 231.

f. Siber suçların niteliği itibariyle suçlunun yakalanması için genellikle ortak bir çalışmayı, iş birliğini gerektirmektedir.

g. Siber suçları belli bir alanda sınırlandırmak ya da ortadan kaldırmak mümkün görünmemekte aksine yöntemler çoğaldıkça siber suçlar da çoğalmaktadır.

h. Çok az bir bilgi ile ciddi siber suçlar işlenebilmektedir.

i. Siber suçunu işleyenler arasındaki bağlantı, genellikle ekonomik ya da geçici özellikte olup, klasik bir organize suç örgütünün hiyerarşisi ve yapısı bu örgütlerde görülmemektedir. Ancak her siber suç eyleminde örgütlenmeden söz edemeyiz.

j. Siber suçlular, saldırılarını yapmak amacıyla anonimlik, güvenlik, esneklik ve kolluk birimlerinin engellemesine karşı mukavemet göstermesini sağlayan bir altyapıya gereksinim duymaktadırlar.

k. Siber suçlular, her ne kadar çok büyük tahrifat yapsalar da suçu siber alanda işlediklerinden dolayı herhangi bir sorumluluk duymamaktadırlar.[91] Yani gerçek yaşamda aynı mekânda bulunularak sözlü tacizin yapılması, çok ahlaki olmazken ve toplumda büyük bir çoğunluk bu eylemi yapmaya cesaret gösteremezken, internet ortamında yapılan sohbetlerde bireyler, sözlü tacizi kimliğini gizleyerek çok rahatlıkla yapabilmektedir.

B. Siber Terörizm

Siber terör, teröristlerin siber saldırı düzenleyerek, barajın kapaklarını açabilecekleri, askeri ordunun iletişim sistemlerine sızıp yanlış ve yanıltıcı bilgiler bırakabilecekleri, şehrin tüm trafik ışıklarını çalışamaz hale getirebilecekleri, bilişim sistemlerini bozabilecekleri, yolları bozabilecekleri, finans ve bankacılık alanını çökertebilecekleri, kamu kurumlarının

---

91 Nurullah Sandilaç, "Siber Dünyada Hacker Kültürü, Hacktivizm ve Bilişim Suçları" (Yüksek lisans tezi, Sakarya Üniversitesi, 2021), 51.

faaliyetlerini (kolluk, acil yardım, hastane ve itfaiye çalışmaları vb.) engelleyebilecekleri ve nihayet hükümet kurumlarını alt üst edebilecekleri bunun sonucunda da sistemin durdurulabileceği bir siber tehdit unsurudur.[92]

Siber terörü iyi anlamamız için öncelikle terör ve terörizm kavramını açıklamamız gerekmektedir. Ancak her devlet, terör kavramının tanımını kendi politikalarına göre yorumlamaktadır. Bu sebeple, her devlet, uluslararası terör saldırılarını tanımlarken, kendisini hedef alan saldırıları kapsayacak biçimde ve gelmekte olan ya da gelme ihtimali olan dahili ve harici düşmanlarının olası saldırılarını, uluslararası kanuna göre yasa dışı görmek istemektedir. Bununla birlikte her devlet, herhangi bir şekilde otoritelerini kötü biçimde etkiyebilecek ifadelerden uzak durmaktadır. Neticesinde, bir ülke tarafından terörist olarak yaftalanan kişi ya da kişiler, diğer bir ülke tarafında da "özgürlük savaşçısı" olarak görülmektedir.[93] Bu nedenle terörün tanımında uzlaşma tam olarak sağlanamamaktadır.

Terör, sosyolojik açıdan, siyasi yapıda yer alan faaliyettir. Temelde hedef olarak tespit ettiği bireyin, grubun veya toplumun ardındaki yönetim felsefesine, yani legal veya illegal kabul edilmiş olan egemenlik ilişkisine saldırır. Bu faaliyetlerin, otoriter bir yönetime yönelik yapılıyorsa haklı bir tepki, demokratik bir yönetime yönelik yapılıyorsa haksız bir tepki olarak algılanmaktadır. Demokratik yönetimlerde bu faaliyetlerin kabul edilmeyişinin nedeni ise, demokratik yönetimlerdeki egemenlik ilişkisinin, yani yönetim felsefesinin toplumun isteğine ve kabulüne bağlı olmasından kaynaklanmaktadır. Bu egemenlik ilişkisine yapılan saldırılar,

---

92 Sedat Sertoğlu, "Büyük tehlike," Sabah Online, son değiştirilme Aralık 6, 1999, http://arsiv.sabah.com.tr/1999/12/06/y11.html.

93 Mehmet Yayla, "Siber Savaş ve Siber Ortamdaki Kötü Niyetli Hareketlerden Farkı," *Hacettepe Hukuk Fakültesi Dergisi* 4, no. 2 (2014): 195.

doğrudan egemenlik ilişkisini dönüştürmeye ve bu ilişkiye hakim olmaya yönelik olduklarından ve insanların da ölümüne neden olduklarından, tanım gereği bu eylemi yapan kişi veya kişiler, terörist olarak nitelendirilmektedir.[94]

