T.C.
SAKARYA ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ

SİBER DÜNYADA HACKER KÜLTÜRÜ, HACKTİVİZM VE BİLİŞİM SUÇLARI

YÜKSEK LİSANS TEZİ

Nurullah SANDİLAÇ

Enstitü Anabilim Dalı: Sosyoloji

Tez Danışmanı: Dr. Öğr. Üyesi Yaşar SUVEREN

HAZİRAN – 2021

T.C.
SAKARYA ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ

SİBER DÜNYADA HACKER KÜLTÜRÜ, HACKTİVİZM VE BİLİŞİM SUÇLARI

YÜKSEK LİSANS TEZİ

Nurullah SANDİLAÇ

Enstitü Anabilim Dalı: Sosyoloji

"Bu tez sınavı 21/06/2021 tarihinde online olarak yapılmış olup aşağıda isimleri bulunan jüri üyeleri tarafından oybirliği / ~~oyçokluğu~~ ile kabul edilmiştir."

JÜRİÜYESİ	KANAATİ
Doç. Dr. Osman ÖZKUL	BAŞARILI
Doç. Dr. Emre GÖKALP	BAŞARILI
Dr. Öğr. Üyesi Yaşar SUVEREN	BAŞARILI

SAKARYA ÜNİVERSİTESİ	**T.C.** **SAKARYA ÜNİVERSİTESİ** **SAKARYA ÜNİVERSİTESİ ENSTİTÜSÜ** **TEZ SAVUNULABİLİRLİK VE ORJİNALLİK BEYAN FORMU**	Sayfa : 1/1

Öğrencinin

Adı Soyadı	:	**NURULLAH SANDİLAÇ**
Öğrenci Numarası	:	**Y166013001**
Enstitü Anabilim Dalı	:	**SOSYOLOJİ**
Enstitü Bilim Dalı	:	**SOSYOLOJİ**
Programı	:	☑ YÜKSEK LİSANS ☐ DOKTORA
Tezin Başlığı	:	**YENİ TOPLUMSAL HAREKETLER: TÜRKİYE'DE HACKERLIK VE HACTİVİZM KÜLTÜRÜ**
Benzerlik Oranı	:	**%18**

SAKARYA ÜNİVERSİTESİ ENSTİTÜSÜ MÜDÜRLÜĞÜNE,

☑ Sakarya Üniversitesi Sosyal Bilimler Enstitüsü Enstitüsü Lisansüstü Tez Çalışması Benzerlik Raporu Uygulama Esaslarını inceledim. Enstitünüz tarafından Uygulalma Esasları çerçevesinde alınan Benzerlik Raporuna göre yukarıda bilgileri verilen tez çalışmasının benzerlik oranının herhangi bir intihal içermediğini; aksinin tespit edileceği muhtemel durumda doğabilecek her türlü hukuki sorumluluğu kabul ettiğimi beyan ederim.

Nurullah Sandilaç **01/06/2021**

☐ Sakarya Üniversitesi ..... Enstitüsü Lisansüstü Tez Çalışması Benzerlik Raporu Uygulama Esaslarını inceledim. Enstitünüz tarafından Uygulalma Esasları çerçevesinde alınan Benzerlik Raporuna göre yukarıda bilgileri verilen öğrenciye ait tez çalışması ile ilgili gerekli düzenleme tarafımca yapılmış olup, yeniden değerlendirilmek üzere .....@sakarya.edu.tr adresine yüklenmiştir.

Bilgilerinize arz ederim.

...../...../20.....
İmza

Uygundur

Danışman
Unvanı / Adı-Soyadı: Dr. Öğr. Üyesi Yaşar Suveren

Tarih: 01/06/2021

İmza:

☐ KABUL EDİLMİŞTİR ☐ REDDEDİLMİŞTİR **EYK Tarih ve No:**	**Enstitü Birim Sorumlusu Onayı**

ÖNSÖZ

Bu tezin yazılması sırasında, çalışmamı takip eden danışmanım. Dr. Yaşar SUVEREN'e değerli katkı ve emekleri için teşekkürlerimi ve saygılarımı takdim ederim. Tezimin nihai aşamaya gelmesinde önemli katkıları olan savunma sınavı jüri üyeleri Doç. Dr. Osman ÖZKUL ile Doç. Dr. Emre GÖKALP hocalarıma çok teşekkür ederim. Bu vesileyle tüm hocalarıma teşekkürlerimi borç bilirim. Son olarak bu günlere ulaşmamda emeklerini hiçbir zaman ödeyemeyeceğim aileme şükranlarımı sunarım.

NURULLAH SANDİLAÇ

21.06.2021

İÇİNDEKİLER

KISALTMALAR

ARPANET : Advanced Research Projects Administration Network

NSFNET : National Science Foundation

DARPA :Defence Advanced Research Project Agency

EARN : Europian Academic And Research Network

TÜBİTAK : Türkiye Bilimsel ve Araştırma Kurumu

ODTÜ : Orta Doğu Teknik Üniversitesi

NASA : National Aeronautics and Space Administration (Ulusal Havacılık ve Uzay Dairesi)

DOS : Disk Operating System (Disk İşletim Sistemi)

MIT : Massachusetts İnstitute Ot Technology (Massachusetts Teknoloji Enstitüsü)

FBI : Federal Bureau of Investigation (Federal Soruşturma Bürosu)

TCK : Türk Ceza Kanunu

ABD : United States of America (Amerika Birleşik Devletleri)

ATM : Automatic Teller Machine

CD : Compack Disc (Yoğun Disk)

DVD : Digital Versatile Disc (Çok Amaçlı Sayısal Disk)

WWW : WorldWideWeb

TV : Television (Televizyon)

MGK : Milli Güvenlik Kurulu

KHK : Kanun Hükmünde Kararname

UDHB : Ulaştırma Denizcilik ve Haberleşme Bakanlığı

USOM : Ulusal Siber Olaylara Müdahale Merkezi

SOME : Siber Olaylara Müdahale Ekipleri

YÖK : Yüksek Öğrenim Kurumu

TİB : Telekominikasyon İletişim Başkanlığı

DDOS : Distributed Denial Of Service

ECHELON : Elektronik İzleme Sistemi

NATO : North Atlantic Treaty Organization (Kuzen Atlantik Antlaşma Örgütü)

NSA : National Security Agency (Ulusal Güvenlik Ajansı)

TCP : Transmission Control Protocol

Sakarya Üniversitesi
Sosyal Bilimler Enstitüsü Tez Özeti

Yüksek Lisans	X	**Doktora**	

Tezin Başlığı: Siber Dünyada Hacker Kültürü, Hacktivizm ve Bilişim Suçları

Tezin Yazarı: Nurullah SANDİLAÇ **Danışman:** Dr. Öğr. Üyesi Yaşar SUVEREN

Kabul Tarihi: 21/06/2021 **Sayfa Sayısı:** vii(önkısım)+ 121(tez)

Anabilim Dalı: Sosyoloji

Enformasyon çağında yeniden biçim kazanan kapitalizmin yarattığı siber dünyada siber, suç, siber terör, siber savaş ile hacker, cracker, hacing, cracking kavramları ön plana çıktığı görülmektedir. Siber alanın aktörleri, direniş kimlikleri etrafında örgütlendiği anlaşılmaktadır. Bu aktörlerin bir kısmı geleneksel suçları bilgisayar vasıtasıyla işleyen siber suçlular, bir kısmı terörizmden beslenen siber teröristler bir kısmı da bilişim sistemlerinin mucitleri sayılan hackerlar ve hacktivistlerden oluşmakta ve kendi mücadelelerini verdikleri görülmektedir. Günümüzde birçok devlet tarafından hackerların eylemleri, suç olarak nitelendirilmekte ve buna göre yasal düzenlemeler ile tedbirler alınmaktadır. Sınırı kestirilemeyen bu yeni alanda devletlerde panik havası oluşturmuş ve kontrol altına almak için baskıcı tavırlar sergilemişlerdir. Otorite erkleri tarafından baskılandığını düşünen azınlık grupları, demokratik hak ve özgürlük savunucuları ise devletlerin yapılan tüm hukuki ve fiziksel tedbirlerin yurttaşları gözetlemek, izlemek ve denetim altına alabilmek için bir araç olarak kullanıldığını savunmaktadırlar. Bir anlamda devletler kendi insanları ile çatışmaya girmektedirler. Günümüzde hem devletlerin resmi görüşü hem de toplumsal algı açısından hacker kelimesine olumsuz anlamlar yüklenmekte ve çağrıştırmaktadır. Popüler olanın bir adım ötesine geçtiğimizde hackerlerin azılı birer suçlu, menfaat ve para peşinde koşan ya da basit bir hareket, duruş olarak değil, temel etik kuralları, dünyaya bakışları ve yaşam tarzları olduğunu yani bir kültürü temsil ettiğini, alt/karşı kültür olarak nitelendirildiğini görmekteyiz.

Anahtar Kelimeler: Siber Suç, Siber Savaş, Siber Terör, Hacker Kültürü, Hacktivizm

Sakarya University
Institute of Social Sciences Abstract of Thesis

Master Degree	X	**Ph.D.**	

Title of Thesis: Hacker Culture, Hacktivism and Cybercrime in the Cyber World

Author of Thesis: Nurullah SANDİLAÇ **Supervisor:**Assist. Prof. Yaşar SUVEREN

Accepted Date: 21.06.2021 **Number of Pages:** vii (pre tex) +121(body**)**

Department: Sosyology

In the cyber world created by capitalism, which has reshaped in the information age, it is seen that the concepts of cyber, crime, cyber terrorism, cyber war and hacker, hacking, craking come to the fore. It is understood that the actors of the cyber space are organized around the identities of resistance. Some of these actors are cybercriminals who commit classical crimes through computers, some of them are cyber terrorists who feed on terrorism, and some of them are hackers and hacktivists, who are the inventors of information systems, and it is seen that they are fighting for themselves. Today, the actions of hackers are considered as crimes by many states and legal regulations and measures are taken. In this new area, the border of which cannot be predicted, the states created an atmosphere of panic and displayed oppressive attitudes to take it under control. Minority groups and defenders of democratic rights and freedoms, who think that they are oppressed by the authorities, argue that all legal and physical measures taken by the states are used as a tool to spy on, monitor and control citizens. In a sense, states conflict with their own people. Today, in terms of social perception, the word hacker has negative meanings and connotations. When we go one step beyond the popular, we see that hackers are not only criminals, pursuit of profit and money, or simply a movement or stance, but that they represent a culture and are described as a sub/counterculture.

Keywords.Cyber Crime, Cyber Warfare, Cyber Terror, Hacker Culture, Hacktivism

GİRİŞ

Enformasyon çağında yeniden oluşan/biçim kazanan kapitalizmin yarattığı siber dünyada, siber, suç, siber terör, siber savaş ile hacking, cracking kavramları ön plana çıktığı görülmektedir. Siber alanın aktörleri, direniş kimlikleri etrafında örgütlendiği anlaşılmaktadır. Siber dünyadaki aktörlerin bir kısmı klasik suçları bilgisayar vasıtasıyla işleyen siber suçlular, bir kısmı terörizmden beslenen siber teröristler bir kısmı da bilişim sistemlerinin mucitleri sayılan hackerlar ve hacktivistlerden oluşmakta ve kendi mücadelelerini verdikleri görülmektedir. Tabiri caizse siber dünyayı toz duman kaplamakta ve eylemlerin nasıl, kimin, kime karşı yapıldığı kestirilemediği bir durumla karşı karşıya kalınmaktadır. Böyle bir kargaşada tanımlamalar, tanımlayanların bulunduğu konuma göre değişmekte, kavramlar üzerinde uzlaşılamamakta sonuç olarak bu olgu ve kavramlar üzerinde anlam kayması veya anlam karmaşası görülmektedir.

