International
JOURNAL OF SOCIAL,
HUMANITIES AND ADMINISTRATIVE SCIENCES
Open Access Refereed E-Journal & Refereed & Indexed

Article Type
Research Article
Subject Area
International Relations, Political Science

e-ISSN: 2630-6417
International Journal Of Social, Humanities And Administrative Sciences (JOSHAS JOURNAL)

Vol: 8
Issue: 48
Year: 2022
pp
91-99

Arrival
25 December 2021
Published
30 January 2022

Article ID
884
Article Serial Number
11

Doi Number
http://dx.doi.org/10.31589/JOSHAS.884

How to Cite This Article
Altun, A. (2022). "Siber Suçların Kriminolojik Analizi", Journal Of Social, Humanities and Administrative Sciences, 8(48):91-99.



# Siber Suçların Kriminolojik Analizi

## Criminological Analysis Of Cybercrimes

Dr. Öğr. Üyesi Altun ALTUN
Hakkari Üniversitesi, İktisadi ve İdari Bilimler Fakültesi, Siyaset Bilimi ve Uluslararası İlişkiler Bölümü, Hakkari, Türkiye

**ÖZET**

Siber suçlar, internetin ortaya çıkmasından sonra yeni bir suç biçimi olarak ortaya çıkmıştır. Bu suçlar küçük hırsızlıktan kötü niyetle terörist yıkıma kadar uzanmaktadır. Bilgi teknolojilerindeki hızlı değişimle birlikte terörist oluşumlar faaliyetlerinde bilgi teknolojilerini daha yıkıcı olmak için kullanmayı hedeflemiş durumdadırlar. Siber terörizm, çeşitli amaçlara sahip gruplar veya bireyler tarafından gerçekleştirilen suç faaliyetlerinin bir birleşimidir. Diğer suçlardan farklı olarak siber suçlarda failler görünmezken, uzaklık ve mesafe kavramı yoktur. Siber suç kavramına bakıldığında, bilgisayar sistemlerinin illegal olarak kullanılması söz konusudur. Siber teröristler kritik ve zayıf noktalara bilinmeyen bir zamanda, herhangi bir nedenden dolayı herhangi bir noktadan saldırıda bulunabilmektedir. Siber suçun genel hukuki, siyasi ve akademik tanımlamada çok önemli bir güvenlik meselesi olduğu görülmektedir. Bu nedenle siber suçlara kriminolojik bir yaklaşım siber suçlarla mücadelenin geliştirilmesine yardımcı olabilir. Bu çalışmanın amacı siber suçların kriminolojik gerilim, öğrenme ve kontrol teorileri açısından değerlendirilmesidir.

**Anahtar Kavramlar:** Siber Suçlar, Siber Terörizm, Suç Teorileri, Kriminoloji.

**ABSTRACT**

Cybercrimes have become a new form of crime after the emergence of the internet. These crimes vary from petty theft to terrorist destruction. With the rapid changes in information technologies, terrorist groups have aimed to use information technologies to become more destructive. Cyberterrorism is a combination of criminal activities carried out by groups or individuals who have various goals. As opposed to other crimes, while the perpetrators are invisible in cybercrimes, there is also no concept of place or distance. In the context of cybercrimes, the illegal use of computer systems is in question. Cyberterrorists may attack critical and weak points at an unknown time, for any reason and from any location. It is seen that cybercrime is a highly significant issue of security with its general legal, political and academic definition. Therefore, a criminological approach to cybercrimes may help strengthen the fight against cybercrimes. The purpose of this study is to analyze the concept of cybercrime in terms of strain, learning and control theories.

**Keywords:** Cybercrime, Cyberterrorism, Criminal Theories, Criminology.

## 1. GİRİŞ

İnternet belki de günümüzün en etkili teknolojik icadıdır ve dünyadaki hemen hemen herkes için günlük yaşamı değiştirmeye devam etmektedir. Milyonlarca insan siber uzaya bağlanıyor ve binlercesi her gün çevrimiçi dünyaya giriyor. İnternet sadece başkalarıyla etkileşim ve öğrenme biçimimizde devrim yaratmakla kalmadı, yaşam biçimimizi de sonsuza dek değiştirdi. İnternet ve bilgisayar teknolojileri gelişmeye devam ederken; suçlular, bu teknolojileri sapkın eylemleri için bir araç olarak kullanmanın yollarını bulmuşlardır. Siber suçlar, bilgisayarlar kullanılarak işlenen veya başka bir şekilde bilgisayarlarla ilgili olan yeni bir suç türüdür. Siber suç, suçun elektronik bir ortamda işlenmesi ve suçlunun izlenmesini ve tanımlanmasını zorlaştırması bakımından geleneksel suçtan farklıdır. En yaygın siber suç türleri arasında siber dolandırıcılık, karalama, bilgisayar korsanlığı, zorbalık ve kimlik avı yer alır. Kriminoloji alanında, bazı insanların neden sapkın davranışlarda bulunurken diğerlerinin bundan kaçındığını açıklamaya çalışan bir dizi teori mevcuttur. Bu teoriler başlangıçta 'gerçek dünyada' işlenen suçları açıklamayı amaçlasa da, yine de siber suçlara uygulanabilirler. Bu teoriler, sosyal öğrenme teorisi, , genel gerillim teorisi ve kontrol teorisini içerir. Bu çalışma, siber suçun nedenini en iyi açıklayanı görmek amacıyla yukarıdaki teorilerin özelliklerini analiz edecektir. Diğer fiziksel suç biçimleri gibi, siber suçlular, bazı faktörler nedeniyle siber suçlar işlemeye çekilmektedir. Bu nedenle, siber suçları engellemek için, kolluk kuvvetleri, doğalarını, neden ona çekildiklerini ve nasıl yapabileceklerini anlamalıdır. Çalışma, siber suçun ardındaki nedeni ve neyin sebep olduğunu tartışmaktadır. Çalışmadaki amaç, bilişim teknolojilerinin gelişmesine paralel bir artış gösteren siber suçların suç teorileri açısından değerlendirilmesinin yapılarak konuya kriminolojik bir bakış açısı kazandırmak ve siber suçlar ile mücadelede küçük de olsa bir boşluğu doldurmaktır.

## 2. SİBER SUÇUN TANIMLANMASI

Suç genel anlamdan sapan bir davranış biçimidir. Böyle bir durumda suç sapma olarak görülmektedir. Suç kuralları yasalar tarafından tanımlanmış olma ve maddi yaptırım gücüne sahip olma özelliklerine haizdir. Zamanla birlikte suç algısı değişmektedir. Geçmiş dönemlerde suç işleyenlere karşı daha sert kurallar söz konusu iken giderek suç işleyen bireyleri topluma kazandırma amaçlı çözümler üretilmeye başlamıştır. Uluslararası Kriminoloji Kongresi'nin Tokyo toplantısında yaptığı tanıma göre suç "itaate çizilen bir sınır ve bir başkasına zarar verme kastıyla yapılan her türlü fiili ve sözlü davranışlardır" (Fındıklı, 2011:2).