Yine de terörün tanımını yapmak gerekirse "*şiddet kullanma ya da şiddet tehididi barındıran anormal yollarla siyasal davranışları etkilemek üzere tasarlanmış sembolik bir fiildir.*"[95] Ayrıca terör, 3713 saylı Teörörle Mücadele Kanunu'nun 1. maddesinde "*cebir ve şiddet kullanarak; baskı, korkutma, yıldırma, sindirme veya tehdit yöntemlerinden biriyle, Anayasada belirtilen Cumhuriyetin niteliklerini, siyasi, hukuki, sosyal, laik , ekonomik düzeni değiştirmek, Devletin ülkesi ve milletiyle bölünmez bütünlüğünü bozmak, Türk Devletinin ve Cumhuriyetin varlığını tehlikeye düşürmek, Devlet otoritesini zaafa uğratmak veya yıkmak veya ele geçirmek, temel hak ve hürriyetleri yok etmek, Devletin iç ve dış güvenliğini, kamu düzenini veya genel sağlığı bozmak amacıyla bir örgüte mensup kişi veya kişiler tarafından girişilecek her türlü suç teşkil eden eylemlerdir"* şeklinde tanımlanmıştır. Terörizm ise şiddetin sistematik olarak kullanıldığı bir yöntem biçimidir ve aşağıda belirtilen özelliklere sahiptir:

- Önceden planlanmıştır ve korku iklimi yaratmak amacıyla tasarlanmıştır,
- İlk (yakın) mağdurlardan çok daha geniş bir hedefe yönlenmiştir,
- Sivilleri de içine alan rastgele ve sembolik saldırıları içerir,
- Toplum tarafından anormal olarak nitelendirilir,
- Görünürde ayrımcı olmasa da aslında gerçek anlamda ayrımcı bir yapıya sahiptir,

---

94 Emre Kongar, *Küresel Terör ve Türkiye (*İstanbul: Remzi Kitapevi, 2002), 73-74.

95 Çakmak ve Demir, "Siber Dünyadaki," 36.

- Öncelikle, hükümetlerin ve toplulukların siyasi davranışlarını etkilemek için kullanılır.[96]

Yukarıda ifade edilenlere göre; terör örgütünün herhangi bir devlet kurumuna yöneltilecek saldırının temel amacı o kurumun hizmetlerini tamamen sona erdirmek değil, kitlelerin gözünde devleti küçük düşürmek ve toplumda korku duygusunun hâkim olmasını sağlamaktır. Nereye ve kimlere güvenileceğini bilemeyen toplumun paralize (toplumsal felç) edilmesi kolaylaşır ve terörizm de böylelikle nihai amacına ulaşır.[97]

Terör örgütleri siber ortamda sıklıkla internetin sağladığı kolaylıklardan faydalanır. İnternet, teröristler için eşi bulunmaz avantajlar sunmaktadır. Bu avantajlardan bazıları; merkezi bir kontrolden uzaklığı, herhangi bir sınırlamaya uğramaması, isteyen herkesin ulaşımına açık olması, hızlı bilgi akışı, diğer iletişim metotlarına göre ucuz ve kolay olması, multimedya ortamı sağlaması, anonimlik halinin elverişli olması şeklindedir. Bunların dışında internet özellikle hayli küçük grupların kendilerini duyurabilmesi için de önemli fonksiyon görür.[98] Bir kısım terör eylemleri siyasi olmakla birlikte, her siyasi eylem de terör niteliği taşımamaktadır. Bir saldırının terör olarak tanımlanabilmesi için "eylem, örgüt ve ideoloji" unsurlarının bir arada bulunması elzemdir. Belirtilen unsurlardan birinin eksik olduğu takdirde, o eylemin terörizm eylemi dışında bir sınıflamaya tabi tutulduğu görülmektedir. Örneğin bir politik nitelik taşımayan şiddet hareketleri (ırk-mezhep kavgaları) örgütlü görünseler dahi, bu gruplar organize suç faaliyetleri olarak değerlendirilmemesi gerekmektedir.[99] Çünkü toplumda korku duygusunu oluşturma, devletin egemenliğe saldırı gibi ideolojik unsuru ve buna yönelik doğrudan bir eylemi

---

96 Çakmak ve Demir, "Siber Dünyadaki," 36.

97 Çakmak ve Demir, "Siber Dünyadaki," 37.

98 Çakmak ve Demir, "Siber Dünyadaki," 38.

99 Özkan, "Siber Terörizm," 6.

bulunmamaktadır. Bu tür küçük gruplar arasında eylem, örgüt ve ideoloji unsurları birbirleriyle uyumlu bir şekilde bulunmamaktadır.

Siber terörizm ise, terörizmde belirtilen özellikleri taşımak suretiyle siyasal içerikli olup siber alanda, bilgisayar sistemlerine karşı sızma, ihlal etme veya bozma eylemlerinin gerçekleşmesi ya da gerçekleştirme tehdidi gibi bir eylemin sebep olduğu engellenme sonucu, milyonlarca insanın davranışını etkileyerek günlük yaşamını bozmaktır.[100] Stanford Üniversitesi, Uluslararası Güvenlik ve İşbirliği Merkezi (CISAC), Hoover Kurumu ve Bilgi Güvenliği ve Politikaları Alanında Araştırma Konsorsiyumu başkanlığında 9 kişilik bir gruba yaptırdığı siber suçlar ile ilgili bir çalışmada siber terörizmi "*Hukuken yetkili kılınmış görevlilerin eylemleri dışında, siber sistemlere karşı girişilen ve kişi veya kişilerin ölümü veya yaralanması, kamu düzeninin bozulması veya önemli ekonomik zararlara veya mallara karşı önemli zararlara neden olması muhtemel olan şiddet, bozma ve engelleme eylemlerinin kasıtlı şekilde yapılması veya yapılacağı tehdidi* şeklinde tanımlamıştır."[101]