Hacker, en genel anlamıyla bilişim sistemlerine hakim olan, bilgisayar yazılımlarını sıradan insanlardan daha fazla bilgi ve beceriye sahip olan ve sürekli yazılım geliştiren kişi olarak tanımlanmaktadır. Hacking ise, hackerların bir başka bilişim sistemine sızma faaliyeti olarak kabul edilmektedir. Hackerlar, sızma girişimlerini genel kabul gören hacker ilkeleriyle bağdaştırmamakta, bu eylemleri cracking kavramıyla ifade etmekte ve bu eylemleri yapanları kendilerinden ayırmak için cracker kavramıyla ifade etmektedirler.

Kitle iletişim araçlarının yaygınlaşması ile bireylerin duygularını, düşüncelerini ve tepkilerini ifade etme biçimi olarak sanal eylemcilik ortaya çıkmıştır. Hacktivizm ise, hacking ve aktivizm sözcüklerinin birleşiminden doğmuş ve sanal eylemciliğin bir yönetimi olarak kabul edilmiştir (Yegen, 2014, s. 85). Bu yönetimi kullanan kişilere ise hacktivist denilmektedir.

Ancak günümüzde birçok devlet tarafından bu kişilerin yaptıkları eylemler, suç olarak nitelendirilmekte ve buna göre yasal düzenlemeler ile tedbirler alınmaktadır. Bu anlamda günümüzde birer suçlu olarak kabul edilen hackerlar ve hacktivistler küresel ölçekte yapılan direniş mücadele biçimleri, çalışmamızın temel konusunu oluşturmaktadır.

Bu nedenle çalışmamızın birinci bölümü, küreselleşme kavramı ve küreselleşmeyle birlikte yeni toplum biçimini meydana getiren süreçler ile başlanmıştır. Bilgi ve iletişim teknolojilerinin sürekli gelişmesi ve tüm dünyaya yayılmasıyla, küreselleşme kavramının ortaya çıkmasındaki etkenlerden biridir. Aynı zamanda küreselleşmenin genişlemesiyle de itici bir kuvvet olmaktadır (Büyükbaykal, 2008: 40).

Küreselleşmenin miladı veya tohumların atıldığı dönemler konusunda her ne kadar sosyal bilimciler arasında ayrılıklar mevcut ise de yine de mutabık kalınan, daha kabul gören dönemin, yani birinci dalganın 1870 lerden itibaren sanayi devrimi ile başlayıp 1920 lere kadar devam ettiği, ikinci dalganın ise ikinci dünya savaşı ile devam ederek siyasal ve ekonomik yapıların yeniden oluşturulduğu, 1970'li yıllardan itibaren bilgi teknolojilerindeki gelişmeler, birleşen ekonomilerin yarattığı cazip yatırım olanakları, bütünleşen pazarların getirdiği karlılık fırsatları küreselleşme dürtülerini uyarmış olup, hız kazanan ulusal sınırlar dışındaki pazar arayışları, çok uluslu firmaların çoğalıp büyümeleri, uluslararası anlaşmalar ve iletişim teknolojisindeki hızlı gelişmeler sonucu 1990 yıllara gelindiğinde küreselleşme olgusu görmezden gelinemeyecek kadar belirginleşmiştir. Bu anlamda küreselleşmeyi ortaya çıkarak faktörleri siyasi, ekonomik ve teknoloji olarak 3 grupta toplamam mümkündür.

Küreselleşmenin ne olduğu konusunda genel hatları çizildikten sonra küreselleşmenin teknolojik etkileri daha ayrıntılı bir şekilde açıklanmıştır. Bilişim ve iletişim teknolojilerinin gelişmesiyle zaman/mekan sıkışmasıyla dünyanın küçülmeye başladığı görülmektedir. Kitle iletişim araçları, iletişim hızını artırmak suretiyle maliyetini düşürüp, daha ucuz ve hızlı etkileşimle, birçok ürünü ve faaliyeti yerelleştirip bütünleşmiş ağlar sayesinde dağıtımı kolay hale getirerek küreselleşmeyi mümkün kılmıştır.

Bu itibarla teknolojilerin gelişmesiyle küreselleşmeye etkileri büyük katkılarının yanında internetin ortaya çıkışı ile kendi başına küreselleşmeye farklı bir boyut getirmiştir. Bu sürecin yanında gün geçtikçe küçülen bir evrende yeni fırsatlar ve meydan okuyucu gelişmeler yaşanmış ve halen yaşanmaya devam etmektedir.

Sonrasında çalışmamızın kuramsal yönünü esas teşkil eden, küreselleşme konusunda en kapsamlı çalışmayı yapanlardan biri olan Manuel Castells'in ağ toplumu teorisinden bahsedilmiştir. Küresel ağ karşısında bireyin durumunu, teknik-bilimsel gelişmeler ve siyasal yapılanmalar ışığında incelemiştir. Küreselleşme ve kimlik çelişkilerinin sebep olduğu gerilim içerisinde, enformasyon teknolojilerinin etkisiyle şekillenen, bir tarafta demokrasiyi sekteye uğratıp dünyayı enformasyon yoklusu/zengini olarak kutuplaştırıp, diğer tarafta radikal toplumsal oluşumlara imkân tanıyan yeni bir toplum biçiminden bahsetmiş ve enformasyon çağındaki bu yeni topluma "ağ toplumu" adını vermiştir.

Ağ toplumunu, birbirinden bağımsız üç süresin meydana gelmesinden oluşmaktadır. Bu süreçler açıklandıktan sonra, ağ toplumunun bir önceki sanayi toplumu ve enformasyon toplumlarından farklılıkları açıklanmıştır. Bu anlamda hız, hacim, yoğunluk, esneklik ve dağıtım yönüyle diğer toplum biçimlerinden ayrıştığı anlaşılmaktadır.

Bu bölümün son kısmında, ağ toplumunun temel yapıları açıklanmaktadır. Devlet ve ekonomi yapısının ilişki biçiminden öte, kültürün yani gerçekliğin nasıl sanallaştırıldığı izah edilmiştir. Ardından ağ toplumunda sınıf ve kimlikler üzerinde durulmuştur. Bu itibarla ağ toplumunda kapitalizmin klasik sınıf anlayışı ortadan kalkmaktadır. Yerine teknolojiye uyum sağlayan ağ işçileri sınıfı ortaya çıkmaktadır. Yine kimlikleri; meşrulaştırıcı, direniş ve proje olarak kategorileştirmiştir. Manuel Castells'e göre direniş kimlikleri bu kimlikler arasında en önemli kimlikler olduğunu ifade etmektedir. Çünkü bu kimlikler komünler ve cemaatleri birlikte getirerek tahammül edilemeyen baskılara karşı direnişin sınırlarının içselleştirilmesini kolaylaştırdığını söylemektedir.

İkinci bölümde ana konular; bilişim sistemi, siber suç, siber terörizm ve siber savaş konuları etrafında şekillenmiştir. Öncelikle bilişim sisteminin ne olduğu hangi unsurlardan oluştuğu açıklanmıştır. Bilişim sistemleri temelde bilgisayar ve internetten oluşmaktadır. Bu nedenle internet ve bilgisayar tarihinden bahsedilmiştir. Bilgisayar ve internetin ortaya çıkmasından sonra suçun sanal dünyada da işlenebilme kolaylığı görülmüştür. Tek bir tıklama ile dünyanın bir ucundan diğer bir ucuna siber saldırı yapılabilecek teknolojiye kavuşulmuştur. Bu nedenle suç olgusu ve suçun siber dünyaya nasıl yansıdığı ele alınmıştır.

Siber suç, elektronik bilgi işlem kayıtlarına yasadışı yollarla erişilmesi veya bu katıların kanuni olmayan şekilde değiştirilmesi, silinmesi veya bu tür kayıtlara girilmesi veyahut bilgi tecavüzü için hazırlık yapılması olarak tanımlanmaktadır (Aydın, 1992, s. 27-28). Çalışmamızın bu bölümün ortalarında siber suçun aşamaları, saldırı türleri ve kullandıkları siber silahlar nelerdir bunlardan bahsedilmiştir. Ardından siber terörizm ve siber savaş kavramları açıklanmıştır. Sonrasında siber saldırı biçimlerinin ve eylemlerin birbirleriyle olan ilişkili irdelenmiştir. Her ne kadar siber suç, siber terörizm ve siber savaşın eylemleri ve kullandıkları araçlar benzerlik gösterse de motivasyonları, elde edilen kazanımları ve doğurduğu toplumsal sonuçları bakımından farklılıklar görülmektedir.

Bu bölümün sonunda ise ülkemizde bilişim suçların TCK'daki yeri ve cezai müeyyideleri açıklanmıştır. Bu anlamda ülkemizde, bilişim suçları ile ilgili olarak ayrı bir kanuni düzenleme bulunmamakta, TCK içerisinde bir başlık oluşturulduğu görülmektedir.

Çalışmamızın üçüncü ve son bölümünde, araştırmanın konusu başlığında ayrıntılı olarak izah edileceği üzere hack ve hacker kültürü ele alınmıştır. Hacker ve hacker kültürüyle ilgili alandaki kavramsal ve olgusal karmaşa sonucunda en azından popüler düzeyde çoğu kez yanlış düşünce ve algıların söz konusu olduğu söylenebilir.

Araştırmanın Konusu

Castells'e göre, enformasyonel devrimlerin meydana gelmesindeki alt yapı internet ve bilgisayardır. Enformasyonel devrimlerdeki ticari boyut ise yeni iş türleri alanı olarak karşımıza çıkmıştır. Başka bir ifadeyle enformasyonel devrimler, kendini yeniden üreten ve büyük şirketlere (Apple, Microsoft, Dell Computer, Cisco Systems, oracle, Sun Microsystems vs.) evrilenler sayesinde olmuştur. Peki enformasyon ruhu ile biçimlenen ve dönüşen büyük şirketler, hangi temel ilkeler üzerine yapılanmışlardır? sorusuna dönük Castells, bu temel unsurun hem yenilikçi hem de yaratıcı hacker kültürünü temsil eden bir kültürün kaynağı üzerine yapılandırıldığını ifade etmektedir (Castells, 2005, s. 160).