Siber suç çalışmaları geliştikçe, araştırmacılar terimi en iyi nasıl tanımlayacaklarını araştırdılar. Bugüne kadar, siber suçun evrensel bir tanımı geliştirilmemiştir. Bazen 'elektronik suç', 'bilgisayar suçu', 'bilgisayar bağlantılı suç', 'yüksek teknoloji suçu', 'teknoloji destekli suç', 'e-suç' veya 'siber uzay suçu' olarak adlandırıldı. Avrupa Ekonomik Topluluğu Uzmanlar Komisyonu 1983 tarihli Paris toplantısında, siber suçları; "bilgileri otomatik isleme tabi tutan veya verilerin nakline yarayan bir sistemde kanuna, ahlaka aykırı olarak veya yetki dışı gerçekleştirilen her türlü davranış" şeklinde tanımlamaktadır (Keçeci, 2012). Doktrinde ortak bir tanım olmasa da genel olarak, siber suçlar "verilerin bilişim temelli olarak ve otomatik bir biçimde işlenmesi, saklanması, tasnif edilmesi, terkibi ve iletilmesi ile ilgili ve bilişim alanı içerisinde işlenen, bir bilgisayara veya bilgisayar ağına yahut bir bilişim sisteminin bir kısmına ya da tamamına yahut bu sistemde bulunan verilere yönelik olarak veya bu sistemlerin araç olarak kullanılması suretiyle gerçekleştirilen haksız eylemler" olarak tanımlanmaktadır (Erdem ve Özocak, 2017).

Bilgi teknolojisi sistemlerinin ve ağlarının kapsamlı kullanımı, hem bireylere hem de kuruluşlara şüphesiz faydalar sağlamıştır. Ne yazık ki, aynı zamanda istismar ve suç faaliyetleri için yeni fırsatlar sunmaktadır. İnternet, bilgisayarlar, cep telefonları ve diğer teknoloji biçimleri, son birkaç on yılda, iletişim kurma, bankacılık işlemleri yapma, alışveriş yapma, haberleri alma ve kendimizi eğlendirme dahil olmak üzere insan yaşamının her alanında devrim yaratmıştır. Bu teknolojik gelişmeler, suçluların çeşitli suç türlerini işlemeleri için sayısız fırsatlar da sunmuştur. Çevrimiçi suçlara genellikle siber suçlar denir ve 'faillerin özel siber uzay bilgisi kullanması' nedeniyle ortaya çıkmaktadır. Bu nedenle siber suç, bilgisayarların ve teknolojinin destekleyici bir rolde kullanıldığı, örneğin taciz edici mesajlar göndermek için bir bilgisayarın kullanılması gibi bilgisayar destekli suçları kapsayan geniş bir şemsiye terim olarak görülebilir. Aynı zamanda, siber suç terimi, bilgisayar teknolojisinin doğrudan bir sonucu olan ve onsuz var olamayacak bilgisayar odaklı örneğin yetkisiz bilgisayar sistemine izinsiz giriş gibi suçları da içermektedir (Furnell, 2002:21). Siber suçlar, doğru ve yanlış arasında seçim yapma isteği ve yeteneği olan bireyleri cezbeder. Seçme isteği çevre ve kalıtım faktörlerinden etkilenir. Rogers, bir siber suçlunun suç türü ile ilgili olarak kişilik özellikleri ve sosyo-demografik özelliklerin ilişkili olduğunu ifade etmektedir. Rogers'e göre bu ortak özellikler kullanılarak psikologlar suçluların sınıflandırmasını ve profillerini geliştirebileceklerdir (Rogers, 2010).

Rogers, Smoak ve Jia siber suçları dokuz modele ayırmaktadır (Rogers, Smoak ve Jia, 2006):

- ✓ Script Kiddies (SK) veya Acemiler (NV)
- ✓ Siber Serseriler (CP)
- ✓ Hacktivistler (H) veya Siyasi Aktivistler (PA)
- ✓ Hırsızlar (T) veya Küçük Hırsızlar (PT)
- ✓ Virüs Yazarlar (VW)
- ✓ İçeridekiler (IN)
- ✓ Koruyucu Hackerlar (OG)
- ✓ Profesyonel Suçlular (PC)
- ✓ Siber Teröristler (CT) veya Bilgi Savaşçıları (IW)

Rogers (2010), beceri düzeyini ve motivasyonu bir sirkumfleks modelinde birleştirmektedir. Bu dört motivasyon yönü (1) intikam, (2) finansal, (3) kötü şöhret ve (4) meraktır. Bilgi Savaşçıları (IW), Profesyonel Suçlular (PC), Siyasi Aktivistler (PA) ve Eski Muhafız Korsanlarının (OG) beceri düzeyi en yüksek seviyededir. İçeridekiler (IN) ve Virüs Yazarları (VW) intikam tarafından motive edilir; Bilgi Savaşçıları (IW), Küçük Hırsızlar (PT) ve Profesyonel Suçlular (PC) finansal güdülerle motive edilir; Siber Serseriler (CP)ve Siyasi Aktivistler (PA) şöhret tarafından motive edilir; ve Acemi (NV) ve Eski Muhafız Korsanları (OG) merak tarafından motive edilmektedir.

Başka bir sınıflandırma, Gordon ve Ford tarafından benimsenen sınıflandırmadır. Sürekli bir ölçek kullanarak siber suçları Tip I ve Tip II suçlar olarak sınıflandırdılar. Tip I siber suç, doğası gereği daha teknik olan (örneğin bilgisayar korsanlığı) suçtur, Tip II siber suç ise teknolojiden (örneğin çevrimiçi kumar) daha çok insan temasına dayanan

suçtur. Bununla birlikte, bu yazarlar, ' *tamamen* Tip I veya Tip II olan çok az olay olması muhtemeldir; bu tipler bir sürekliliğin her iki ucunu temsil eder' (Gordon ve Ford, 2006:16). Bununla birlikte, yapay zeka ve robotikteki gelişmeler, teknolojik ortamı hızla değiştirmiştir. Bu fenomenlerin kendi kendine öğrenebilen araçlar tarafından işlenen bir 'Tip III' siber suça yol açabileceği iddia edilebilir.

Siber suçlar, McGuire ve Dowling tarafından 'siber etkin' suç ve 'siber bağımlı' suç olarak sınıflandırılmıştır. Siber destekli suçlar, bilgisayarların kullanımıyla kolaylaştırılan geleneksel suçlardır. 'Siber erişimli' suçların kapsamı hileli finansal işlemler, kimlik hırsızlığı ve ticari kazanç için elektronik bilgi hırsızlığı gibi beyaz yakalı suçlardan, uyuşturucu kaçakçılığı, anormal röntgenci faaliyetler, taciz, takip veya takip etme gibi suçlara kadar sayısızdır. Bunlar her zaman suç faaliyetleri olarak görülse de, artık bir bilgisayarla takip etmek çok daha kolaydır (McGuire ve Dowling, 2013:30).

Siber bağımlı suçun bir başka modern tezahürü, bir örgütün eylemlerini veya politikalarını protesto eden "hacktivist"in işidir. 2010 yılında WikiLeaks üzerindeki teknolojik ve ticari çatışmalar WikiLeaks'in anonim destekçiklerinin ortak bir çevrimiçi saldırısının internet güvenliğini ciddi bir şekilde ihlal ederek MasterCard, Visa ve PayPal'ı bozmayı başardığı tam bir çevrimiçi saldırıya dönüşmüştür. Anonymous, bu üçlünün web sitelerine (DDoS) saldırılarının yayılmasını teşvik etmiştir. DDoS saldırısı, bir kişinin çevrimiçi bir hizmeti birden çok kaynaktan gelen trafikle ezerek hizmetin çökmesine neden olarak kullanılamaz hale getirmeye çalışmasıdır. Bu özel siber suçtan kaynaklanan hasar önemliydi. Yalnızca PayPal için hasarın 5,5 milyon ABD doları olduğu tahmin edilmiştir (TheGuardian,2020). Anonymous, çeşitli siyasi olaylar nedeniyle devlet ve devlet bağlantılı sitelere çok sayıda saldırı gerçekleştirmiştir. Kendilerini hacktivist olarak adlandıran grup 2003 yılından itibaren faaliyetlerini sürdürmektedir. Kendilerine "anonnimler" adını veren grup "Biz Anonymous'uz, orduyuz, affetmeyiz, unutmayız, bizi bekleyin" sloganını kullanmaktadır (CNNTÜRK. 2021).