Başka tanımlara göre ise siber terörizm, siyasi ya da sosyal amaçların gerçekleştirilmesi için bir ülkeyi ya da halklarını aşağılamak ya da korkutmak için bilgisayarlara, ağlara ya da verilerin saklandığı bölümlere gerçekleştirilen yasadışı saldırı ya da saldırı tehditleridir. Siber terörizm, bilgisayar ve iletişim teknolojisi yeteneklerinin siyasi olarak motive olmuş ulus-altı gruplar ya da ajanlarca şiddet, bir toplumu etkilemek ya da bir hükümetin politikalarını değiştirtmek gayesiyle silah ya da hedef olarak kullanılması biçiminde de tanımlanabilir.[102]

Siber terörizm, sadece bilgisayar ve ilgili teknolojilerin bir araç olarak kullanılmasını değil, bir hedef olarak belirlenmesini

---

[100] Çakmak ve Demir, "Siber Dünyadaki," 39.

[101] Özcan, "Siber Terörizm," 309.

[102] Yayla, "Siber Savaş," 195.

işaret etmektedir. Ancak sınır aşan organize suç örgütleri ile terörist örgütlerin eylem alanlarının ve yöntemlerinin yakınlaştığı günümüzde bilgisayarın araç olarak kullanıldığı bazı örnekler konunun karmaşıklaşmasına sebep olmaktadır. Örneğin mali alt yapısının kredi kartı sahteciliğine dayandığı bir terör örgütünün, temel eylemi kredi kartının sahtesini üretmek olduğundan bilgisayarların bu amaçla kullanılması sadece fiilin niteliğini değiştirmektedir. Bu nedenle salt bu gibi eylemler siber terörizm olarak değerlendirilemez. Ancak terör örgütünün kamuya açık bir alanda güvenlik kuvvetlerinin elektronik sistemlerine girilmesi suretiyle gerçekleştireceği eylemlerde ve bunun sonucunda insanlarda yaralanmalara, ölümlere yol açarak toplumda korku, kaygı ve panik duygusunu yaratması siber terörizm kapsamı içinde değerlendirilebilir.[103] Görüldüğü üzere siber suçlarla siber terörizmi birbirinden ayıran temel etken, eylemin siyasal bir sebeple işlenmesi, bilişim teknolojilerinin, araç veya hedef olarak kullanılması ve bunun sonucunda toplumda panik duygusunu yaratması gerçeği yani suçun terörden ayrıldığı noktada ortaya çıkmaktadır.

Bu açıklamalar doğrultusunda siber terörün, klasik terörden farkını Özcan altı maddede açıklamıştır:

- Öncelikle terör örgütleri geleneksel anlamda faaliyetlerini bir nebze de canlarını da gerektiğinde ortaya koymadırlar. Eline silah ya da bomba alan bir terörist ihtimaldir ki bir polis ya da asker tarafından etkisiz hale getirilsin. Fakat dünyanın herhangi bir yerinde internete bağlanan bir siber terörist canını tehlikeye atmadan ülkenin toplumsal yaşamına ciddi zarar vererek eylemini gerçekleştirebilir. Ayrıca siber terörizm kamu binaları gibi terörist eylemlerin hedefi olan yerlerin fiziki güvenliklerinin artırılmalarının yanında daha cazibeli hale gelmektedir. Çünkü, siber terörist kendine çok daha güvenli bir ortamda eylemlerini hazırlayabilmektedir.

[103] Çakmak ve Demir, "Siber Dünyadaki," 39-40.

- İkincisi ise terörün asıl gayesinden yola çıkarak ulaşılan farklı sonuçlardır. Terörün asıl gayesi, yapacağı terör eylemleri ile topluma ve hükümete mesaj vermektir. Ancak siber terörde şiddet araç olmaktan farklı olarak amaç haline dönüşebilmektedir. Bilgisayar aracılığı ile bir siber terörist finans kurumlarının, büyük bankaların ve borsa bilgilerini ve iletişimini mahvedebilir. Bu şekilde toplumun ekonomik yaşamı sekteye uğrayabilir. Ya da bir ilaç firmasının sistemine girerek ilaç içeriğine dair bilgilerde en ufak bir değişiklik yapıldığında dahi binlerce insanın hayatına mal olabilmektedir.
- Üçüncüsü ise klasik terör faaliyetleri ile yapılmak istenen propaganda geniş kitlelere her ne kadar ulaşabilse de aslında eylem itibariyle lokaldir. Yani bir terör eyleminde hedef alınan bir kamu binasına yapılan bombalı saldırı sonucu çökebilir ve sadece orda bulunan insanlar hayatını kaybedebilir. Ancak siber terörde ise eylemin etki alanı klasik terörden çok daha fazladır. Bir terörist, oturduğu yerden, hedef aldığı sisteme sızarak, sistemi çökertebilir. Bu zararın etki alanı ise ülkenin geneline yayılmaktadır. Böylelikle insanların gündelik hayatına daha fazla etki edebilmektedir. Örnek vermek gerekirse operatör şirketlerinden herhangi birine yapılacak saldırı sonucu sızılan bilişim sisteminde bir siber terörist tüm telefon faturalarını artırabileceği gibi azaltabilir. Bu durumda şirketin uğrayacağı zarar ile toplumsal huzursuzluk, devlet kurumuna yapılacak terör faaliyetinden daha fazla olabilmektedir.
- Dördüncüsü, siber terörizmin psikolojik yanı, bilgi teknolojilerini kullanan birey, grup, toplum ve devletlere kadar uzanabilmektedir. Hedefler gerçek ancak sembolik olmadığından, klasik terörizm kadar yaygın dalga içermemektedir. Ayrıca siber terörde bugüne kadar ölüm ve yaralanma gerçekleşmediğinden kamuoyundan duygusal bir tepki daha az doğmaktadır.
- Beşincisi, klasik terör eylemlerinde seçilecek elemanın genelde belirli bir yaşın üzerinden seçilmektedir. Ancak siber terörde böyle bir sınırlama bulunmamaktadır. Çünkü bilgisayar kullanımı çocuk yaştaki birisinin bile kolaylıkla öğrenebileceği,