Ancak günümüzde hem devlet otoriteleri ve medya organları tarafından hem de toplumun genel kesimi tarafından bakıldığında, *hacker* denen kişiler, onlar için sadece sisteme izinsiz sızarak kişisel belgeleri elde eden, kredi kartı bilgilerini çalan gibi olumsuz yönde anlamlar yüklenmekte ve çağrıştırmaktadır. Popüler algının ötesinde bakıldığında bambaşka bir gerçeklikle karşılaştığımızı söyleyebiliriz. Bu gerçeklik, hackerlerin azılı birer suçlu, menfaat ve para peşinde koşan, ya da basit bir hareket, duruş olarak değil, etik kuralları olan, dünyaya bakış açılarıyla ve farklı yaşam tarzlarıyla esasında bir kültürü temsil ettiğini hatta sadece kültür olarak değil bir alt/karşı kültür olarak nitelendirildiğini görmekteyiz.

Çalışmamızın son bölümünde hacker kültürünün daha iyi anlaşılabilmesi için hack ve hacker kavramlarının ortaya çıkışı ve tarihsel gelişiminden söz edilmiştir. Başlangıçta bilgi ve becerileri göstermek maksatlı yapılan eşek şakalarının, bilgisayarların kullanımının yaygınlaşmasıyla bu kavramların kullanımının bilişim alanlarına kaydığı görülmektedir. Sonrasında kişisel bilgisayarların yaygınlaşması ve kötü niyetli kişilerin bu alanı istismar etmesiyle hacking faaliyetlerin devletler tarafından suç kapsamına alındığı görülmekte ve artık olumsuz anlamlara doğru evrildiği görülmektedir.

Sonrasında hacker kültürünün beslendiği kaynakları ve eylem motivasyonları irdelenmiştir. Hack kültürünün temelde Hakim Bey, Wiliam S. Burroughs gibi yazarların eserlerinden etkilendiği görülmektedir. Yine cyberpunk kültüründen etkilendikleri ve bu kültürün maddi boyutunun File Jargon'da toplandığı anlaşılmaktadır.

Bu kısımdan sonra, hacker etiğinin genel kabul gören ilkelerinden bahsedilmiştir. Ayrıca bu etik değerlerin günümüz toplumunun hakim anlayışına karşı nasıl bir muhalefet gösterdiği konusunda bir eleştirel bakış açısı geliştirilmiştir. Bu eleştirel bakış açısından Pekka Himanen'in eserinden yararlanılmıştır.

Daha sonra geçmişten günümüze doğru hacker çeşitlerinden bahsedilmiştir. Başlangıçta sadece tek bir hacker çeşidi varken zamanla ve günümüzün kabul ettiği en genel kategorileştirmesiyle renklere göre; beyaz, gri, siyah ve kırmızı şapkalı hacker

çeşitlerinin olduğu görülmektedir. Ardından Dünya'da ve ülkemizde tanınmış hacker gruplarından bahsedilmiştir. Bu hacker grupları aynı kategoride değerlendirmek mümkün olmamıştır. Kimileri ideolojiden, kimileri hacker etik ilkelerinden, kimileri de devlet yanlısı gruplardan oluştukları görülmüştür. Dünyaca en ünlü hacker grubu olan Anonymous grubu ile ülkemizdeki en ünlü olan Redhack adlı hacker gruplarına ayrı parantez açılmış ve günümüzdeki konumları değerlendirilmiştir. Son olarak Türkiye'de hacker kültürü ve hacktivizmin nasıl algılandığı ve neler yapıldığı konusunda Ufuk Eriş'in yapmış olduğu çalışmasından bahsedilmiştir.

Araştırmanın Amacı

Bu çalışmamızda siber suç, siber savaş ve siber terör kavramları ile hacker, hacktivizm kavramları arasında bir ayrım gözeterek daha geniş bir perspektif üzerinden bu olgu ve kavramlar ele alınması amaçlanmıştır. Konu ile ilgili temel araştırma sorusu: hackerlar Hack kültürüne alt/karşı kültür olarak ele alındığında: Hackerlar ağ toplumunda birer siber suçlu mu yoksa direniş kimliği etrafında örgütlenmiş toplumsal hareketlerin aktörleri midir? şeklinde oluşturulmuştur. Çalışmanın alt problemlerini açıklamak için oluşturulan diğer sorular şu şekildedir:

- Hack kültürüne, karşı kültür olarak ele alındığında hackerlar yasaları çiğnemek için eylemlerini meşrulaştırmak ve isnat edilen suçlamalara mantıklı bir savunma yapmak mı istemektedirler yoksa demokrasinin ve ifade özgürlüğünün mevcut olduğu ülkelerde baskıcı iktidarların politikaları sonucu şekillenen siyasi, ekonomik, eğitim, kültürel alanlarında bir direnişi, tepkiyi mi ifade eder?
- Hackerlar, yaşadıkları ülkelerde yasalarla düzenlenen bilişim suçlarına karşı nasıl bir düşünceye sahiptirler?
- Siber suç, siber terörizm ve siber savaş kavramları farklı mıdır? Farklı ise, farklı kılan etmenler nelerdir?

Çalışmamızda yukarıda yazılı olan sorulara cevap aranmıştır.

Önemi

Bu çalışma, ağ toplumuna yönelik hâkim anlayışa karşın eleştirel bir bakış açısı sunmaya çalışmaktadır. Bunu yaparken hacker etiği ve hackerların eylem pratikleri üzerine odaklanarak gerek mikro analizler geliştirmek gerekse de alan yazındaki boşluğu kapatmaya yönelik katkıda bulunmak ve farkındalık oluşturması açısından önem arz etmektedir.

Yöntemi

Bu çalışmamızda, nitel araştırma yöntemi esas alınmıştır. Nitel araştırma, "gözlem, görüşme ve doküman analizi gibi nitel veri toplama yöntemlerinin kullanıldığı, algıların ve olayların doğal ortamda gerçekçi ve bütüncül bir biçimde ortaya konmasına yönelik nitel bir sürecin izlendiği araştırma" şeklinde tanımlanmaktadır (Yıldırım ve Şimşek, 2011: 39).

Bu çalışma, nitel perspektife uygun olarak, belgelere dayalı gözlem tekniği uygulanmıştır. Bu nedenle alan yazında literatür taraması yapılmış olup çalışma kapsamında gerekli görülen kitap, dergi, makale, yayınlanmış tezler, internet belgeleri, vb. dokümanlar incelenmiştir.

Sınırlılıkları

Çalışmanın sınırlılıklarından şu şekilde bahsedilebilir. İlk olarak ele alınan küreselleşme sürecinin ekonomik, kültürel, antropolojik ve dini boyutları göz ardı edilmiştir. Küreselleşme kavramına, sürecine ve küresel toplumu oluşturan süreçlere temas edildikten sonra teknolojik gelişmelerin küreselleşmeye etkileri üzerine odaklanılmıştır. Yine küreselleşme konusunda derin tartışmalara gidilmemiş, yabancı literatür konusunda Türkçe diline çevrilmiş temel metinlere ve önemli yazarlara değinilmiştir. Daha sonra ülkemizde yapılmış olan ikincil kaynaklar diyebileceğimiz çalışmalardan yararlanılmıştır.

Bilişim sistemleri, bilgi güvenliği, siber savaşlar, hacker gibi başlıklarda alanyazında yapılan çalışmaların çoğunlukla mühendislik bilimiyle alakalı olarak teknik meseleler

üzerinden ele alındığı tespit edilmiştir. Ayrıca uluslararası ilişkiler ve hukuk biliminin sınırlarında çalışmalar yapıldığı da görülmüştür

Bu anlamda temel problemin cevabı aranırken hackerlık ve hackerlık kültürü ile ilgili net bir biçimde ayrışan üç tür kaynağın olduğu görülmüştür. Bu kaynaklardan ilki, hackerlar hakkında olumsuz bir algı oluşturmayı amaçlayan ve geneli bilgisayar teknolojisine yakın olmayan bireylerin kaleminden çıkan ve tarafgirlikleri düşmanlıktan öteye gitmeyen metinlerden oluşmaktadır. İkincisi, Siber Ulusal Güvenlik Politikalar çerçevesinde özel veya kamu kurumlarının kriminal suç perspektifinden ve hukuksal boyutlarının ele alındığı metinlerden oluşmaktadır. Üçüncü kaynak türleri ise, hackerlara yönelik dolaylı ya da doğrudan yakınlıkları olan ya da hackerlar ile ilgili malumatları mevcut olan insanların çalışmalarından çıkan kaynaklardan oluştuğu görülmüştür.

Çalışmanın ikinci bölümünde, siber suç, siber terörizm ve siber savaş konularından bahsedilirken birinci ve ikinci tür kaynaklardan yararlanılmıştır. Ayrıca alanyazında bilişim suçları ve siber suçların birbirlerinin yerine kullanıldığı görülmüştür. Her ne kadar bilişim suçlarından, siber suç kavramına göre bir üst kavram olsa da, Avrupa Birliği ile müzakere sürecinde bulunulan, AB müktesebatında uyum adı altında yedi paket halinde yüzlerce yasada değişiklik yapıldığı, Türk Ceza Kanunu, Ceza Muhakemesi Kanunu, Medeni Kanun, Hukuk Usulü gibi 80 yıllık temel kanunların değiştirildiği, en önemlisi Avrupa Birliğine uyum sağlamak için Anayasa'nın değiştirildiği, bir dönemde Türkiye'nin üyesi olduğu Avrupa Konseyi'nin "Siber Suç" kavramını kullanması ve özellikle son zamanlarda yapılan çalışmalarda siber suç kavramının tercih sebebi olduğunu ifade edildiğini belirtmek gerekir. Bizde bu görüşe katılmaktayız. Ancak bilişim suçu kavramına yüklenen kültürel ve dönemsel anlam bütünlüğü de göz önüne alındığında geçmiş ve mevcut yasal düzenlemeler ışında Türk Ceza Kanunu'nda bilişim suçu kavramı hem öğreti de hem uygulamada görüş birliği halinde yerleşmiş olduğu ve tercih edildiği görülmekte, bu nedenle çalışmada ülkemizdeki durumu ifade ederken bilişim suçu kavramı, dünyadaki gelişmeleri ifade ederken siber suç kavramı kullanılmıştır.

Hacker, hacker kültürü, hacktivizm konularında çok fazla çalışmanın bulunmadığı tespit edilmiştir. Araştırma yöntemine uygun düşen, konuya dahil olan hacker topluluklarının kullandıkları sözlü ve yazılı dil, algıları, davranış kalıpları ve paylaştıkları tecrübeleri içeren üçüncü tip kaynaklardan yararlanılmıştır.

Ayrıca hacker etiği konusu ele alınırken, çağımızın hakim anlayışı olduğu belirtilen dinden arındırılmış Weber'in kapitalizmin ruhuna atfettiği iş etiğine karşı eleştirel bir yaklaşım eseri olan Pekka Himanen'in "Hacker Etiği" eserinden oldukça yararlanılmıştır.

Çalışmamızda hacker ve cracker ayırımlarına dikkat edilmiştir. Bu doğrultuda hacker kavramını, belli etik ilkeleri olan, günümüzde beyaz şapkalı hackerlar diyebileceğimiz kişiler, cracker kavramını ise yeraltı dünyasında bilişim suçlarını işleyen kişiler olarak ifade edilmiştir.