Siber bağımlı suçlar, çevrimiçi olarak kolayca bulunabilecek araçlar kullanılarak kolayca ve ucuza kurulabilir. Bununla birlikte, muhtemelen hükümetler için en büyük endişe, dünya genelindeki siber suçluların interneti casusluk ve terörizm amaçlarıyla kullanma becerisidir. İnternetin sınırsız doğası ve dolayısıyla siber suç, hükümetlerin dünyanın herhangi bir yerinden hedef alınabileceği anlamına gelir ve bu da kolluk kuvvetlerini yalnızca zorlayıcı değil, bazı durumlarda neredeyse imkansız hale getirmiştir. Üstelik günümüzün suçluları, üst düzey teknik becerilere ihtiyaç duymadan casusluk yapabilmektedir (Sarre, 2017:167).

### 2.1. Faillerin Suç İşleme Nedenleri

Siber suç failleri işten çıkarılma veya birtakım memnuniyetsizlikler nedeniyle, intikam alma hissi (Vandalizm, sabotajlar, yağma gibi), "Biri" olma hissi, mali sıkıntılar ve bilgisayarı aşabilme hissi (operatör makine ilişkisi kökenli problemlerde dahil) gibi nedenlerle suç işlemektedir. Bunlara ek olarak ekonomik nedenler, rekabet hissi ve şirkete zarar verme hissi de suç işleme nedenleri olabilmektedir (Yılmaz, 1997:103). İsveç'te SOLARZ için National Council For Crime Prevention adına yapılan bir araştırmada siber suç faillerinin yaş ortalaması 35.2 ve % 44'ü kadın olarak tespit edilmiştir. İtalya'da Serviziyo Securinet'in 1990, 1991 ve 1992 yıllarına ait incelediği verilere göre ise güvenlik güçleri tarafından tespit edilen siber suç failleri 19 yaşından büyüktür. Faillerin % 25'i 35-45, % 29'u 35-35, % 55'i 19-25 yaş arasında kişilerden oluşmaktadır. Bu kişilerin % 38'i işsizken % 47 gibi büyük bir bölümü ise üniversiteli öğrencilerden oluşmaktadır. Bir meslek sahibi olan faillerin % 43'ü ise bilgisayar alanında bir işte çalışmaktadır (Alaca, 2020:51).

Shinder ise siber suç faillerini suç işlemeye yönelten ve onları motive eden unsurları beş başlık altında toplamıştır (Shinder, 2012). Bunlar;

- ✓ Oyun amaçlı (just for fun): Meraklı gençler ve hackerler tarafından internet bir oyun alanı bilgisayarlarda bir oyuncak gibi görülmektedir. Bu nedenle eğlenmek amacıyla müzik ve film indirmek, diğer kişilerin ağlarına izinsiz girmek, web sayfalarını kopyalamak, bireysel yeteneklerini sergilemek için virüs göndermek veya küçük miktarlarda para kazanmaktır. Esas niyetleri zarar vermek değildir ancak bu eylemleriyle başkalarına zarar verebilmektedirler.
- ✓ Para (Money): Bireyleri suç işlemeye yönelten en önemli sebeplerden birisi de önemli bir değer olan paradır. Bankada çalışan bir kişi veya hacker tarafından bankada hesabı olan başka birinin hesabının ya da kredi kartının çalınması bazen de bir şirketin ticari sırları gibi maddi değer taşıyan unsurların çalınmasıdır. Bu grupta beyaz yakalı suçlar olarak tanımlanan gençler, yaşlılar, erkekler, kadınlar, profesyoneller ve sosyo-ekonomik düzeyi farklı olan kişiler de olabilir.
- ✓ Duygu/öfke/intikam (emotion): Öfke, kin ve aşk gibi duygusal etkenlerin paradan daha öne çıktığı bir durumdur. Hoşnut olunmayan ilişkiler ağı, memnun olunmayan alışverişler, düşük not alınan ders öğretmenleri gibi

etkenlerden olumsuz etkilenen kişiler e-mail yoluyla taciz, hakaret, tehdit, hesaplara izinsiz giriş, gizli kalması gereken özel sır ve fotoğrafları açığa çıkarma, şirketlerin bilgilerini çalma, kopyalama, silme ve Ddos saldırıları gerçekleştirme gibi suçları işlemekte veya işlenmesine neden olmaktadır.

- ✓ Cinsel amaçlar (sexual impulses): Bu gruptakiler seri tecavüzcüler, çocuk pornosu sapkınları ve istismarcılarıdır. Çocuk pornografisi başkalarından ticari kazanç elde etmek için de yapılabilmektedir.
- ✓ Politik ve dini amaçlı (politic/religion): Bu amaçla suç işleyenler interneti bir propaganda aracı olarak kullanmakta ve kendi politik hedeflerine yönelik saldırılar gerçekleştirmektedir. Dinsel inanışlar ve siyasi bağlılıklar da insanların suç işlemesine neden olmaktadır. Siber terör saldırıları bu grupta yer almaktadır.

Siber suçlar için politik motivasyon, devlet düzeyinde olmak üzere aktör ve devlet dışı aktör düzeyinde iki düzeyde görülebilir. Devlet dışı aktör düzeyinde siyasi motivasyonlar duygularla yakından ilişkilidir, çünkü insanlar politika hakkında çok tutkulu olabilirler. Bu seviyedeki politik motivasyon genellikle sağ kanat ile ilişkilidir. Devlet aktörleri düzeyinde siyaset ve dış politika ülkeleri siyasi ve askeri avantajı korumak için sabotaj ve casusluğu kullanmaya motive etmiştir. Bu kategori motivasyonu en iyi iki politik alt kategori direniş ve siber savaş/siber casusluk gözden geçirerek açıklanabilir. Ülke içindeki belirli bir grubun hakları veya ülkeleri için savaş verdiklerini düşünen milliyetçi hackerler ve siyasi aktivistler vatansever olarak kabul edilebilir. Örneğin kendilerini Filistin, İsrail, İran gibi terimlerle tanımlama eğilimindedirler. Siyasi siberde kullanılan bilgisayarlar-saldırılar bir botnet ordusunda botlar veya çok sayıda direnişin koordineli bir çabası olabilir. Siyasi direniş için kullanılan siber saldırılar diğer türlerden daha az sıklıkta görülür. Siber savaş, ulus devletlere saldırmalarına izin verdiği için elverişli bir seçenektir. Bu yeni birbirine bağlı casus teknoloji düşmanı entegrasyon ve bağlılığını kullanarak saldırı dünya ve başka bir kıtadaki bir bilgisayardan geleneksel savaşa tercih edilirler. Fiziksel savaş yoluyla resmi olarak elde edilen aynı siyasi hedeflerin çoğu ve casusluk artık vatandaşların hayatını tehlikeye atmadan casusluk olmak üzere iki ana hedef üzerinde odaklanmaktadır (Smith, 2015). 2009 yılında bazı Amerikan ve Güney Kore devlet daireleri koordineli siber saldırılara uğramıştır. Her iki durumda da dağıtılmış hizmet reddi saldırıları hükümet web sitelerini bozmak için kullanılmıştır. Güney Kore saldırının büyüklüğünden dolayı Kuzey Kore'den şüphenildiğini açıklamıştır (Amerikanınsesi, 8 Temmuz 2009). Sabotaj siber savaşta yaygındır ancak casusluk şu anda baskın biçimidir. Siber ortamda Çin ve Rusya lider ülkeler olarak yerini alırken siber savaş araçlarını geliştirmektedirler. Çin'in kayda değer casusluk çabalarından birisi "Titan Yağmuru"dur. 2002 yılından itibaren Çin ABD Savunma Bakanlığı'na devam eden bir dizi saldırı gerçekleştirmiştir (Smith, 2015).