kullanabileceği bir teknolojidir. Bu nedenle siber terörde çocuklar araç olarak kullanılabilmektedir. Ortaokul ve liseli gençler, devlet kurumlarına macera arayışı ile bir hevesle saldırmaktadırlar.

- Son olarak klasik terörde, teröristler eylemlerini silah ya da bomba gibi araçlarla gerçekleştirmekte iken siber terörde ise bilgisayar ve internet gibi araçları kullanarak eylemlerini gerçekleştirmektedirler.[104]

Siber terörizm ile ilgili karşıt görüşler de mevcuttur. Örneğin Joshua Green, "The Myth of Cyberterroism" başlığını taşıyan makalesinde bilgisayarlar tarafından öldürülen insanların olmadığını, devletlerin çok gizli ve güvenlik gerektiren bölgelerinde internet bağlantılarının bulunmadığını ifade ederek siber terörizm kavramının abartıldığı belirtmektedir.[105]

Akman'a göre, siber terörizm kavramı; 2002 yılında yazılan "The Next War Zone" (Geleceğin Savaş Bölgesi) adlı kitapta ortaya atıldığını ifade etmiştir. Bu kitap, Amerika Birleşik Devletleri Hükümetinin görüşlerini dile getiren bir çalışma olduğunu, bu çalışmada Irak, Kuzey Kore ve Çin'in de ellerinde "Kimyasal Başlıklı Füzeler", "Zehirli Gaz Bombası Atan Uzun Menzilli Silahlar" olduğu; bu ülkelerin, sahip oldukları bu silahları "Sibernetik Sistemler"e yönlendirerek başka ülkelere fırlatma gücüne sahip bulundukları için yakın bir gelecekte, bir "siber terörizm" yaratacakları şeklindeki iddiaları içermektedir.

Siber terör uzmanları şu an için çalıntı araçların, bomba yüklü kamyonların ve biyolojik silahların siber terörizmden daha büyük bir tehlike yarattığından bahsetmektedirler. Siber

---

104 Özcan, "Siber Terörizm," 311-313.

105 Çakmak ve Demir, "Siber Dünyadaki," 35.

terör tehdidi abartılmış olarak gözlemlense de ne yok sayılabilir ne de göremezlikten gelinebilir.[106]

Siber terörizmin gerçekleştirilebilirliği tartışma konusudur. Çünkü bugüne kadar devletlerin güvenlik sistemlerine oldukça zarar veren herhangi bir siber terörizm saldırısı meydana gelmemiştir. Bunun nedeni ise devletlerin önemli yerel ağ sistemlerini, genel ağ sistemlerinden ayırmalarından kaynaklanmaktadır. Ancak bu durum gelecekte böyle bir saldırı olmayacağı anlamına da gelmemektedir.[107]

C. Siber Savaş

Savaş kavramı, ulus ya da devlet içerisindeki düşmanlar arasında meydana gelen, açıkça ilan edilmiş silahlı çatışmaları tanımlamak için kullanılmaktadır. Siber savaş ise, rakip devletlerin siber ortamdaki siber saldırılarını ifade etmektedir. Ancak hangi siber saldırıların, siber savaş kapsamında değerlendirilmesi gerektiği konusunda görüş birliği bulunmamaktadır. Bunun nedeni olarak kimileri; siber savaşa gerektiğinden çok ehemmiyet verildiğini, meydana gelecek bir siber saldırının, savaş nedeni olarak kabul edilemeyeceğini, ülke kaynaklı siyasi bir siber saldırının, savaş kadar eski olan casusluk, sabotaj veya tahrip maksatlı bir saldırı ile aynı neticeyi doğuracağını ve konvansiyonel anlamda silahlı kuvvet kullanılmayacağını savunmaktadırlar. Bunun yanında İran,[108]

---

106 Taner Altınok ve Zeynep Kaya, "Siber Tehditlerle Mücadele," iç. *Suç, Terör ve Savaş Üçgeninde Siber Dünya*, ed. Haydar Çakmak ve Taner Altunok (Ankara: Barış Platin Kitabevi, 2009), 160.

107 Çakmak ve Demir, "Siber Dünyadaki," 43.

108 2010 yılında ABD ve İsrail'in, İran'ın nükleer çalışmalarını sekteye uğratmak için kullandığı Stuxnet adlı solucan yazılımı ile gerçekleştirdiği siber saldırı olayı.