BÖLÜM 1: KAVRAMSAL VE KURAMSAL YAKLAŞIM

Küreselleşmenin ne olduğu konusunda zengin bir literatür mevcuttur. Bu olgu ve kavramsallaştırma, dünyadaki her türlü yaşamsal ve kavramsal alanı etkilediği için, küreselleşme hakkında yazılan metinler, yazarların uzman oldukları alanın olanakları ve araçlarıyla toplumsal etki ve sonuçlarını anlamaya ve açıklamaya çalışmaktadırlar. Bu nedenle tek bir küreselleşmeden bahsetmek mümkün değildir.

Küreselleşme üzerine yapılan araştırmalarda sosyal bilimlerin tek tek konusunu aştığından disiplinler arası incelenmek durumunda olduğu söylenmektedir (Çiftçi İ. , 2015, s. 17).

Çalışmamızın esas konusunu doğrudan Manuel Castells'in ağ toplumu teorisi ihtiva etmektedir. Kuramsal bakış açımızı daha iyi anlayabilmek için öncelikle küreselleşme kavramını açıklamamızda zorunluluk bulunmaktadır.

Ancak yukarıda az önce bahsettiğimiz gibi birçok sosyal bilimcinin küreselleşme hakkında birbirinden farklı görüşleri bulunduğundan ve yine çalışmamız ile dolaylı bir bağlantısı olduğundan çalışmamızda, küreselleşme hakkındaki tüm çalışmalara derin bir şekilde açıklamaya ve tartışmaya çalışılmamıştır. Çünkü bunu yaptığımız takdirde konu bütünlüğünün sağlanamayacağı, çalışmanın odak noktasından uzaklaşılacağı ve okuyucunun kuramsal yaklaşıma yoğunlaşamayacağını düşünmekteyiz.

Bu doğrultuda küreselleşme kavramı hakkında genel bir çerçeve çizilmiş çoğunluğunun hemfikir oldukları noktalara temas edilmiş ve ardından Manuel Castells'in ağ toplumu kuramı açıklanmaya çalışılmıştır.

1.1 Küreselleşme

Küreselleşme, sosyal bilimlerde neredeyse her şeye muktedir olan sihirli kavramı haline gelmiş, bu kavram sosyolog Peter L. Burger'in ifadesiyle, Japon gençlerinin cinsel alışkanlıklarındaki değişimden, Alman kömür endüstrisindeki gerilemeye kadar her şeyi açıklayan veya açıklamakta kullanılan bir kavram haline gelmiştir (Çiftçi İ. , 2015, s. 15).

Küreselleşme veya “globalleşme”, İngilizce terimi ile “globalization” kelimesinin karşılığıdır. Globalleşme küresel olma, küreyi kapsar hale gelme anlamına gelmektedir. Küreselleşme kavramı ile ilgili farklı görüşler bulunmaktadır.

Küreselleşme Modelski’ye göre dünyanın büyük ve güçlü medeniyetlerinin karşılıklı bağlantının tarihi olduğunu ifade etmektedir (Held ve McGrew, 2008, s. 71). Friedman’ a göre küreselleşme, Lexus ve zeytin ağacının başrollerini paylaştığı bir drama olduğunu söylemektedir (Friedman, 2002, s. 58). Ona göre küreselleşme sürecinde toplumların, ekonominin ve ülkelerin; teknoloji alanında yapılan ilerlemenin etkisiyle geçmişe göre yoğun hareketli biçimde birbirinden daha ucuz ve derinlikli etkilenmesi ve bütünleşmesi engellenemez şekle geldiğini (Friedman, 2002, s. 17).

Paul Hirst ve Grahame Thompson küreselleşme kavramı ile ilgili olarak, yerel kültürlerin, ekonomilerin ve devlet sınırların çözülmeye gittiği, sosyal yaşamın büyük bir çoğunluğu küresel gelişmeler tarafından şekillendiği bir çağ olduğunu söylemektedirler. Bu düşüncenin altyapısında, yeni ve hızlı ekonomik küreselleşme süreci fikri olmaktadır (Hirst ve Thompson, 2007, s. 26).

Küreselleşme kavramı Bauman’a göre dünyanın kaçamayacağı kaderi ve geri dönüşü olmayan bir süreç olduğunu ifade etmektedir (Bauman, 2018, s. 7). Bauman, zaman/mekan sıkışmasının küreselleşme sürecinde aynı etkilere sahip olmadığını, zaman ve mekanın dönüşümüyle bu alanın kullanımları hem farklılaşmış hem de farklılaştırdığını iddia etmektedir. Küreselleşme birleştirirken aynı zamanda bölmektedir. Birleşme ile bölünmenin nedenleri aynı sebeplere dayanmaktadır. Ekonomi ve bilgi işlem akışlarının küresel boyutlara ulaşmanın yanında yerelleşme süreci de devam etmektedir (Bauman, 2018, s. 8).

Giddens ise küreselleşme sürecinin sağlamış olduğu faydalar kazandırmış olduğu tecrübeler ve getirmiş olduğu olumsuz sonuçlara rağmen ne olursa olsun, önceki dönemlerde mevcut olan ekonomi yapısından farklı bir şey olmadığını dünyanın büyüm ölçekte eskisi gibi döndüğünü söylemektedir (Giddens, 2000, s. 20). Yine küreselleşmeyi, batı modernleşmesinin bir sonucu olduğunu ifade etmekte, toplumsal ilişkilerin yoğunlaşması anlamında kullanmaktadır. Bu anlamda birbirlerinden uzak

olan mekanlar birbirleriyle iletişim kurabilmekte, yine bir yerde yaşanan hadise nedeniyle başka bir yerdeki bölgeyi etkilemekte ve şekillendirmekte ya da bunun tam zıttı da geçerli olabilmektedir (Giddens, 2018, s. 66).

Robertson'a göre küreselleşme, bir yandan dünyanın küçülmesine bir yandan da bütünsel olarak dünya bilincinin güçlenmesine gönderme yapmaktadır (Robertson, 1999, s. 21). Robertson burada küreselleşmeyi yorumlarken küresel kültüre önem verdiği görülmektedir. Ona göre küreselleşme ister istemez küresel bir kültürün oluşmasına imkan tanırken aynı zamanda farklılıkların ve kırılmalarında yaşanacağı bir süreci de içinde barındırdığını ifade etmektedir (Robertson, 1999, s. 54). Dünyayı aşırı karmaşıklıktan ve kaostan korumanın anahtarı ise yerel geleneklere ve kültürel çeşitliliklere mümkün olduğunca saygılı bir küresel toplum oluşturmak fikrini dile getirmektedir (Robertson, 1999, s. 134).

Görüldüğü üzere küreselleşme kavramı ile ilgili her ne kadar farklı görüşler bulunsa da herkesin hemfikir olduğu nokta, küreselleşmenin şeyler, mekânlar ve insanlar arasındaki karşılıklı etkileşimi ve bağlantısallığı arttırdığıdır.

Küreselleşme kavramının tüm dünyayı kapsayan ve etkileyen modern anlamdaki manada kullanılmaya başlaması hususunda farklı tezler mevcuttur. Bu tezlerden bazılarına göre; küreselleşme (globalization) kavramı ilk defa 1980 yılında Stanford, Harvard, Columbia gibi itibarlı Amerikan okullarında kullanılmaya başlanmış ve bu çevrelerce popülerliğini kazanmıştır. Diğer bir teze göre, başlangıçta 1960 yılında Marshall McLuhan'ın ünlü "*küresel köy*" kavramının ilk kullanımına işaret etmektedir (Erbay, 2011, s. 283). Ancak birkaç istisna dışında kavramın isim babasının M. Mcluhan olduğunda hemfikirdiler.

Genel olarak küreselleşme olgusu "mal ve hizmet ticareti, insanların göç etmesi, teknik bilginin değiş tokuş edilmesi, doğrudan yabancı yatırım ya da yurtdışında fabrika ve şirket kurmak ya da satın almak ve hisse senedi, bono gibi finansal varlıklara sınır ötesi yatırım yapmak" şeklinde tanımlanmıştır (Harford, 2008, s. 41).

Küreselleşme kavramı, ilk önce ekonomi alanında daha sık kullanılmıştır. Son yüzyılda dünyadaki üretim, geçmiş zamana kıyasla, akışkanlığı teknolojik gelişmelerin etkisiyle hızlanan sermayenin yapısı gereği herhangi bir güçle karşılaşmadan giderek artmaktadır. Endüstri devrimi sonrası gelişmiş devletlerdeki iç taleplerin doyum noktasına erişmesiyle sanayicilerin yeni pazar arayışları bulma arzuları bu durumu hızlandırmakta, toprak sınırları aşılarak gümrükler kolaylaştırılmakta ya da ortadan kaldırılmaktadır. Komünizmin yıkılmasıyla dünya genelinde kapitalist serbest piyasa ekonomisi yayılmıştır. Bundan sonra en az iki devlet topraklarında faaliyet yapan uluslararası şirketlerin üretim ilişkileri mevcuttur. Bu şirketlerden bir kısmı ülkelerden bile büyük bütçelerle bir başka ülkedeki siyasi otoriteleri etkileme gücüne sahip aktörlere dönüşmektedirler (Giddens, 2018, s. 73).

Görüldüğü üzere küreselleşme, başlangıçta ekonomi ile ilgili bütünleşmiş, dünyanın tek pazar durumuna gelmesi olarak algılanmış ise de zamanla kavrama siyaset, sağlık, teknoloji ve benzeri alanları da kapsayacak şekilde anlamlar yüklenmiştir. Ülkeler artık sadece ekonomik açıdan birbirlerine bağımlı kalmamış, zamanın ve mekânın değişimiyle ilgili bağlantılı bir kavram haline dönüşmüştür. Küreselleşme çağında, devletlerin toprak sınırları önemini kaybetmiştir. Dünyamızın tek ve büyük bir toprak parçası olarak anlaşılması ve toplumların bütünleşmesi gibi simgesel bir mana yüklenmiştir (Kaypak ve Haytoğlu, 2016, s. 717-718).

Küreselleşme, bağlantılık, zamanın hızlanması, teknoloji, mekânın küçülmesi ve sermaye başlıkları altında beş ortak özelliğe sahiptir. Bağlantılılık, farklı kültürlere veya aynı kültürlerden olan ancak birbirlerinden uzak yerlerdeki insanların bağlantılı duruma gelmesini ifade etmektedir. Bir yerden başka bir yere gitmenin kolay ve hızlı olması ile artık mekânın küçülmesinden bahsedilir hale gelmiştir. Teknolojinin gelişmesiyle bilginin, paranın ve yatırımın döngüsü (sermaye) olanaklı hale gelmiş, bir o kadar da bu döngünün akışı hızlanmıştır (Kaypak ve Haytoğlu, 2016, s. 718).

Küreselleşme olgusu, tek bir süreçten bahsedilmemekte kendi içerisinde dört farklı değişim sürecini içermektedir: Ekonomik, siyasal ve toplumsal faaliyetler devletlerin siyasal sınırların ötesinde başka bölgelere yaymakta; ticaret, finans, yatırım, kültür ve

göç transferlerinin artmasını gerçekleştirip bağlılıkları kuvvetlendirmekte; dünyayı hızlandırmakta, iletişim ve taşıma sistemlerindeki buluşlar, insanların, düşüncelerin, sermayenin ve bilginin daha hızlı hareket etmesi kabiliyetini kazanmakta; yerelde yaşanan yenilikler dahi makro ölçekli küresel neticelere neden olabilmektedir. Devlet problemleriyle küresel olaylar arasındaki çizgi gittikçe belirsizleşmektedir (Kaypak ve Haytoğlu, 2016, s. 718).