## 3. SİBER SUÇUN TARİHSEL EVRİMİ: BİLGİSAYAR SUÇLARINDAN SİBER TERÖRE

Siber suçların tarihsel gelişimi bilişim teknolojilerinin özellikle de internetin gelişimine eşit bir şekilde ilerlemiştir. Sanayi çağının yerini bilişim çağına bırakmasıyla birlikte toplumda köklü değişimler ve ekonomik alandaki etkileşimler artmıştır. Bilişim teknolojilerinin büyük bir hızla gelişim göstermesi, boyutlarının küçülmesi ve daha düşük ücretlere kullanılabilmesi kullanıcı sayılarını artırmıştır. Doksanlı yılların başlarından itibaren çok sayıda bilgisayarın birbirine bağlanmasıyla birlikte suç işlemeye eğilimli kişiler bu alanlarda toplanmaya başlamışlar ve farklı suçlar ortaya çıkmaya başlamıştır. Resmi kurumların sanal ağlar için olmazsa olmaz bir öneme sahip olması bu sistemlerin her an saldırılarla karşılaşma riskini artırmaktadır.[1] Son dönemlerde NASA, NATO benzeri örgütlere ve büyük kuruluşlara yapılan saldırılar neticesinde sistemleri büyük zarara uğramıştır (Küçükvardar, 2018:11).

11 Eylül terör saldırılarından önce yaşanan bazı olaylar Amerikan ordusu ve enerji sektöründeki bilişim teknolojilerinin zayıflığını ortaya çıkarmıştır. Bu durum askeri sistemlere güvensizlik yaratırken 11 Eylül'den sonra siyasi ve askeri çevrelerden gelen uyarılara ek olarak yoğun terör ve güvenlik söylemleri siber terörizmin belirgin tehlikelerini ön plana taşımıştır. Amerikalı bilgisayar bilimi uzmanı Dorothy Denning siber terörizm hakkında şu açıklamada bulunmuştur. "Siber terörizm, siber bolluk ve terörizmin bileşimidir. Siber terörizm, siyasi ve sosyal mercilere ve bireylere gözdağı vermek, baskı oluşturmak maksadıyla resmi birimlerin bilgisayarlarına, network sistemlerine, bilgi ve veri tabanlarına yapılan yasadışı tehdit ve zarar verici saldırılardır. Daha da ötesi, bir saldırının siber terörizm olarak tanımlanması için bireye ya da mala karşı şiddet içermesi gerekmektedir. En azından "korku

[1] Bir ülkenin savunma ve ekonomik gücünün temelini oluşturan sistemler ve kuruluşlar terörün en bariz hedefleridirler. Bunlar sırasıyla; (Şeker, 2009:4).
✓Enformasyon ve komünikasyon sistemleri,
✓Bankalar, finans kuruluşları ve borsalar,
✓İnsan taşıma sistemleri. Hava, deniz ve tren trafik sistemlerini bozmak,
✓İlaç üreticilerinin laboratuarları (Bioterörizm),
✓Doğal gaz , petrol hatları ve depolama kontrol sistemleri,
✓Elektrik güç sistemleri,
✓Su temin sistemleri,
✓Hükümet hizmet servisleri,
✓Acil servisler,
✓TV ve basın kuruluşları

yaratacak kadar hasara" yol açmalıdır. Siber terör ölümcül olan ya da fiziki hasara yol açan, şiddetli ekonomik kayba neden olan saldırılar olarak örneklenebilir. Kritik altyapı odaklarına yapılan ciddi saldırlar yarattığı etkiye göre siber terörizm olarak tanımlanabilir" (Alnıak, 2004:1-5).

Gerçek dünyadaki birçok suç, siber uzayda uzun süredir tekrarlanmaktadır. Terörizm ve aşırıcılık farklı değildir. Bugünün terörist grupları internetin sunduğu avantajlardan yararlanıyor. Her şey gibi, suç, terörizm, şiddet ve hatta savaş siber uzaya dönüştü: çevrimiçi radikalleşme yüz yüze radikalleşme kadar önemli hale geliyor, çevrimiçi platformlarda şiddet içeren gruplar ortaya çıkmıştır ve devletler düşmanlarına saldırmak için hacker grupları kullanmaktadır. Böyle bir bağlamda, siber terörizm bir ulusal güvenlik sorunu haline gelmiştir. IŞİD, etkisini genişletmek için internet ve iletişim platformlarını kullanan terör gruplarının örneklerinden biridir. Grup, terörist ideolojiyi yaymak için web siteleri, çevrimiçi dergiler ve sosyal medya profilleri işletmektedir. IŞİD ayrıca interneti para toplamak ve işe almak için kullanıyor. Bu tür çevrimiçi çekicilikler, eş zamanlı olarak ilerlerken ve rakiplerle dijital savaşlara girerken, grubun fiziksel dünyadaki hedeflerini desteklemiştir. IŞİD'in siber bölümü olan Birleşik Siber Hilafet, grubun hedeflerini desteklemek için operasyonlar başlatmış ve IŞİD, grubun ilgili ve maceracı gençlere çekici görünmesini sağlayarak bilgisayar korsanlarını üye yapmıştır Böylece genç bilgisayar korsanlarına ulaşarak onlara dijital ve "çarpık" cihatlarında bir rol sunmaktadırlar ( Baştuğ, 2021).

Artan sınır kontrolleri ve askeri ve kolluk kuvvetleri dünyasında, teröristlerin fiziksel sınırlar yerine siber sınırlara girme şansı daha yüksek olabilmektedir. Şiddet yanlısı aşırılık yanlıları, sürekli uluslararası terörle mücadele çabalarıyla karşı karşıya ve fiziksel dünyada zemin kaybetmektedir. Siber saldırılar, dünyanın herhangi bir yerinden ve nispeten daha az kaynakla gerçekleştirilebildikleri için terör örgütleri için cezbedici olmuştur. Amerika İç Güvenlik Bakanlığının (DHS) Ekim 2020 ulusal tehdit değerlendirme raporu, ulus devletlerden veya devlet dışı aktörlerden gelen siber tehditleri Anavatan'a yönelik yedi büyük tehditten biri olarak sıralamıştır. Rapora gore, Rusya ve Çin en yetenekli ulus-devlet siber düşmanları, İran ve Kuzey Koreli siber aktörler de ABD için tehdit oluşturmaktadır (DHS, 2020:9). Büyük ölçekli bir siber saldırı, ekonomide büyük hasara ve olası fiziksel zarara neden olabilir.