Gürcistan[109] ve Estonya'ya[110] yönelik yapılan siber saldırılar, siber savaşın ehemmiyetini gözler önüne sermekte, savaş hukuku ve uluslararası çerçevesinden konu değerlendirilmektedir. Rakip ülke ya da devlet destekli alt grupça yapılacak bir siber eylemde, siber saldırıya uğrayan devlet tarafından Birleşmiş Milletler Antlaşması'nın 51. maddesindeki "meşru müdafaa hakkı"nın kullanılabileceği düşünülmek ve savunulmaktadır.[111]

Görüş birliğinin olmamasının bir başka neden ise, gelişen teknoloji karşısında bilgi çağı öncesi düzenlenen Birleşmiş Milletler Antlaşması'nın, siber ortamdaki gelişmeleri ve potansiyel tehditleri öngörememesidir. Örneğin silahlı çatışma olarak ifade edilen konvansiyonel savaştan farklı olarak siber ortamda gerçekleşen siber saldırılarda silah kavramının ne olduğu, siber saldırıda kullanılan araçların silah kapsamında değerlendirilmesi gerekip gerekmediği tartışma konusu olmuştur.

ABD Başkanı George W. Bush'un siber güvenlik danışmanı olarak çalışmış olan Richard Clark'e göre siber savaş, bir ülkenin, başka bir ülkenin bilgisayar sistemlerine ya da ağlarına zarar vermek veya kesinti yapmak üzere gerçekleştirilen sızma faaliyetleridir.[112] Yine ABD Genelkurmay Başkanlığı siber savaşa yakın bir anlam içeren tanım yapmış olup, "bilgi savaşı" kavramını kullanmış ve "*düşmanın insan ve araç kaynaklı karar alma sistemlerini etkilemek, etkinliğini azaltmak, bozmak veya ele geçirmek buna karşın kendi sistemlerini korumak*" olarak tanımlamıştır. Birleşmiş Milletler Terimler Sözlüğü'nde, siber

---

[109] 2008 yılında Rusya Federasyonu'nun Gürcistan'a yönelik konvansiyonel saldırısını gerçekleştirmeden önce bu saldırıyı desteklecek şekilde planlama yaptığı ve gerçekleştirdiği siber saldırı olayı.

[110] 2007 yılında Estonya Parlementosu'nun Tallinn Meydanı'ndaki Bronz Asker anıtını kaldırma kararından sonra Rusya Federasyonu tarafından gerçekleştirdiği iddia edilen siber saldırı olayı.

[111] Yayla, "Siber Savaş," 183-184.

[112] Çiftçi, Her Yönüyle Siber Savaş, 5.

savaş (*cyberwar*) bilgi savaşı (*information warfare*) ile aynı anlamda, "*bilgisayar sistemlerinin düşman sistemlerine zarar vermek veya yok etmek maksadıyla kullanıldığı savaş tipidir*" şeklinde tanımlanmaktadır. Siber savaşın, İngilizce karşılığı olan "*cyberwar*", bazı sözlüklerde de bilgi savaşının yani "*information war*" teriminin eş anlamlısı olarak kullanılmakta ve "*elektronik iletişim ve internetin bir ülkenin iletişim sistemi, güç kaynakları, ulaşım sistemi ve benzeri sitemlerini bozması veya çökertmesi*" olarak tanımlanmaktadır. Şangay İş birliği Örgütü ise bilgi savaşını, "*toplum ve devlet düzenini bozmak için toplu psikolojik beyin yıkama faaliyetlerinin yanında devleti, düşman devlet isteklerine göre karar almaya zorlamak*" olarak tanımlamaktadır.[113] Bu tanımlardan dikkat edilecek birinci husus, siber savaşın devletler arasında cereyan etmesi; diğeri ise, karşı tarafın sistemlerine hasar vermeye veya sistemlerde kesinti yapmaya yönelik eylemlerin siber savaş olarak nitelendirilmesidir.[114]

Siber savaşın iki önemi mevcuttur. Birinci önemi, siber savaş yönteminin nasıl uygulanacağı ve gerginliğin artırılmasından nasıl kaçınılacağını içermektedir. İkinci önemi ise, siber savaşın asıl gayesidir. Rakip gördüğü tarafa boyun eğdirmeyi, verilerini çalmayı, sistemlerine sızarak belirli bir süre etkisiz bırakmayı veya komple bozmayı içermektedir.[115]

Siber savaşın silahları sentaktik saldırılar, semantik saldırılar ve karışık saldırılar olmak üzere üç kategoriye ayrılmıştır. Sentaktik saldırıların hedefi, bilgisayar sistemleri olup, zararlı programlar, hizmet engelleme eylemleri ve sisteme girmektir. Semantik saldırılar, bilgisayar sistemini hedeflemez, sadece bilgisayar kullanıcısının ulaşmış olduğu verinin doğru olup olmadığını hedef almaktadır. Sistem problemsiz bir biçimde çalışmasına rağmen içerdiği veriler doğru olmaktan uzaktır. Bu saldırılar, özellikle resmi internet sitelerinin veya

---

113 Yayla, "Siber Savaş," 190-191.

114 Çiftçi, Her Yönüyle Siber Savaş, 5.