Böylelikle küreselleşme, yukarıda bahsettiğimiz tüm bu özelliklerden ötürü, 20. yy. sonuna doğru toplumsal hareketler konusunda yeni belirleyici kıstas haline gelmiştir. Sinema, televizyon, radyo ve internet aracılığıyla insanoğlu her alanda daha önce hiç olmadığı kadar farklı kültürlerin değerleri ile karşılaşmaktadır.

Yukarıda küreselleşmenin ne olduğu konusunda bir fikir verilmeye çalışılmış olup bir sonraki başlıkta temel düzeyde küreselleşmeye dair yaklaşımların nasıl sınıflandırıldığı konusunda izah getirilmeye çalışılmıştır.

1.1.1 Temel Yaklaşımlar

Küreselleşmenin nasıl kuramsallaştırılacağına dair üç temel yaklaşımın mevcut olduğu kabul edilmektedir. Bunlar: hiper-küreselleşmeciler(radikaller), kuşkucular ve dönüşümcülerdir (Held ve McGrew, 2008).

Hiper-küreselleşmeciler, dünya toplumunda, geleneksel devletin yerini almakta olduğu ve yeni tip toplumsal örgütlenme biçimlerini belirmeye başladığını düşünmektedirler. Küreselleşme, ulus ötesi üretim, ticaret ve finansal ağlarıyla ekonomilerin milli özelliğini ortadan kaldırmaktadır. Tek pazar haline gelmekte olan sınırsız dünya ekonomisi içinde ulusal hükümetlerin konumu, güçlü yerel kuruluşlar arasındaki trafiği idare etmekten başka nedir? diye sormakta ve bütün yaklaşımlarında, küreselleşmenin kaçınılmaz bir kader ve insanın da buna uymakta acele etmesinden başka bir seçeneğinin olmadığını her türlü yerel ve ulusal değerlerinde sonunu ilan etmektedirler (Çiftçi İ. , 2015, s. 49).

Kuşkucular, yani küreselleşme karşıtları, aşırı küreselcilerin karşısında yer almaktadırlar. Küreselleşme olgusuna yönelik her duruma şüpheyle yaklaşmaktadırlar. Toplumsal yaşamda her şeyin yeni olmadığını söylemektedirler. Küreselleşme karşıtları, küreselleşmenin geçmişine bakarak, günümüzde olduğu gibi önemli düzeyde mal ve para akışının olduğunu söylemektedirler. Günümüzde halen devletlerin birçoğu, ülke giriş çıkışlarına yönelik sıkı güvenlik uygulamalarına karşın, 19. yüzyılda insanların pasaport ve vize işlemleri gibi bir kontrol uygulamaları kullanmadıklarını öne sürmektedirler. Küreselleşme karşıtları, dünya ticaretindeki sınırlamaların kaldırılması doğrultusunda günümüzde yaşanan hadiselerin, 100 yıl öncesine benzer bir duruma geri dönüşün olduğunu iddia etmektedirler. Kısacası, küreselleşmenin yeni bir süreçten meydana gelmediğini kabul etmektedirler. Herkesin küreselleşme terimiyle gereğinden fazla alakadar olmasını devrin ideoloji haline dönüşmesine bağlamaktadırlar. Kuşkucular için küreselleşme, refah ve huzur içinde yaşayan devletini yok edecek asgari düzeyde hükümet ve devlet oluşumunu hedefleyen çevrelerin kullandığı basit bir kelime olduğunu düşünmektedirler (Bozkurt V. , 2000, s. 21).

Dönüşümcüler hem kuşkucuların küreselleşmeyi önemsizleştirme girişimlerini hem de radikal küreselleşmecilerin ortak bir küresel kültür içinde serbest piyasa kapitalizmi görüşünü reddederler. Bu kuramcılar için küresel bağlantıların eşsiz ölçeği, hızı ve yoğunluğu, küresel bağlar ve etkileşimlerin alanını büyük ölçüde genişletmiştir. Küresel bağlar daha fazla yayılmakta ve bilgi ile kültürü olduğu kadar sosyal, ekonomik ve politik ve askeri güçlerden çok daha hızlı, yaygın ve yoğun bir nitelik göstermektedir. Devam eden koca bir dönüşüm mevcut ve bunun önemi hafife alınmamalıdır. Bu değişimlerin ve bunların sonuçlarının doğasını kestirmenin kolay olduğu anlamına gelmemektedir. Sosyal bilimciler, yeni dünyayı tanımlamada yeni benzetmeler kullanmaktadırlar. Fakat bundan yeni tek bir sosyal yapının ya da sonuçları tanımlayabilecek tek bir sosyolojik modelin doğduğu anlamı çıkarılmamaktadır. Aksine, küreselleşme benzerlik ve bütünleşme kadar bölünme farklılıkta üretmektedir. Birleşmiş milletler içinde ve başka yerlerde küresel yönetişim biçimleri gibi güçlü bütünleştirici öğeler doğuyor. Aynı zamanda devletler ulus devletlere bölünmekte ve ayrılıkçı hareketler serpilip gelişirken parçalanma ve çatışmalar ortaya çıkmaktadır.

Bağlar ve etkileşimler, insanları biricik olan küresel bir sistem dâhilinde birbirine bağlamaktadır. Ancak meydana gelen bu durum, birbirine bağlanmış bu sistem, enformasyon, güç ve zenginlik eşitsizlikleri de ortaya çıkarmaktadır (Bilton, ve diğerleri, 2009, s. 51-52).

Aslında bu üç anlayış içerinde esas farklılık, temsil ettikleri dünya görüşlerindedir. Küreselleşmeyi daha iyi kavrayabilmek için onu meydana çıkaran faktörleri de açıklamak gerekmektedir.

1.1.2 Küreselleşme Sürecini Ortaya Çıkaran Faktörler

Küreselleşmenin ortaya çıkması veya hızlanmasını teknolojik, bilimsel, ekonomik ve siyasal nedenlere bağlı olarak incelemek mümkündür. Bu bağlamda küreselleşmeyi besleyen olgulardan bahsetmek gerekmektedir. Küreselleşme sürecinin ortaya çıkmasında teknoloji, ideolojik ve ekonomik faktörler şeklinde üç ana başlığı altında toplandığı görülmektedir.

1.1.2.1 Teknolojik Faktörler

Enformasyon teknolojisinin gelişmesiyle ve bu teknolojinin kullanımının yaygınlaşmasıyla zaman ve mesafe kavramının eski anlamını ortadan kaldırmıştır. Yani mesafe tanımadan insanlar birbiriyle iletişim kurmakta, ülke sınırlarını aşan ticaretler büyümekte, finans piyasalarında etkileşim artmaktadır. Bunun nedeni ise kullanılan teknolojinin (bilgisayar ve internet) hızla yaygınlaşarak uluslararasındaki değişim süresinde küresel dönüşümü hızlandırmaktan kaynaklanmaktadır. Bu süreç halen hızlanarak devam etmektedir.

1.1.2.2 İdeoloji Faktörü

Doğu Blok'unun yıkılmasının ardından serbest piyasaya yönelik güven oluşmuştur. Kısa süre içinde tüm maliyetine rağmen, eski devletçi/planlı ekonomiler, piyasa aygıtı süreci içinde, yabancı sermayenin ve liberal piyasanın olanaklarından faydalanma girişiminde bulunmuşlardır. Yani duvarların yıkılmasından sonra, küreselleşmenin önündeki en önemli engellerden birisi bertaraf edilmiştir. Bu durum her ne kadar Asya

krizinden sonra küreselleşmeye yönelik itirazları artırmış olsa da neo-liberal düşüncenin temel kurallarına güven anlayışı içerisinde hızlandırılarak sürdürülme çabası söz konusudur. Başta Amerika devleti olmak üzere, IMF ve Dünya Bankası gibi uluslararası kuruluşların önderliğinde sürdürülen küreselleşme süreci hızlandıkça, Hegel'in diyalektik görüşünden yararlanarak, anti-tezini meydana getiren anti-küreselci akımlar da tepkilerini göstermeye başlamışladır (Bozkurt V. , 2000, s. 27-28).

1.1.2.3 Ekonomik Faktörler

Gelişmiş devletler, petrol krizi sonrasında dış piyasalara yelken açarak ticari hacimlerini artırma girişimleri ile küreselleşme sürecini ekonomik yönden etkileyen bazı hususlardan olduğunu söyleyebiliriz. Çok uluslu şirketler, ürettiği malları dünyaya yaymaya çalışmışlardır. Bu nedenle her gün yüklü miktarlardaki para, bir ülkeden başka bir ülkeye aktarılmaktadır. Bu şekilde ekonomik faaliyetler gelişince devletlerin bir bölümü birbiriyle bütünleşmeye başlamıştır. Örneğin ülke sınırları içerisinde yaşanan krizler başka bir ülkeyi farklı düzlemlerde etkileyebilmektedir. Yaşanan bu durum doğal olarak ülkelerin ekonomik ve siyasal politikalarını diğer ülkelere göre stratejik olarak belirlemeye itmektedir. Artık devletlerin iç politikalarında yaşanılan problemler ile dış politikalarda yaşanılan problemler arasındaki çizgi gittikçe incelmeye başlamıştır (Bozkurt V. , 2000, s. 28).

Yukarıda küreselleşmeyi besleyen faktörleri kısaca bahsettikten sonra çalışmamızın asıl konusu ile doğrudan bağlantılı olan teknolojinin gelişmesiyle internetin yaygınlaşması ve internetin yaygınlaşmasıyla da küreselleşme sürecindeki fonksiyonlarını ayrı bir başlık altında açıklamaya çalışacağız.

1.1.3 Teknolojik Küreselleşme ve Etkileri

Küreselleşme olgusunun köklerini incelediğimiz zaman Rönesans'taki coğrafi keşiflerle ilk başta yerkürenin her yanının tanınmasına kadar uzandığı görülmektedir. Olayın ilk basamağını bu oluşturmaktadır. Birinci sanayi devrimi dönemince yeni icatlar ve keşiflerle ulaştırma-haberleşmeye yeni boyutlar katılmıştır. İlerleme, denizyollarında ve buhar makinasında uygulamaya girmesiyle 19. yüzyılın ortalarında dünya pazarının

oluşması sağlanmıştır. Telgrafın icadı, fotoğraf, haberleşmenin hızlanmasını ve haber gereçlerinin artışını sağlayan yeni icatlar olmuştur. Bu dönemde sermaye küreselleşmeye başlamış, İngiltere hem sanayi devrimini yaratan hem de coğrafi keşifleri yapan ülke olarak buna öncülük etmiştir. İngiltere serbest ticaretin, sermayenin ve malların küresel çapta serbestçe dolaşmasını, o dönemde daha zayıf olan ABD ve Almanya gibi ülkelerin karşı çıkmasına rağmen devam etmiştir (Kazgan, 2000, s. 26).