Mevcut siber tehdit ortamı, devlet destekli hacker gruplarının terör örgütlerinden daha yakın bir tehdit olduğunu göstermiştir. Devlet destekli hacker gruplarının, korunan bilgisayar sistemlerine sızmak ve önemli zararlar vermek için kaynaklara ve yeteneklere sahip olma olasılığı daha yüksektir. Ancak, siber saldırı yeteneklerini geliştirmenin ve yıkıcı saldırılar başlatmanın uzun zaman aldığını belirtmek gerekir. Güvenlik açıklarını keşfetmek ve yetkisiz erişim elde etmek zaman ve kaynak yoğundur. Terör grupları şu anda hazırlık aşamasında ve bu değişen ortama nasıl uyum sağlayacaklarını ve gelişeceklerini öğreniyorlar. Faaliyetleri kesintiye uğramazsa er ya da geç bu kapasiteye ulaşabileceklerdir. Ulusal savunmada devam eden bir paradigma kayması yaşamakta geleneksel savaş alanları, kara, deniz ve havanın yanı sıra artık başka bir arena olan siber uzaya doğru yönelmektedir. Hükümetler, hacker gruplarını rakiplerine karşı vekil ordular olarak kullanarak siber uzayın sağladığı anonimliğin arkasına saklanmaktadır. Siber suç örgütlerinin ve devlet bağlantılı hacker gruplarının göreceli başarısı, terörist grupları siber uzaya daha fazla yatırım yapmaya teşvik etmiştir (Baştuğ, 2021).

## 4. SİBER SUÇU AÇIKLAYAN KRİMİNOLOJİ YAKLAŞIMLARI

Kriminioloji alanında 20.yüzyılın başlarından itibaren yapılan çalışmalar suçun sırf bireyin iradesine indirgenemeyecek kadar kompleks bir davarnış olduğunu ve bireyin iradesi dışındaki bazı unsurların da değerlendirilmesi gerektiğini yoğun olarak tartışmaya açmışlardır (Büker, 2011:60). Kriminiloji çalışmaları yeni ve gelişmekte olup suçla ilgili biyolojik yaklaşımlardan feminist yaklaşımlara kadar farklı açıklamaları incelemektedir. Son dönemlerde gelişen teorilerin de bağımsız teorileri bütünleştirmeye yöneldiği görülmektedir. Suçu açıklayan klasik teoriler bireylerin akılcı varlıklar olduğu ve buna paralel de suç işleme özgürlüklerinin olduğunu ileri sürmüştür. Kriminilojik çalışmaların suçu açıklamak üzere uzun bir süreçte geliştirdiği teorik perspektifler konumuz olan siber suçu açıklamak için de önemli temeller sunmaktadır. Gerilim teorisi bireylerin ulaşmaya çalıştığı şeylere yasal yollardan erişememesinin gerginlik ve gerilim ürettiğini geçen sürecin ise bireyleri suça teşvik ettiğini iddia etmektedir. Öğrenme teorisi de bireylerin suçu sonradan çevresindeki kişilerden ve medya gibi kanallardan görerek öğrendiğini savunmaktadır. Bu iki teorinin ortak noktası bireylerin neden suç işlediğini araştırmasıdır. Sosyal kontrol teorileri ise bunlardan farklı olarak tüm bireylerin suç işlemediğini, suç işleyen faillerin işlemeyenlere gore daha az olduğunu , suçla mücadelede bunu gözeterek suç işlemeyenleri araştırıp bu bireyleri suç işlemesini önleyen unsurları tespit etmenin daha mantıklı olacağını ileri sürmüştür (Altuntop, 2012:1).

### 4.1. Gerilim Teorisi

Kriminolojik çalışmaların suçu açıklamak için geliştirdiği gerilim teorisi suçu toplumda ve bireyin yakın çevresinde oluşan anomi (stres) veya gerilimin yansıması olarak görmektedir. Bu bağlamda birinci olarak kişiyi gerilime ve

neticede suça sürükleyen sebeplerin toplum nezdinde değer verilen geliri iyi bir meslek sahibi olma, başarılı bir ebebeyn ve kariyer sahibi olma hedeflerine ulaşamama olduğu görülmektedir. İkincisi bireyin nezdinde hayatında pozitif uyaranları oluşturan aile üyelerinin kaybedilmesiyle yas süreciyle tetiklenen stres neticesinde kişi alkol, uyuşturucu ve şiddete sürüklenebilmektedir (Büker, 2011:60).

Gerilim kuramı, Merton tarafından geliştirilmiştir. Merton'un klasik gerilim teorisine göre anomi, mevcut yapının bireylerden bekledikleri ile bireylerin mevcut yapının istekleriyle çatışan istekleri arasındaki kopukluk olarak tanımlanmıştır. Merton'a göre anonimin ortaya çıkması bireylerin toplumun ihtiyaçlarını karşılamak için başka yollar bulmalarına neden olurken daha yüksek bir sapmayı da beraberinde getirmektedir. Merton, Amerika ve diğer kapitalist toplumların önüne çok fazla para kazanma ve servet sahibi olma hedefleri belirlenerek çalışmanın vurgulandığını ancak bireyleri bu hedeflere ulaştıracak ahlaki ve kanuni tedbirlere çok vurgu yapılmadığını belirtmektedir. Zamanla birlikte bireylerde servet sahibi olmak için her şeyin yapılabileceği düşüncesi ortaya çıkmakta ve toplumsal normlardan sapma durumunu ortaya çıkarmaktadır (Yasuntimur, 2019). "Bu sebeple Merton"a göre suç, ani sosyal değişme ile ortaya çıkan bir olgu değil, daha çok toplumsal yapı fenomenidir." Bu çerçevede Merton, suçun kaynağını sosyal yapılar içinde aramıştır (Merton, 1968).

Alt kültürel gerilimi inceleyen Cohen bunları faydasız ve olumsuz olarak ifade etmiştir. Cohen buna örnek olarak hırsızlık yaparak çete içerisinde itibar kazanmayı, başka bireylerin üzüntüsünden mutluluk duymayı ve orta sınıf değerlerine karşı çıkmayı belirtmiştir. Alt kültürel gerilim teorileri bazı grupların ya da alt kültürün suça onay verdiğini savunmaktadır (Yasuntimur, 2019).