115 Çiftçi, Her Yönüyle Siber Savaş, 7.

kritik altyapı tesislerinin sistemleri hedeflendiğinde ciddi neticeler oluşabilir. Karışık saldırılar, semantik ve sentaktik saldırıların bir arada yapılmasıdır. Kritik işletim sistemlerinin yanlış bilgi ile belgelerden beslenerek etkisizleştirilmesi karışık saldırıya örnek teşkil etmektedir.[116]

Siber savaş, genelde parasal kazanç hedeflenen suçtan ve politik amaçlı sembolik saldırılar içeren terörizimden temelde farklılık göstermektedir. Siber savaşın, suç ve teröre nazaran daha belirgin farklılıkları vardır. Her ne kadar bazı ülkeler siber suç veya terör eylemlerinin işlenmesini doğrudan ya da dolaylı olarak desteklese de savaşın örgütlenmiş ve hükümet oluşturmaya niyetli meşru gruplar tarafından uygulandığı, diğer ikisi için genelde böyle bir durumun olmadığı dikkatlerden kaçmamalıdır. Siber savaş, siber suçların ve siber terörün aynı sanal sistemi kullanmaları bir benzerlik gibi görünse de amaçlarda ve motivasyonda farklılık mevcuttur. Ayrıca siber savaş, suç ve terörizmden daha düzenli ve yoğun saldırıları içermektedir. Bunun yanında siber terörizm ve siber suçlar, bireyler veya gruplar tarafından işlenirken siber savaş devlet veya örgütlenmiş bir otorite tarafından işlenmektedir. Bu nedenle kişisel boyutta yapılan eylemler siber savaş içerisinde değerlendirilmemektedir.[117]

SONUÇ VE ÖNERİLER

Bilgisayar ve internetin ortaya çıkmasından sonra suçun sanal dünyada da işlenebilme kolaylığı görülmektedir. Tek bir tıklama ile dünyanın bir ucundan diğer bir ucuna siber saldırı yapılabilecek teknolojiye kavuşulmuştur. Dolayısıyla suç örgütleri devletlere ve toplumun yıkıcı mantığına karşı eski klasik yöntemlerle savaşmamakta, gelişen teknolojik gelişmeler neticesindeki araç ve gereçlerden yararlanmaktadırlar.

---

116 Yayla, "Siber Savaş," 187-188.

117 Çakmak ve Demir, "Siber Dünyadaki," 44-45.

Bunun sonucunda yeni bir dünya; siber dünya ortaya çıkmasının yanında küreselleşme ile birlikte internetin yaygınlaşması, küreselleşmenin negatif etkileri, devletlerin sınırsız müdahaleleri ile yerel milliyetçiliklerin yükselmesi, siber dünyanın boşluklarından faydalanan kötü niyetli, suça meyilli veya suçlu, birey ve grupların ve teröristlerin bu alana yönelmeleri nedeniyle yeni suç türlerinin, suçluların, suç örgütlerinin doğmasına neden olmuş ayrıca siber suç, siber savaş ve siber terörizmi kavramlarını ortaya çıkarmıştır. Ancak hukuk ve güvenlik politikaları bakımından siber dünyada işlenen suçların karmaşıklığından dolayı kavram karışıklığına neden olmuştur. Bu nedenle çalışmamız, bilişim sistemi, siber suç, siber terörizm ve siber savaş konuları etrafında şekillenmiş, siber dünyadaki diğer kavramların, aktörlerin ve eylemlerin de tanımlanması yapılmıştır.

Araştırmanın sonucuna göre, siber dünyada işlenen suçlar; bilgisayar suçu, internet suçu, siber suç, bilişim sistemi aracılığıyla işlenen suç, bilgisayar ile ilgili suç, bilgisayarlara karşı işlenen suç, bilişim suçu ve bilgisayarlar aracılığı ile işlenen suç, bu alanı tanımlamak için kullanıldığı görülmüştür. Yine bu alanı tanımlamak için kullanılan kıstaslar; bilgisayarın amaç veya araç olmasını arayan tanım, bilişim suçlarını malvarlığı ihlalleriyle sınırlayan tanım, bilişim sistemleriyle herhangi bir şekilde ilişkili olan suçları esas alan tanım, bilgisayar kullanımını esas alan tanım, suçu işleyen faili esas alan tanım ve sınıflandırmaya tabi tutulamayan olarak sıralandığı görülmektedir.

Çalışmamızın neticesinde, siber suç, siber terörizm ve siber savaşın saldırı yöntemleri her ne kadar benzerlik gösterse de motivasyon ve amaçları bakımından ayrıldıkları görülmüştür. Buna göre siber suç, bilişim sistemlerinin kullanılması suretiyle kişiden kişiye işlenen suçlar olduğu değerlendirilmektedir. Burada herhangi bir örgütsel eylemin olmadığı anlaşılmaktadır. Bireysel eylem söz konusu olmaktadır. Siber suç, bilişim sistemlerine geçici veya kalıcı zarar vermek, verileri elde etmek

veya yok etmek şeklinde ifade edilmektedir. Ancak bu saldırılar örgütlü bir şekilde ideolojik unsuru barındırıyorsa, devlete karşı bir eylem ise ve toplumları paniğe sokmak, korkutmak ve karışıklık meydana getirmeyi amaçlıyorsa, bu saldırı biçimini, devlet yetkilileri tarafından siber terörizm kapsamında değerlendirdiği anlaşılmıştır. Yine siber saldırılar, doğrudan veya dolaylı yoldan bizatihi devletlerarası gerçekleştiriliyorsa bu saldırı biçimi ise siber savaş kapsamında değerlendirildiği görülmüştür.