Olayın ikinci basamağı olan İkinci Sanayi Devrimi döneminde ise içten patlamalı motorların icadı, ulaştırma ve haberleşmede yenilikçi gelişmelerle devam etmiştir. Avrupa ve ABD'de kitlesel eğitim yaygınlaşmış ve yetişmiş insan gücü ortaya çıkmıştır. Bu dönemde ayrıca karayolları araçlarının devreye sokulması, ilk önce telefon, ardından radyonun icadı, sinemanın icadı ve haberleşmenin yoğunlaşması dünyanın küçülmesini sağlayan en önemli teknolojik gelişmelerden olmuştur. İçten patlamalı motorlar sanayide kullanıldığı gibi birçok tüketim malını da bireyselleştirme imkânı getirmiştir. Otomobil bunun başını çekmiştir. Kitlesel tüketime dönük üretim başlamıştır. İngiltere artık tek büyük devlet değildi. ABD, Fransa, Almanya aynı seviyede seslerini duyurabilir olmuşlardı. İkinci Dünya Savaşı döneminde de yeni teknolojilerin yayılması devam etmiştir. Görüleceği üzere savaşlar yeni teknolojik icatların yayılmasında etkili olmuştur (Kazgan, 2000, s. 27). Tabi ABD, İkinci Dünya Savaşı'nda en az zarar görmesi sebebiyle aslında dünyaya en çok fayda sağlayan devlet olduğu görülmektedir. Savaşta birçok devlet çökmeye kadar götürürken ABD tek güç haline gelerek her alanda güçlenmiş ve 1970'li yıllardan itibaren bilgi teknolojilerindeki gelişmelerle dünyayı tek pazar haline dönüştürmüştür.

Üçüncü Sanayi Devrimi ise inanılmaz mücadelelerin yaşandığı, güç dengelerinde beklenmedik kaymaların ortaya çıktığı, en yerleşik düzenlerin bile kısa sürede allak bullak olduğu bir dönem olduğu görülmektedir. Bu dönem 1970'li yıllarda başlamış ve günümüze kadar devam etmektedir. Birleşen ekonomilerin yarattığı cazip yatırım olanakları, bütünleşen pazarların getirdiği karlılık fırsatları hep küreselleşme dürtülerini uyarmıştır. Bu dönemde küreselleşme; hız kazanan ulusal sınırlar dışındaki pazar arayışları, çok uluslu firmaların çoğalıp büyümeleri, uluslararası anlaşmalar ve iletişim

teknolojisindeki müthiş gelişmeler sonucu 1990'lı yıllara gelindiğinde yadsınamaz ve dışında kalınamaz bir olgu olarak belirginleşmiştir (Biber, 2000, s. 159).

Bu gelişmelere bakıldığında, iletişim teknolojilerinin gelişmesiyle dünyanın küçülmeye başladığı görülmektedir. Monopollerin ortadan kalkması ve rekabetin önemli hale gelmesiyle iş dünyası küreselleşmiştir. Ticari oluşumlarda da politika ve ekonomilerin birbirine bağımlı hale gelmesinde önemli bir rol üstlenerek, küreselleşmeye hız kazandırmıştır. Her insanın, ihtiyaç gördüğü hizmetlere veya ürünlere dünyanın herhangi bir yerinde temin edebilmesi, aradaki mesafenin küçülmesi, paranın, değerli madenlerin anlık olarak dünyanın bir yerinden başka bir yerine gönderilebilmesi, küreselleşmenin önüne geçilmez bir boyuta ulaşmasına sebep olmuştur (Güçdemir, s. 532).

Bilgi ve iletişim teknolojilerinde yaşanan gelişmeler ile iletişimin hızı artmış ve maliyet düşmüştür. Böylece birçok ürün ve faaliyet bütünleşmiş ağlar sayesinde dağıtımı kolay hale getirerek küreselleşmeyi mümkün kılmıştır. Ayrıca ekonomik mesafelerin azalması ile iş dünyasında çalışmaların idaresi için zamandan tasarruf edilmiş, değişim maliyetlerini düşürmüş ve finans pazarlarını kıtalar boyutunda 24 saat aktif konuma getirmiştir. Bu şekilde yeni ekonomik düzenin imparatorlukların ya da ulusal devletlerin başaramadığı ölçüde bir küresel bütünleşmeyi, gelişmiş ülkeler açısından sağlamıştır.

Meydana gelen bu gelişmelerle birlikte birçok düşünür, içerisinde bulunduğu dönemi tanımlamaya ve analiz etmeye çalışmıştır. Ağ toplumu teorisyeni Manuel Castells'de dönemin ruhunu anlamaya çalışan düşünürlerden biridir

1.2 Manuel Castells'in Ağ Toplumu Teorisi

Küreselleşmeye yönelik "ağ toplumu" kavramsallaştırması kuramsal boyutuyla yapılan en kapsamlı çalışmalardan biri Manuel Castells'e ait olduğu söylenebilir. Castells'in "ağ toplumu" teorisini, "Enformasyon Çağı: Ekonomi, Toplum ve Kültür" adlı genel başlıklı eserinde detaylıca işlemektedir. Bu eserde, küresel ağlar karşısında bireyin durumunu, bilimsel ve teknolojik gelişmeler ile siyasal oluşumlar ışığında ele almıştır.

Ağ toplumuna küreselleşme ve tarihsel boyutuyla ele almakta ve geleceğe dönük öngörülerde bulunmaktadır.

Bu eserindeki temel argümanına göre, bilgi teknolojilerinde yaşanan gelişmeler ile kapitalizmin yeniden yapılanmasını sağlamakta ve yeni bir toplumsal biçimlenmenin ortaya çıkması söz konusu olmaktadır Ayrıca yeni kapitalizmin baskısı altında kalan insanların, bu baskıya direnerek yeni iletişim ağları etrafında örgütlenmekte ve yeni toplumsal hareketlerin oluşumuna neden olmaktadır. Bu anlamda yeniden oluşan ve yeni olan bu yapılanmanın siyaset, kültür ve ekonomi alanındaki değişimlerin ile yeni iletişim teknolojilerindeki işlevlerinin ne olduğunu analiz etmiştir.

1.2.1 Endüstri Toplumu

Teknolojik sistemler, yeni bir teknoloji devrimi yaratana kadar gelişir ve çağın hâkim teknolojisi, toplumun esas yapısını değiştirmektedir. Castells'e göre teknoloji "çoğaltılabilir formdaki performans için yöntemler belirlemek amacıyla bilimsel bilginin kullanılmasıdır" (Castells, 2005, s. 146). İnsanlar doğaya hâkim olarak ürettikleri gereçler ile enerji üretme ve dağıtma kapasitesine erişti. İnsanlar kendi gelecekleri ve her çeşit eylem için enerjiye bağlı olduklarından doğadaki hâkimiyetini artırdı. Bu hareket her alanda ortak gelişimlerini sürdürdü ve bir noktada birleştiler. Bu şekilde endüstri çağının temelini, ilk olarak buhar gücüyle, devamında elektrikle, enerji teknolojisindeki devrimlerin attığını ifade etmiştir.

Yaşanan bu endüstri devrimi ile toplumda yeni tüketim, üretim ve toplumsal organizasyonlar oluşmuştur. Oluşan endüstri toplumun altyapısını, teknolojik devrimler sayesinde mümkün kılmıştır.

Castells, sanayi toplumunun temel özelliklerini; büyük şirket, endüstriyel fabrika, akılcılaştırılan devlet yöneticileri, tarımsal işgücünün peyder pey tükenmesi ve kamu hizmetlerinin dağıtımı için merkezi sistemlerin oluşturulması, büyük ölçekli şehirleşme süreci, kitle iletişimin yükselişi, kitle imha silahlarının geliştirilmesi, ulusal ve uluslararası taşımacılık sistemlerin inşa edilmesi şeklinde sıralamaktadır (Castells,

2005, s. 146).Ayrıca Castells'e göre endüstri toplumun üretim biçimleri, refah devleti, hayat standartların yükselmesi, tam istihdam ve seri üretim ilkelerinden oluşmaktadır.

1.2.2 Enformasyonculuk

1970 tarihinde meydana gelen petrol kriziyle ve ardından kapitalist düzende yaşanan buhran sonrası, mevcut endüstriyel üretim biçimlerinin yetersiz kaldığı görülmüştür. Kapitalist sistem kendini mevcut koşullara göre yenilemek ve yeni üretim biçimine geçmek zorunda kalmıştır. Bu yeni endüstriyel üretim biçimi olarak; seri üretim yerine esnek üretim, esnek dağıtım, dikey ilişkiler yerine yatay ilişkilerin hâkim olduğu daha fazla akışkan bir endüstriyel üretim biçimini doğurmuştur (Çeler, 2012, s. 113).

Bunun yanında aynı dönemlere rastlanan endüstriyel kalkınma biçimi olarak endüstriyelliğin yerini almaya çalışan bir teknoloji paradigması ile karşı karşıya kalmıştır. Bu teknolojik paradigma artık endüstriyelliğin yerini almıştır. Castells'e göre bu paradigma uygulandığında, eleyerek rekabete son vermektedir. Toplum üzerinde hâkim olan yeni teknolojik paradigmayı, endüstriyelliği de içine almış olan "enformasyonculuk" olduğunu ifade etmektedir (Castells, 2005, s. 147).

Castells'e göre enformasyon ve bilgi, geçmiş dönemlerdeki birçok toplumda esastı. Geçmişten günümüze dek zenginlik, güç, bilim, teknoloji ve iletişim arasında bir bağlantılılık mevcuttur. Roma İmparatorluğundan örnek vererek teknolojileri, siyasal yapısı ve ekonomik faaliyetleri ve akla mantığa uygun kanunların yazılmasının aslında tüm toplumların özünde enformasyon toplumu olduğunu söylemektedir. Bu nedenle tarihsel bağlamda günümüzü, enformasyon toplumu olarak değilde diğer enformasyon toplumlarından ayırarak "enformasyonculuk" olarak tanımlamaktadır (Castells, 2005, s. 148).

Castells, enformasyon toplumu değil de "enformasyonculuk" olarak tanımlamasının nedenini şu şekilde açıklamaktadır (Castells, 2005, s. 148):

> "Tarihsel dönemimizin ayırt edici özelliği, bir bilgiişlem teknolojileri kümesi çevresinde merkezlenmiş olan bilgiişlem teknolojisi devrimi tarafından başlatılan, yeni bir teknoloji paradigmasıdır. Yeni olan ise, bilgiişlem teknolojisi ve bu teknolojinin, bilgi üretimi ve

uygulaması üzerindeki etkisi. İşte bu yüzden bilgi ekonomisi ya da enformasyon toplumu kavramları yerine enformasyonculuk kavramını kullanıyorum."

Roberts'e göre Castells'in enformasyon toplumu ile teknoloji paradigmasını, Marx'ın teknolojinin toplumu doğrudan etkilediği görüşünün tersine metaları yeniden üretebilmek için sahip olunan bilimsel bilgiyi toplumsaldan ayrı saf bir maddesel kültür alanına yerleştirmektedir (Roberts, 1999, aktaran; Çeler, 2012, s. 113).