Robert Agnew'in genel gerginlik teorisi, gerginliğin olumsuz duygulara yol açtığını ve bunun da suçluluk da dahil olmak üzere bir dizi sonuca yol açabileceğini öne sürmüştür. Teoride tartışılan spesifik zorlamalar, pozitif değerli hedeflere ulaşamama (örn. para), pozitif değerli uyaranların ortadan kaldırılmasını (örn. değerli bir mülkün kaybı) ve negatif değerli uyaranların sunulmasıyla ortaya çıkmaktadır. İlk gerginlik, bireyin beklentileri ile gerçekte elde ettikleri arasındaki boşluğa bakar, bu da hayal kırıklığına ve kırgınlığa yol açar. İkinci tip zorlanma, pozitif değerli bir uyaran kaldırıldığında ortaya çıkar ve sonuç suçluluktur. Bu suç davranışı, uyaranları hafifletme veya değiştirme girişimi olarak kendini gösterebilir. Son gerginlik türü, olumsuz uyaranlarla karşılaşıldığında ortaya çıkar. Bu, olumsuz uyaranlardan kaçınma veya sonlandırma aracı olarak suçluluğa neden olabilir (Patchin ve Hinduja, 2011). Agnew'e göre, gerginlik doğrudan suça neden olmaz, aksine saldırganlık ve hayal kırıklığı gibi olumsuz duyguları teşvik eder. Bu, Yale Üniversitesi psikologlarının hayal kırıklığı-saldırganlık hipotezi ile doğrudan bağlantılıdır. Öfkenin engellenmeden önce geldiğine ve hayal kırıklığının hem saldırgan hem de saldırgan olmayan davranışlarda kendini gösterebileceğine inanıyorlardı (Runions, 2013). Buna karşılık, bu olumsuz duygular, iç baskıyı hafifletmenin bir yolu olarak başa çıkma tepkilerini gerektirir. Yasadışı davranış ve şiddetle başa çıkma, sınırlı kaynakları ve sinir bozucu ortamlardan kaçamamaları nedeniyle özellikle ergenler için doğru olabilir. Makalelerinde, Siber zorbalık, gençlerin kasıtlı olarak doğrudan veya dolaylı zarar vermek amacıyla akranlarını taciz etmek veya korkutmak için elektronik kullandıklarında ortaya çıkan ciddi ve büyüyen bir sorundur. Dijital ortamda çevrimdışı olmayan bazı benzersiz öğeler vardır, örneğin: anonimlik, sürekli bağlantı ve kalıcılık. Bu yeni teknoloji, kurbanların her an saldırıya uğramasına izin veriyor ve siber zorbaların anonimliği, onları tanımlamayı zorlaştırıyor. Agnew, gerginliğin insanları öfkeli, hüsrana uğramış, depresif hissettirdiğini ve esasen mağdur tarafında düzeltici eylem için baskı oluşturduğunu savunuyor. Bu baskıya yanıt olarak mağdurlar, kötü duyguları hafifletmek için bir araç olarak düzeltici bir eylemde bulunmak isteyerek tepki verirler. Sonuç olarak, bazı mağdurlar için, Siber zorbalık, ergenlerin kötü duygularını azaltmak için yapabilecekleri düzeltici eylemlerden biridir (Patchin ve Hinduja, 2011). Genel gerilim teorisi ve engellenme saldırganlığı hipotezi birlikte, insanların, özellikle gençlerin, başkalarına zorbalık yapmak mı yoksa gerilimi hafifletmek için sapkın davranışlarda bulunmak mı, olumsuz gerilime nasıl tepki verdiğine ve bunlarla nasıl başa çıktığına dair bir anlayış sağlar.

### 4.2. Sosyal Öğrenme Teorisi

Sosyal öğrenme teorisi suçu, kriminolojik olaylarla birlikte toplumdaki normlar, değerler ve davranışların öğrenilmesiyle ilgili olarak açıklamaya çalışmaktadır. Bu teori, hem hukuksal olmayan davranışta suç değerini rasyonelleştirirken hem de suç tekniklerinin öğrenilmesini kapsamaktadır. Sosyal öğrenme teorisi diğer taraftan da "ayırıcı birleşenler, ayırıcı pekiştirme ve nötrleştirme teorisi" gibi kuramları da içermektedir. Sutherland suçluluğu sosyal etkileşim kavramıyla ifade etmektedir. Sutherland'a göre, suçun oluşmasına suçluların bir araya toplanması yeterli bir sebep değildir. Çünkü suçlu davranışının ortaya çıkmasında suç gruplarıyla olan ilişkinin zaman sıklığı, süresi, önceliği ve yoğunluğu önemli sebepleri oluşturmaktadır. Bu teoriye göre suç, doğuştan getirilen birtakım eksiklikler zeka geriliği, kişilik bozuklukları ya da fakirlik gibi ekonomik kaynaklı sorunlardan oluşmamaktadır. Suç toplumsal etkileşim çerçevesinde bir öğrenme faaliyeti olarak ortaya çıkmaktadır. Bu yaklaşım suçlu davranışının

öğrenildiğini savunmaktadır. Toplum içerisinde özellikle de kültürel çevresiyle etkileşim içinde olan bireyler suçlu davranışını daha çabuk öğrenmektedir (Cömert ve Sevim, 2017:35).

Akers'in sosyal öğrenme teorisi genel bir suç teorisidir ve çeşitli suç davranışlarını açıklamak için kullanılmıştır. Bu çalışma, içinde farklı ilişkilendirme, tanımlar, farklı pekiştirme ve taklitten oluşan dört temel önermeyi bünyesinde barındırmaktadır. Sosyal öğrenme teorisi, bireylerin suça karışan diğer kişilerle ilişki kurma veya bunlara maruz kalma (yani, sapkın akranlarla ilişki kurma) yoluyla suç işlemek için motivasyon ve beceriler geliştirdiği fikrine dayanır. Akers, sapkın davranışa maruz kalmanın, bireylere davranışı onaylayan veya etkisiz hale getiren tanımlar sağladığını öne sürdü. Bu tanımlar, suç işlerken suçlular için rasyonalizasyon haline gelir. Farklı pekiştirme, belirli bir suç davranışıyla ilişkili ödülleri ifade eder. Bu suç davranışı, başlangıçta, bireylerin başkalarını izleyerek ve dinleyerek eylem ve davranışları öğrendiğinde ortaya çıkan taklit süreci yoluyla öğrenilir. Dolayısıyla, bir kişi bir suç işlediğinde, başkalarının yaptığını gördüğü eylemleri taklit etmektedir (Burruss vd., 2012). Siber suçla ilgili olarak, araştırmalar, sosyal öğrenme teorisinin yazılım korsanlığının gelişimini ve devam eden sorununu açıklayabildiğini bulmuştur. Yazılım korsanlığı üzerine yaptıkları çalışmada Burruss ve diğerleri, yazılım korsanlığı akranlarıyla ilişki kuran bireylerin sapkın davranışları öğrendiğini ve ardından kabul ettiğini buldu. Yazılım korsanlığı, erişmek için belirli bir düzeyde beceri ve bilgi ve bu becerileri orijinal olarak öğrenmek için sapkın akranlar gerektirir. Ayrıca, sapkın bireyler suç davranışlarını rasyonalize eder ve diğer bireylere bu rasyonalizasyonları ve davranışları öğreten ve birbirine bağlayan bir ağın geliştirilmesine yardımcı olur. Çalışma ayrıca, diğerlerinin katılımları için olumlu pekiştirme gördüklerini gördüklerinde, bireylerin yazılım korsanlığına katılma olasılıklarının daha yüksek olduğunu ileri sürdü (Burruss ve diğerleri, 2012). Yazılım korsanlığını yalnızca sosyal kontrol teorisi açıklamakla kalmaz, bu teorinin unsurları diğer siber suçlara atfedilebilir. Örneğin, herhangi bir suçta, rasyonelleştirmeler ve beceriler öğrenilmeli ve davranış, diğerlerinin çağrışımı ve gözlemlenmesi yoluyla pekiştirilmelidir. Bu nedenle, sosyal öğrenme teorisinin arkasındaki ana fikir, çevremize dayanarak olduğumuz kişi olduğumuzdur ve bu açıklama siber suçları açıklamak için kullanılabilir. Sapkın bireyler suç davranışlarını rasyonalize ederler ve diğer bireyleri birbirine bağlayan ve bu rasyonalizasyonları ve davranışları öğreten bir ağın geliştirilmesine yardımcı olurlar. Bu nedenle, sosyal öğrenme teorisinin arkasındaki ana fikir, çevremize dayanarak olduğumuz kişi olduğumuzdur ve bu açıklama siber suçları açıklamak için kullanılabilir.