Bilişim suçları kapsamında değerlendirilen siber saldırılar, vatandaşların hayatlarını etkilemekte, ekonomi alanında şirketlere büyük kayıplara uğratmakta ve devletlerin güvenliğini tehdit etmektedir. Bu nedenle bu tedirginlikler karşısında herkesin önlemler almasına gerek duyulmaktadır.

Öncelikle vatandaşların bilgisayar kullanımı ve güvenliği konusunda sürekli bilinçlendirilmeleri gerekmektedir. Bu konuda gerekli önlemlerin nasıl alınacağını bilmeyen vatandaşların en azından hükümetlerin internet güvenliği ve antivirüs yazılımlarının kullanımının yaygınlaştırılması, maddi anlamda ulaşılabilir olması bu konuda farkındalık yaratılması gerekmektedir.

Siber terör eylemleri ile siber savaşların etkisi düşünüldüğünde, devletlerin gerek ulusal boyutta gerekse uluslararası boyutta siber tehditlere karşı stratejiler oluşturması gerekmektedir. Teknolojik alt yapılarını ve ağ güvenliklerini gözden geçirmeleri gerekmektedir. Siber saldırıların dünyanın bir ucundan diğer bir ucuna yapılabilir olduğu düşünüldüğünde bu anlamda uluslararası sözleşmeler ön plana çıkmaktadır. Bu nedenle uluslararası kuruluşların öncülüğünde bu alandaki gelişmelerin takip edilmesi, buna göre yasal zeminin güncellenmesi ve suçluların yakalanmasına dair ortak anlaşma ve çalışmalar yürütülmesi elzemdir.

Bunun yanında devletin güvenlik güçlerinin siber suçları engelleme veya kontrol altına alma çabalarının yanında birtakım

problemler ortaya çıktığı görülmektedir. Buradaki temel problem güvenlik güçlerinin siber suçları önlemek için vatandaşların internet gezintilerini gözetleme ve izleme faaliyetlerinde bulunmak zorunda olduğu kadar internet kullanıcıların mahremiyet ve gizliliklerinin de aynı kişiler tarafından korunmak zorunda olduğu gerçeğidir. Bu dengeyi iyi bir şekilde kurması gerekmektedir.

Devletin güvenlik güçleri tarafından, siber suç ve suçlarla mücadele etmek için izleme ve gözetlemenin sınırlarını genişletmeye çabalamaları karşısında internet kullanıcıların özgürlük, mahremiyet ve gizliliğin ihlal edilmemesi için devleti yönetenler ve kanun koyucular tarafından her iki tarafında bunu sağlayan güçlendirici araçların düzenlenmesi gerekmektedir.

Hakem Değerlendirmesi: Çift kör hakem.

Finansal Destek: Yazar bu çalışma için finansal destek alıp almadığını belirtmemiştir.

Çıkar Çatışması: Yazar çıkar çatışması bildirmemiştir.

Etik Kurul Onayı: Yazar etik kurul onayının gerekmediğini belirtmiştir.

Peer Review: Double peer-reviewed.

Financial Support: The author has not declared whether this work has received any financial support.

Conflict of Interest: The author has no conflict of interest to declare.

Ethics Committee Approval: The author stated that ethics committee approval is not required.

KAYNAKÇA

Akarslan, Hüseyin. *Bilişim Suçları.* Ankara: Seçkin Yayıncılık, 2012.

Aköz, Burak Cesur. "Türk Ceza Kanunu Kapsamında Bilişim Suç ve Cezaları ile Örnek Yargısal Kararların Analizi ve Mevzuat Önerileri." Bilişim uzmanlığı tezi, Bilgi ve İletişim Teknolojileri Kurumu, 2018.

Altınok, Taner, ve Zeynep Kaya. "Siber Tehditlerle Mücadele." İç. *Suç, Terör ve Savaş Üçgeninde Siber Dünya*, ed. Haydar Çakmak ve Taner Altunok, 137-162. Ankara: Barış Platin Kitabevi, 2009.

Altunok, Ebru, ve Ali Fatih Vural. "Bilişim Suçları." *Denetişim*, no. 8 (2011): 74-84.

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

Balcıoğlu, İbrahim. "İnternet Kullanımı ve Getirip Götürdükleri." *Somuncubaba Dergisi*, (2014): 64-67.

Başaran, Alper. *Siber Savaş Cephesinden Notlar.* İstanbul: Arion Yayınevi, 2016.

Bektaş Şeker, Tülay. *İnternet ve Bilgi Açığı.* Konya: Çizgi Kitapevi Yayınları, 2005.

Bozdoğan Akbulut, Berrin. "Bilişim Suçları." *Selçuk Ünüversitesi Hukuk Fakültesi Dergisi* 8, no. 1-2 (2000): 545-555.

Budak, Ömer Sıddık. "Bilişim Öğrencilerinin Siber Suç Farkındalığı: Erzurum İli Mesleki ve Teknik Liseler Örneği." Yüksek lisans tezi, Atatürk Üniversitesi, 2015.

Burkay, Senem. "Teorik Çerçevede Suç." *ETHOS: Felsefe ve Toplumsal Bilimlerde Diyaloglar* 2, no. 4 (2008): 1-15

Çağıltay, Kürşat. *İnternet.* Ankara: METU PRESS, 1997.

Çakmak, Haydar, ve Cenker Korhan Demir. "Siber Dünyadaki Tehditler ve Kavramlar." İç. *Suç, Terör ve Savaş Üçgeninde Siber Dünya*, ed. Haydar Çakmak ve Taner Altunok, 23-55. Ankara: Barış Platin Kitabevi, 2009.