Castells'e göre "enformasyonculuk", teknoloji paradigmasının yaşanmasında ki gelişmeler ışığında, iki devrime borçludur. Bunlar "mikroelektronik" ve "genetik mühendisliği"dir. Geçmişten günümüze dek yaşanan teknolojilerin geçmiş toplumlara nazaran günümüzün toplumunda etkisi daha fazladır; çünkü üç temel ayırt edici özelliği mevcuttur:

"1. Hacim, karmaşıklık ve hız açısından kendisini genişleten işlem kapasiteleri,
2. Yeniden birleştirme yetenekleri
3. Dağıtım esneklikleri" (Castells, 2005, s. 148-149).

Böylelikle ağların bilgiyi tutması, dağıtılabilir kılması bakımından hacminin genişliği, hızlı olması ve esnek fırsatlar takdim etmeleri bakımından ağ toplumunda önem kazanmıştır (Bozkurt A. , 2014, s. 519).

1.2.3 Ağ Toplumu

Sanayi devrimiyle birlikte ortaya çıkan sanayi toplumu sonrasında meydana gelen teknolojik ilerlemeler siyasetten ekonomiye, kültürel alandan sağlık sistemine kadar hemen hemen tüm alanlarda yeni bir ilişki biçimini ortaya çıkarmıştır. Castells'e göre sanayileşme sonrasında yaşanan teknolojik gelişmelerin ortaya çıkardığı enformasyon çağı bize *Ağ Toplumu'nu* hediye etmiştir.

Ağ toplumu kuramına gelmeden önce *ağ* kelimesine yüklenen anlamdan söz etmek daha anlamlı olacaktır. Manuel Castells, ağ kavramını, *belli bir toplumsal organizasyonda egemen değerler ve çıkarlar tarafından verilen talimatların programını yerine getiren enformasyon ağıdır* şeklinde tanımlamıştır (Castells, 2004, s. 114). Toplumun yapısını analiz ederken ağ kavramını kullanma sebebi, insanın olduğu her alanda temelde bu ağ

örüntüleriyle bağlanmış ve yoğun bir şekilde kullanılabilir olmasından kaynaklanmaktadır.

Castells' in (2008a) başka bir ifadesiyle ağ "birbiriyle bağlantılı düğümler dizisidir". Bu düğümler birbirleriyle bağlanarak iş bölümünü meydana getirmekte ve ortak karar alınmaktadır. Castells'in, ağ toplumundaki düğümlerin ekonomik, politik, sağlık gibi diğer alanlarda hiç olmadığı kadar birbirleriyle etkileşimde bulunan toplumsal organizasyonun dünyaya yayılması anlamında ifade etmektedir. Castells buna örnek olarak, küresel ekonomi ağındaki düğümler; menkul kıymetler piyasaları olduğunu, Avrupa Birliği'ni idare eden politik ağda; devletlerin bakanlar konseyleri ve Avrupa Komisyonu üyeleri olduğunu, basının küresel ağında ise; haber ekipleri, televizyon sistemleri, bilgisayar grafiği ortamları, eğlence prodüksiyonları, sinyaller üreten, gönderen, alan gezici araçlar olduğunu söylemektedir (Castells, 2008a, s. 622).

Castells'e göre ağ toplumu, birbirinden bağımsız üç sürecin bağlantısı sonucuyla oluştuğunu ifade etmektedir. Bu süreçlerden ilki, 1960'lı yıllarda iletişim alanında yeni toplumsal hareketler, ikincisi 1970'li yıllarda bilgi alanında ortaya çıkan teknolojik devrimler, üçüncüsü ise 1980 yılında kapitalizmin köşeye sıkışarak kendini yeniden şekillendirmek zorunda oluşudur.

1.2.4 Ağ Toplumunun Temel Yapıları

Yaşanan teknolojik ilerlemeler birçok toplumun temel yapılarını değişime uğratmıştır. Yeni ilişki ve organizasyon biçimleri görülmektedir. Aynı zamanda bu biçimler, zaman ve mekanın değişimiyle, sanal uzamın bir parçası olmaktadır. Burada Castels'in tasavvur ettiği ağ toplumundaki tüm temel yapılara değil, çalışmamız ile doğrudan ilgili olan kültür, sınıf ve kimlik ve diğer önemli başlıklar işlenmiştir. Yine devletlerin ve ekonominin yeni ilişki biçimleri ile hakimiyetlerini nasıl paylaşıldığı konusu vurgulanmıştır.

Ağ kuramında, toplumunun temel yapılarından bazıları ise ekonomi alanında "ağ ekonomisi", siyasi alanda da "ağ devleti", kültür "gerçek sanallık kültürü" şeklinde

belirlenmiştir (Yüksel, 2014, s. 4). Yine ağ toplumunda sınıf ve kimlik önemli bir konu olmaktadır.

1.2.4.1 Ekonomi: Ağ Ekonomisi

Castells, kapitalist üretim zihniyetinin yok olmadığını, ekonomi sisteminin ağlar oluşturarak küresel anlamda güçlendiğini ifade etmektedir (Castells, 2008a, s. 624). Sermaye(kapital) ve liberal piyasa, elektronik ağlar temelinde inşa edilmektedir. Uluslararası şirket ve bu şirketlere bağlı alt şirketler ile iş birliğine dayalı işletme ve üretim etrafında ağlar kurulmaktadır. Yerel işletmelere ise bu ağa düğümlenerek onların aracılığıyla çalışmaktadır. Aynı şekilde mezo ve mikro firmalarda iş birliğine dayalı ağ kurulmaktadır. Bu şekilde kaynaklarını birleştirerek esnekliklerini muhafaza etmeye çalışmaktadırlar. Büyük şirketler değişken taleplere, ürünlere, pazarlara ve dönemine göre ağlar arasında stratejik iş birliği üzerinden kurulmaktadır. Tabi bu iş birliği neticesinde müşteri ile üretici arasındaki iletişim lisanslı/tescilli girişimci ağlar üzerinden iletişime geçilmektedir. Castells, ağ ekonomisi için tüm bu karmaşanın üstesinden, yalnızca enformasyonculuğun araçlarıyla gelinebileceğini ifade etmektedir (Castells, 2005, s. 154).

Ayrıca Castells göre bu ağlar sebebiyle yönetim, üretim ve dağıtım alanında yaratıcılık ve rekabetçilik ön planda olduğunu belirtmiştir. Yararsız insanlar ve birimler ağ dışına itilmektedir (Castells, 2005, s. 154). Bu sebeple böyle bir ortamda ağ toplumunda öne çıkanlar uzmanlaşmış kişiler değil, teknolojiye uyum sağlayan, tekniğini geliştiren ve buna yatırım yapan girişimciler olduğunu söylemektedir (Yüksel, 2014, s. 4).

1.2.4.2 Siyaset: Ağ Devleti

Castells, ulus devletlerin çağa uyum sağladığını ifade etmektedir. Bir taraftan devletler, kurumlarını ve iş kabiliyetlerini yeniden düzenleyerek kendi içlerinde de birer "ağ" haline dönüşmüşlerdir. Bunun yansıması olarak Uluslararası Para Fonu, NATO, AB, NAFTA vb. örgütlenmeleri örnek göstererek bu fikrini somutlaştırmıştır. Görüleceği üzere siyasal otorite devletlerce oluşturulan örgütlenmeler ile siyasi organizyonlar arasında paylaşılmaktadır. Bir taraftan da bunun tam zıt yönde devletler, siyasal hakimiyetini bölgesel merkezlere dağıtmaktadırlar. Çünkü hakim zihniyetle çatışmamak, vatandaşları ile esnekliğini geliştirmek ve bu anlamda meşruiyetlerini

muhafaza etmek için yetkilerini yerel kurumlarla ve sivil toplum kuruluşlarıyla bölüşmektedirler. Küresellik ve yerellikte zıt yönlüve eş zamanlı bu paylaşım, yeni devlet şekli olan "ağ devleti" ni meydana getirmiştir (Castells, 2005, s. 156).

1.2.4.3 Gerçek Sanallık Kültürü

Castells, ağları bütünleştiren kültürel bir boyutun olduğunu söylemektedir. Bu kültür, "bilgisayarların siber uzamda gerçekliği yeniden düzenleyerek yarattıkları görsel deneyimler gibi çokyüzlü sanal bir kültür" olduğunu ifade etmektedir (Castells, 2008a, s. 269). Ayrıca buradaki kültürelliğin, "küresel bir elektronik hiper-metnin kaleydoskopu etrafında biçimlenir hale geldiğini" ifade etmiştir (Castells, 2005, s. 155). Castells, hiper metnin World Wide Web olduğunu beyan etmektedir. Hiper metnin; alt yapısı mikro elektronik olan teknolojilerin bir özelliği olan, enformasyonu oluşturan her şeyi yeniden üreten ve birleştiren olduğunu söylemektedir (Castells, 2005, s. 150).

Sanal kültür, zihinleri aşan, ağın içinde yer alan farklı ve birçok katılımcıların stratejilerini dayandırdığı, ağın mensupları değiştikçe değişen, ağdaki birimlerin örgütlenme düzeyi ve kültürel dönüşümlerini izleyen, birçok kültür, değer ve stratejiden meydana gelmektedir (Castells, 2008a, s. 270). İşte sanal kültür bünyesinde yaşanan bu dönüşümlerin, biçimlenmenin ve çeşitlenmenin aracı internet olmaktadır. İnternet ile mekânsal sınırların ortadan kalkması, mekânlar arasında eş zamanlı bir nevi elektronik bir bağ kurmaktadır. Ortak deneyimler ve paylaşılan kültüler öğeler(mesajlar)çoğunlukla hiper-metinde tutsak kalmaktadır. Bu durum yaşamımızın anlamsal göstergesi gerçek sanallığın kaynağını oluşturmaktadır. Sanaldır; çünkü elektronik devrelere ve kısa ömürlü işitsel ve görsel mesajlara dayanmaktadır. Gerçektir; çünkü tüm tecrübe alanlarında, fikirlerimizi meydana getirmekte kullandığımız görüntülerin, seslerin, şekillerin ve anlamlı ifadelerin birçoğu küresel hiper-metin sağladığından, bu hepimizin gerçekliğidir (Castells, 2005, s. 155).Ağ toplumunda "Akışların uzamı" ve "zamansız zaman" kavramları sanal kültür içerisinde ön plana çıktığı görülmektedir.

1.2.4.4 “Akışların Uzamı” ve “Zamansız Zaman”

Castells’e göre ağ oluşturma mantığı, zaman ve mekân pratiğimiz içerisinde dönüştürmüştür (Castells, 2005, s. 156). Zaman ve mekân kavramlarının ağ toplumunda kendine özgü özellikleri yansıttığı söylemektedir. Dolayısıyla Castells’in (2005) de belirttiği üzere ağ toplumunda *akışların uzamı* ve *zamansız zaman* mevcuttur.

Zamansız zaman ifadesi, kitle ve iletişim araçlarının kullanımı ile tanımlanan zamanın dilimlenmesini yok etme amacını taşımaktadır. Bu husus tek bir hiper-metinde geçmişi, geleceği ve şimdiyi bir araya getirilmesine benzetilebilir. Bu şekilde, zamanın özelliği olan (uzamsallık) şeylerin birbirini izlemesi ortadan kalkmış olmaktadır (Eriş, 2009, s. 44).