### 4.3. Sosyal Kontrol Teorisi

Kontrol teorileri, bireylerin toplumdaki değer, norm ve kurumlara olan bağlılığını ve bu bağlılıkla oluşan sosyal denetim olgusunu temel alır. Suç olgusunu, bireylerin davranışlarında etkili olan aile yapısı, çevresel faktörler, inançlar gibi sosyal değişkenler ışığında değerlendirmektedir. Bu teori sapmanın ana nedenini sosyal kontrolden eksiklik olarak kabul etmiştir. Temel varsayımı insanların sapma eğilimi gösterdiği ve kontrol altına alınmazsa sapma yapacağıdır. Bu davranışlar ise bağlanma eksikliğinin ürünüdür. Bu konuda dikkate değer bir teori Hershey'inkidir. Ergenlerin ve gençlerin suça yönelik faaliyetlerini önleyen faktörün sosyal bağlantılar olduğunu iddia etmektedir (Bokhaara'ea ve Karimi, 2016:48).

Bu teori aslen kriminologlar Michael Gottfredson ve Travis Hirschi tarafından geliştirilmiştir. Kendi kendini kontrol teorilerinin her zaman her tür suçu açıklayabileceğini öne sürmüştür. Düşük öz denetime sahip bireyler, risk alma, dürtüsellik ve basit ve kolay işleri tercih etme ile karakterize edilmiştir. Bu özellikler, bireyin sapmanın sonuçlarını doğru bir şekilde hesaplama yeteneğini engeller. Bu teoriye göre suç, anında tatmin elde etmenin bir yolu olarak görülür ve bu tür kısa vadeli arzuları geciktirme yeteneği, özdenetim ile bağlantılıdır. Suça karışma eğiliminde olanların yeterli öz denetimden yoksun oldukları düşünülmektedir. Ayrıca, düşük öz denetime sahip insanlar fazla düşünmeden ve o anda ne hissettiklerine bağlı olarak. dürtüsel davranırlar. Bu, eylemlerinin sonuçlarını düşünmedikleri için onları risk alan kişiler yapar. Son olarak, düşük öz denetime sahip insanlar kendilerine odaklanır ve başkalarına karşı empatiden yoksundur. Gottfredson ve Hirschi'ye göre, düşük öz kontrol, ebeveynlerin ebeveynliklerinde etkisiz olduklarında erken sosyalleşmeden kaynaklanmaktadır. Bu nedenle, ihmal eden ve ilgisiz ebeveynler, çocuklarını sosyalleştiremeyebilirler (UKEssays, 2018).

Çocuğa karşı sevgiyle yönlendirilen ve izleme, uygunsuz davranışın belirlenmesi ve uygunsuz davranışın cezalandırılmasından oluşan etkili ebeveynlik, çocuklara (yüksek) özdenetim aşılamak için yeterlidir. Bununla birlikte, daha da önemlisi, özdenetim gelişimi için kritik dönem, yaşamın ilk 8-10 yılıdır. Gottfredson ve Hirschi'ye göre çocukluktan sonra, bireyler arası özdenetim düzeyleri sabitlenir ve özdenetim geliştiremeyenler "sefalet dolu bir yaşam için bir an zevkine" mahkûm olur (Wiatroski, 1981). Sonuç olarak, özdenetim düzeyi düşük olan çocuklar suça daha yatkın hale gelirler ve suç eğilimleri sonraki yaşamlarında da devam eder. Düşük öz kontrolün özellikleri, yazılım korsanlığı da dahil olmak üzere bazı basit siber suç biçimlerine uygulanabilir. Burruss ve diğerleri yaptıkları çalışmada, düşük öz kontrol düzeylerinin yazılım korsanlığı eylemiyle doğrudan ilişkili olduğunu belirtmişlerdir. Örneğin, bir kişinin dürtüsel davrandıkları ve yazılımın bir kopyasını satın almak için

bekleyemedikleri için yazılım korsanlığı yapması muhtemeldir. Bu kişilerin telif hakkı sahibine karşı anlayışlı olmaları ve herhangi bir sorumluluğu ihmal etmeleri olası değildir. Ayrıca, bu kişilerin yazılım korsanlığına katılmanın heyecanı ve kolaylığından etkilenmeleri muhtemeldir. Çalışma ayrıca, düşük öz kontrolün yazılım korsanlığı üzerinde bir etkisi olduğunu ve sosyal öğrenme teorisinin ölçtüğünü (yani, sapkın akranlarla ilişki kurmak ve yazılım korsanlığına karşı olumlu tutumlar) bu etkiyi koşullandırır. Bu nedenle, düşük öz-denetim özelliklerinden, düşük öz-denetim düzeyine sahip olanlar, hemen tatmin olma istekleri nedeniyle hem çevrimiçi hem de çevrimdışı olarak sapkın davranışlara katılmaları muhtemeldir (UKEssays, 2018).

Sosyal Kontrol Teorisi insanların kurallara neden ve nasıl uyduklarına dair bir açıklama sunmaktadır. Davranış, toplumdaki beklentilere uygundur. Sosyal Kontrol Teorisine göre içsel kısıtlamalar çocukluk döneminde gelişir ve yetersiz kısıtlamalar nedeniyle suç oluşmaktadır. Başka bir deyişle, özgür irade suçlulara sapkın davranışları için seçim ve sonuç olarak sorumluluk vermiştir. Sosyal Kontrol Teorisi, çevrimiçi anonimliğin serbestliği teşvik ettiği iddiasını desteklemektedir. Buna göre Sosyal Kontrol Kuramı, bireyleri suç ve sapkın davranışlardan kaçınmaya mecbur bırakmaktadır. Sosyal dışlama ve yasalar dahil olmak üzere sosyal kontroller mevcuttur. Ancak, sapma nerede büyürse kontroller veya kontrollerin varsayılan gücü eksik veya azalmıştır (Zuhri, 2017).

## 5. SONUÇ

Bilgisayarlar ve internet günümüz toplumunda ortak bir yer haline gelmiştir. Bu yeni teknoloji, yeni bir suç türü olan siber suçların gelişmesine neden olmuştur. Suçlu davranışı tamamen tek bir teoriyle açıklanamamakta ve çeşitli teorilerin birleşimini gerektirmektedir. Her teorinin farklı yönleri, her bir teorinin açıklayamadığı şeyi telafi etmek için birlikte kullanılabilir. Örneğin, sosyal öğrenme teorisi, suçun sapkın akranlarla ilişkilendirme yoluyla öğrenildiğine inanır ve araştırmalar, bir bireyin sahip olduğu sapkın akran sayısı ile yazılım korsanlığına katılımı arasında bir ilişki olduğunu zaten göstermiştir. Ancak araştırmacılar, sosyal öğrenme teorisinin tüm siber suç türleri için mi yoksa yalnızca belirli siber suçlar için mi geçerli olduğunu incelemediler. Diğer taraftan, kontrol teorisi, düşük öz denetimin her zaman suçun nedeni olduğunu ileri sürer. Bu, bazı suçlular için doğru olabilir, ancak beyaz yakalı suçlara karışanlar gibi birçok suçlu, düşük öz kontrol ilkelerine bağlı değildir. Bununla birlikte, kontrol kuramı, bireylerin neden belirli bir şekilde hareket edebildiklerini açıklamada faydalı olurken, bir suçun oluşması için yerine getirilmesi gereken durumları açıklamaz

Kontrol teorisine benzer şekilde, gerilim teorisi, bir bireyin hedeflerine ulaşamaması durumunda, stres yaşayarak bunun sonucunda suça yönelebileceğini söylemektedir. Ancak araştırmacılar, bir bireyin 'gerçek dünyadaki' gerginliğinin sanal dünyadaki sapkın davranışlarını etkileyip etkilemediğini daha fazla inceleyebilir. Bu nedenle, bir bireyin düşük öz-kontrol ve onun sapkın çağrışımları ve düzenli faaliyetleri ile birleşen olumsuz gerilimi, bireyin çevrimiçi ortamda mağdur olma riskini artırabilir. Gelecekteki siber suç mağduriyeti çalışmaları, sorunu araştırmak için bu teorilerin bir kombinasyonunu kullanmaktan fayda sağlayabilir. Siber suç araştırmaları, toplumlar teknolojiye giderek daha fazla bağımlı hale geldikçe, suç anlayışımız için önemli olacaktır.