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

Değirmenci, Olgun. "Bilişim Suçları." Yüksek lisans tezi, Marmara Üniversitesi, 2002.

Dilber, Fadime. "Kitle İletisim Araçları ve Suç Olgusu." *Karamanoğlu Mehmetbey Üniversitesi Sosyal ve Ekonomık Arastırmalar Dergısi* 16, no. Özel Sayı 1 (2014): 60-66.

Dülger, Murat Volkan. *Bilişim Suçları ve İnternet İletişim Hukuku.* Ankara: Seçkin Yayınları, 2014.

Erdoğan, Yavuz. *Türk Ceza Kanunu'nda Bilişim Suçları.* İstanbul: Legal Yayıncılık, 2013.

Ergün, İsmail. Siber Suçların Cezalandırılması ve Türkiye'de Durum. Ankara: Adalet Yayınevi, 2008.

Gallas, Wilhelm. "Cezalandırılabilirliğin Temelleri ve Sınırları (Suç Kavramı Üzerine Düşünceler)." çeviren İzzet Özgenç. *Selçuk Üniversitesi Hukuk Fakültesi Dergisi* 4, no. 1-2 (1994): 305-327.

Gümüş, Çetin. "Bilişim Suçlarıyla Mücadelede Polisin Eğitimi." Doktora tezi, Fırat Üniversitesi, 2008.

Hekim, Hakan, ve Oğuzhan Başıbüyük. "Siber Suçlar ve Türkiye'nin Siber Güvenlik Politikaları." *Uluslararası Güvenlik ve Terörizm Dergis* 4, no. 2 (2013): 135-158.

Helvacıoğlu, Aslı Deniz. "Avrupa Konseyi Siber Suç Sözleşmesi-Temel Hükümlerin İncelenmesi." İç. *İnternet ve Hukuk*. ed. Yeşim M. Atamer, 277-300. İstanbul: İstanbul Bilgi Üniversitesi Yayınları, 2004.

İçel, Kayıhan. "Avrupa Konseyi Siber Suçlar Sözlşemesi Bağlamında 'Avrupa Siber Suç Polistikasının Ana İlkeleri'." *İstanbul Üniversitesi Hukuk Mecmuası* 59, no. 1-2 (2011): 3-10.

İnan, Aslan. *İnternet El Kitabı.* İstanbul: Sistem Yayıncılık, 2000.

Kongar, Emre. *Küresel Terör ve Türkiye.* İstanbul: Remzi Kitapevi, 2002.

Kurt, Levent. Açıklamalı-İçtihatlı Tüm Yönleriyle Bilişim Suçları ve Türk Ceza Kanunundaki Uygulaması. Ankara: Seçkin Yayınevi, 2005.

Malkoç, İsmail. Açıklamalı İçtihatlı Yeni Türk Ceza Kanunu - 2. Cilt. Ankara: Malkoç Kitapevi, 2007.

Özcan, Mehmet. "Siber Terörizm ve Ulusal Güvenlik." İç. *İnternet ve Hukuk*. ed. Yeşim M. Atamer, 301-340. İstanbul: İstanbul Bilgi Üniversitesi Yayınları, 2004.

Özkan, Tezcan. "Siber Terörizm Bağlamında Türkiye'ye Yönelik Faaliyet Yürüten Terör Örgütlerinin İnternet Sitelerine Yönelik Bir İçerik Analizi." Yüksek lisans tezi, Anadolu Üniversitesi, 2006.

Özkul, Davut. "Bilişim Sistemi Kavramı ve Bilişim Sistemlerinin Denetimi." *Sayıştay Dergisi* 13, no. 44-45 (2002): 11-34.

Sandilaç, Nurullah. "Siber Dünyada Hacker Kültürü, Hacktivizm ve Bilişim Suçları." Yüksek lisans tezi. Sakarya Üniversitesi, 2021.

Sertoğlu, Sedat. "Büyük tehlike." Sabah Online. Son değiştirilme Aralık 6, 1999. http://arsiv.sabah.com.tr/1999/12/06/y11.html.

Taşçı, Ufuk, ve Ali Can. "Türkiye'de Polisin Siber Suçlarla Mücadele Politikası: 1997-2014." *Fırat Üniversitesi Sosyal Bilimler Dergisi* 25, no. 2 (2016): 229-248.

Türk Dil Kurumu Sözlükleri. "Güncel Türkçe Sözlük." Haziran 21, 2022. https://sozluk.gov.tr/.

Yayla, Mehmet. "Hukuki Bir Terim Olarak "Siber Savaş"." *Türkiye Barolar Birliği Dergisi*, no. 104 (2013): 177-202.

Yayla, Mehmet. "Siber Savaş ve Siber Ortamdaki Kötü Niyetli Hareketlerden Farkı." *Hacettepe Hukuk Fakültesi Dergisi* 4, no. 2 (2014): 181-200.

Yazıcıoğlu, Recep Yılmaz. Bilgisayar Suçları: Kriminolojik, Sosyolojik ve Hukuksal Boyutları İle. İstanbul: Alfa Yayınevi, 1997.

Yenidünya, A. Caner, ve Olgun Değirmenci. *Mukayeseli Hukukta ve Türk Hukukunda Bilişim Suçları.* İstanbul: Legal Yayıncılık, 2003.