21.yüzyılda büyüyen siber suçlar topluluğunun etkileri yıkıcıdır ve son derece maliyetlidir. Bireyler, özel kuruluşlar, devlet kurumları hatta devlet kurumları hedef olabilmektedir. Siber suç özünde geleneksel suça benzer motivasyonlara sahiptir. Fail hala insan; sadece suç işleme aracı değişmiştir. Bu nedenle, geleneksel suçta olduğu gibi, siber suça katkıda bulunan faktörler, özellikleri, saldırganlar ve kullanılan silahların aralarındaki ilişki kapsamlı bir anlayış için gereklidir. Siber suçlar kriminologların söylediği suçlardan çok farklı değildir. Siber suçlularda diğer suç gruplarına benzemektedir. Bundan dolayı siber suça kriminolojik bir yaklaşım siber suçun temel nedenlerini tanımlamakta ve siber güvenlik politikalarının geliştirilmesine yardımcı olmaktadır. Siber terörizmle başa çıkmak için siber suç davranışını açıklamak için tasarlanmış teorileri operasyonel hale getirerek siber terör ağlarını bozmak ve kapasite geliştirme çabaları hükümetlerin yapılacaklar listesinde olması gerekmektedir.

## KAYNAKÇA

Alaca, B. (2008). Ülkemizde Bilişim Suçları Ve İnternetin Suça Etkisi (Antropolojik Ve Hukuki Boyutları İle). Ankara Üniversitesi SBE, Yayımlanmamış Yüksek Lisans Tezi.

Alnıak, O. (2004). Siber Terörizm Raporu. https://tasam.org/Files/Icerik/File/siber_terorizm_raporu_84be5753-d219-418f-9a68-e6c719b645b1.pdf (14.11.2021).

Altuntop, S. (2012). Suça Bakışta Kontrol Yaklaşımı Ve Kontrol Teorileri, Kriminoloji Dergisi. Yıl:4, Sayı:2, 1-15.

Amerikanınsesi. (8 Temmuz 2009). Amerikan Devlet Daireleri Siber Saldırıya Uğradı, https://www.amerikaninsesi.com/a/a-17-2009-07-08-voa18-88138417/871375.htmlr (10.11.2021).

Baştuğ, M. F.(30 Eylül 2021). Cyber Evolution of Terrorist Groups https://orionpolicy.org/orionforum/58/cyber-evolution-of-terrorist-groups (21.11.2021).

Bokhaara'ea ve Karimi (2016). Sociological Analysis of Cybercrimes, Iranian Amin police university quarterly Quarterly of Criminal and Intelligence Researches, Volume 11, Issue.2, Summer, 39-53.

Burruss, George W., Bossler, Adam M. And Holt, Thomas J. (2012). Assessing the mediation of a fuller social learning model on low self-control's influence on software piracy. *Crime and Delinquency*, 59(5), 1157-1184

Büker, H. (2011). Sosyal Bir Olgu Olarak Tehdit Suçu ve Kriminolojik Yaklaşımlar, İdarecinin Sesi, eylül – ekim, 58-61.

Cömert, Ö. ve Sevim, Y. (2017). Çocuk ve Suç İlişkisinin Sosyolojik Suç Kuramları ile İncelenmesi. Bitlis Eren Üniversitesi Sosyal Bilimler Enstitüsü Dergisi. Cilt: 6, Sayı:1, Haziran, 29-40.

CNNTÜRK.(2021). Anonymous hacker grubu kimdir, nedir, yaptıkları hackler neler? https://www.cnnturk.com/teknoloji/anonymous-hacker-grubu-kimdir-nedir-yaptiklari-hackler-neler (21.12.2021).

DHS, Homeland Threat Assessment October 2020 https://www.dhs.gov/sites/default/files/ publications/2020_10_06_homeland-threat-assessment.pdf (23.11.2021).

Erdem, M. ve Özocak, G. (2017). Sınıraşan Bir Suç Olarak Siber Suçlarla Mücadelede Uluslararası İşbirliği. http://ozocak.com/Dosyalar/d863d5.pdf (15.11.2021).

Fındıklı, R. (2011). Suçların Önlenmesinde Kültürel Değerlerin Rolü. Suç Önleme Sempozyumu. Bursa, 1-6.

Furnell, S. 2002. Cyber Crime: Vandalizing the Information Society. London: Addison Wesley.

Küçükvardar, M. (2018). Suç Olgusunun Değişen Yüzü:Siber Suçlar. Uluslararası Bilişim, Teknoloji ve Felsefe Dergisi. Yıl:2018, Sayı:1, 1-17.

Merton, R. K. (1968). *Social Theory and Social Structure*. New York: Free Press.

McGuire, M., & Dowling, S. (2013). Cybercrime: A review of the evidence: Summary of key findings and implications. Home Office Research Report 75. London: Home Office, October.

Patchin, J. W. ve Hinduja, S. (2011). Traditional and non-traditional bullying among youth: A test of general strain theory. Youth & Society, 43(2), 727-751.

Rogers, M. K. (2010). The Psyche of Cybercriminals: A Psycho-Social Perspective. In S. Ghosh, & E. Turrini, *Cybercrimes: A Multidisciplinary Analysis* (pp. 217–235). Berlin: Springer-Verlag.

Runions, Kevin C. (2013). Toward a conceptual model of motive and self-control in cyber-aggression*:* Rage, reward and recreation. Journal of Youth and Adolescence, 42(5), 751-771.

Sarre, R. (2017). Metadata retention as a means of combatting terrorism and organized crime: A perspective from Australia. Asian Journal of Criminology, 12, 167–179.

Shinder, D. L. (2002). Scene of the Cybercrimes. Syngress Publishing Inc, Rockland, USA.

Smith, T. E. .(2015). A Conceptual Review and Exploratory Evaluation of the Motivations for Cybercrime, DOI: 10.13140/RG.2.1.4358.5129 (25.11.2021).

Şeker, S. (2009). Bilgi Çağının Değerlendirilmesi. https://www.ab.org.tr/ab05/tammetin/9.doc (09.11.2021).

UKEssays. (November 2018). Applying Criminological Theories to Cyber Crime. https://www.ukessays.com/essays/criminology/explaining-cybercrime-using.php?vref= (16.11.2021).

Wiatroski M. (1981) Social control theory and delinquency, american socialogical review, vol 46,525-541 https://www.ncbi.nlm.nih.gov/pmc/articles/PMC8095718/ (03.11.2021)

Yasintimur, A. (2019). Bilişim Suçlarının Suç Sosyolojisi Açısından Değerlendirilmesi. https://www.difose.com.tr/bilisim-suclarinin-suc-sosyolojisi-acisindan-degerlendirilmesi/ (05.11.2021)

Zuhri, Fadi Abu. (2017). Why Are The Cybercriminals Attracted To Commit Crimes, https://digitalforensicsmagazine.com/blogs/wp-content/uploads/2017/05/Why-Are-Cybercriminals-Attracted-To-Commit-Crimes.pdf (06.11.2021).