Castells, 1990 yılının başında akışlar uzamını toplumun hâkim olan çevrenin araçsal ağı olarak tanımlamaktadır. Ancak internet teknolojisinin küresel bir ağ olarak yayılmasıyla akışlar uzamının bir rekabet alanı haline geldiğini, küreselleşme karşıtı hareketler toplumsal hareketler aracılığıyla internet ağlarıyla dünyanın her bir yerine yayıldığını ifade etmektedir. Bunlar, toplumları idare eden hâkim ağların mantığına direnen karşı ağlar oluşturmaktadır. *Akışlar uzamı* giderek hâkim ağlara karşı olan ancak kendileri de ağlar etrafında kümelenen grupların, farklı amaçlarla bir araya gelen sanal grupların/cemaatlerin, genel anlamda gelişen ağ kültürünün uzamı olmaya başlamaktadır (Taş, 2007, s. 317).

Görüleceği üzere Manuel Castells, bu anlamda zaman kavramının yok sayılabilen ve genişletilmiş özelliğine göndermede bulunurken, aynı zamanda teknolojik imkanlarla mekânın, fiziksel sınırlarından ve mesafeden ayrışarak aşıldığını ifade etmektedir.

1.2.4.5 Ağ Toplumunda Sınıf ve Kimlik

Castells, ağ toplumunda eski kapitalist düzendeki gibi bir klasik sınıf olmadığını ifade etmektedir. Ağ toplumu, klasik sınıf anlayışının ötesine geçerek yeni toplumsal sınıflar ortaya çıkarmıştır. Oraya çıkan bu yeni sınıf enformasyon teknolojilerini kullanması, onları dönüştürebilmesi ve kaliteli bir eğitimden geçmiş bireylerden oluşmaktadır. Yeni

sınıflaşmayla birlikte iş ve emek bireyselleştirilmiş olur (Castells, 2008a, s. 630). Böylelikle ağ toplumunda, ağ işçileri sınıfı ortaya çıkarken, ağın dışında kalan diğer birey ve gruplarda ağ toplumunun birer paryasını oluşturmaktadır. Bu şekilde ağ toplumda dışlama, kutuplaşma ve üzerine kurulu düzen hâkim olmaktadır (Çeler, 2012, s. 114).

Castells, kimliklerin, toplumsal aktörler tarafından içselleştirdiğinde kendi anlamlarını bularak bu içselleştirme etrafında örgütlendiğinde de kimlik haline bürüneceğini söylemektedir. Ağ toplumunda toplumsal aktörlerin anlamın, zaman ve uzam içinde kendini muhafaza eden biricik bir kimlik etrafında kümelendiğini ileri sürmektedir. Ayrıca Castells ağ kuramında, bireysel kimlikten ziyade kolektif kimliği ön plana çıkarmaktadır. Ancak Castells burada bireysel kimliği tümüyle yok saymadan bireysel kimliğin kolektivitenin bir parçası olabileceğine beyan etmektedir (Castells, 2008b, s. 13).

Castells, kolektif kimliğin inşa süreci, coğrafyadan, biyolojiden, tarihten, üretken kurumlardan, iktidar aygıtlarından, kolektiviteden, kişisel fantezilerden ve dinsel vahiylerden beslendiğini aynı zamanda toplumların bu kaynakları, içinde bulundukları zaman ve mekân çerçevesinden kaynaklanan toplumsal sözleşmelere ve kültürel projelere göre işleyerek bütün bu kaynakların anlamını yeniden düzenlediğini ifade etmektedir. Castells, kimliğin toplumsal inşa sürecini üç farklı köken ve biçime ayırmaktadır (Castells, 2008b, s. 14):

Meşrulaştırıcı Kimlik: Toplumun hâkim kurumları tarafından, toplumsal aktörler karşısında hâkimiyetlerini yaymak ve akılcılaştırmak için inşa edilmektedir. Bu duruma örnek olarak milliyetçilikler gösterilmektedir.

Direniş Kimliği: Egemen olanın, asıl olanın aklı tarafından değersiz görülen ya da damgalanan koşullarda/konumlarda bulunan aktörler tarafından geliştirilmiştir. Bu duruma örnek olarak etnik kimliğe dayanan milliyetçilikler, cemaatler gösterilmektedir.

Proje Kimliği: Toplumsal aktörlerin, kendilerine verilen kültürel kaynaklar temelinde toplumsal konumlarını yeniden tanımlayarak kimliklerini inşa etmektedirler. Bu süreçte bütün bir toplumsal yapıyı dönüştürmeyi hedeflemektedirler. Örnek olarak feminist hareketi gösterilebilir.

Castells'e göre bir direniş biçimi olarak ortaya çıkan kimliklerin, projeler başlatabileceğini, tarihsel süreç içerisinde toplumsal kurumlarda otorite kurabileceğini, kurulan otoritelerin akılcılaştırmaya yönelik meşrulaştırıcı kimliklere dönüşebileceğini söylemektedir. Ayrıca direniş kimliklerin, kapalı toplumlar ve cemaatleri yanında getirdiğini, toplumda en önemli direniş biçiminin, "direniş kimliği" olduğunu ifade etmektedir. Çünkü tahammül sınırını aşan baskılara karşı kolektif direniş kimliklerini oluşturarak direnişin sınırlarının içselleştirilmesini kolaylaştırdığını söylemektedir (Castells, 2008b, s. 15).

Tüketim toplumun küresel ölçekte hedeflediği tektipleştirici kimlikler, ağ toplumunun tekinsiz kültürel ortamda belirleyici kimlik formlarıdır. Bu yapılara karşı bireyler giderek cinsiyet, etnik ya da inanca dayanan ilksel kimliklerine tutunmaya başlamışlardır. Castells'e göre ağ toplumunun sebep olduğu eşitsizliklere direnmenin tek yolu, toplumsal hareketler olduğunu söylemektedir. Kapitalist ideolojinin klasik sınıfları, ağ toplumunda olmadığına göre direnişin tek şekli toplumsal hareketlerdir. Toplumsal hareketler, oluşan ağ karşısında bir benlik geliştirme isteğinden kaynaklanmaktadır. Globalleşen teknoloji, iletişim ve ekonomi karşısında paralel bir biçimde gelişen bireylerin hayatlarına bir anlam kazandırma arzusundan kaynaklanan kimlik istekleri toplumsal hareketleri doğurmaktadır (Çeler, 2012, s. 114,115).

BÖLÜM 2: SUÇ, SAVAŞ VE TERÖR ÜÇGENİNDE SİBER DÜNYA

2.1 Bilişim Alanında Kullanılan Kavramlar

2.1.1 Bilişim

Bilişim kelimesi aynı kökten gelmekte olan Fransızca dilinde *informatique* kelimesiyle ifade edilen Türkçe dilinde ise enformasyon olarak kullanılmaktadır. Fakat daha sonra bu yabancı kökenli kelime bırakılarak Türkçe karşılığı olan bilişim kelimesi kullanılmaya başlanmıştır (Dülger, 2014, s. 65).

Yazıcıoğlu'na göre bilişim "bilgisayardan da faydalanmak suretiyle bilginin saklanması, iletilmesi ve işlenerek kullanılır hale gelmesini konu alan akademik ve mesleki disipline verilen addır" (Yazıcıoğlu, 1997, s. 131). 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*"*(Yenidünya ve Değirmenci, 2003, s. 27).

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 depolanması ve kullanıcıların erişimine açık bulundurulması bilimidir*"* (Dülger, 2014, s. 67).

Bilişim kelimesi yerine bilgisayar kelimesinin kullanılması yanlış olduğu belirtilmiştir. 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(Yenidünya ve Değirmenci, 2003, s. 31), olsa olsa bilişim sistemi ile bilgisayar kelimelerinin karşılaştırılmasında bu açıklamanın doğru olduğunu ifade etmektedir (Dülger, 2014, s. 66).

2.1.2 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 (Özkul, 2002, s. 14).

Bilişim sistemi, veri ya da bilgileri alan, bu bilgileri işleme tabi kılan, sonuçları veya verileri çıktı şeklinde verebilen elektronik sistemler olarak tanımlanabilir (Akarslan, 2012, s. 27). Bilişim sistemi veya bilişim alanı, verileri toparladıktan sonra bunları otomatik işlemlere tabi kılma olanağı veren sistemlerdir (Malkoç, 2007, s. 1665).

Avrupa Konseyi Siber Suç Sözleşmesi'nde bilgisayar sistemi kavramının, bir ya da birden fazlası belirli bir yazılım etrafında otomatik olarak veri işleyebilen bir aygıtıyla da birbirine bağlı ya da birbiriyle ilişkili bir dizi aygıtı ifade etmektedir (Ergün, Siber Suçların Cezalandırılması ve Türkiye'de Durum, 2008, s. 11).

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. Yönetmenlikte bilişim sisteminin bilgisayardan ibaret görülmesi nedeniyle hatalı olduğu belirtilmiştir (Erdoğan, 2013, s. 16).

2.1.3 Bilişim Sisteminin Unsurları

2.1.3.1 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 (Dülger, 2014, s. 55).

Bilgisayarın birçok tanımı yapılmakla birlikte hızla gelişen bilim ve yeni yeni üretilen teknolojik ürünlerin insan hayatına sokulması sonucunda bilgisayar hakkında yapılmış olan tanımları eksik kalmış, bilgisayarın ne olduğunu tanımlamak zorlaşmıştır. Çünkü klasik bilgisayarı oluşturan unsurların dışında (fare, kasa, monitör) günümüzde bilgisayarın işlevini gören dizüstü bilgisayarı, tablet, akıllı saat gibi yeni bilgisayar türleri çıkmıştır. Yine de genel anlamda bilgisayarın tanımına yer verecek olursak; bilgisayarın yaptığı işler ve işlevlerine göre ile bilgisayarın fiziksel özellikleri ile yaptığı işler ve işlevlerine göre şeklinde iki ayrı yöntem izlenerek tanımı yapılmıştır (Dülger, 2014, s. 55-56). 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" (Yazıcıoğlu, 1997: Aktaran, Dülger, 2014, s. 56). 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 makine olarak tanımlanmıştır(Yenidünya ve Değirmenci, 2003, s. 19).

2.1.3.1.1 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 bütüne denilmektedir. Doktrinde genelde kabul edilen, işletim yazılımı ve uygunluma yazımı şeklinde tasnif edilmektedir (Kurt, 2005, s. 31-36). İşletim yazılımı, bilgisayarın işletilebilmesi için yerine getirmesi gereken yazılımdır. Uygulama yazılımı ise, mevcut olan işletim sistemine yüklenen ve belli bir amaç için kullanılan programlardır(Yenidünya ve Değirmenci, 2003, s. 23-24).

2.1.3.2 İnternet

Türkçe 'ye 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 devamlı olarak üretmekte 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 (İnan, 2000, s. 7-9).

İnsan, internet ile herhangi bir yerdeki bağlanarak elde ettiği bilgiyi bilgisayarına aktarabilmektedir. Ayrıca bilimsel bilgilere, devlet belgelerine, eğlence amaçlı oluşturulmuş listelere, iş ve kişisel ilanlarına ve veri tabanlarındaki her türlü alandaki bilgiye erişmeyi ve bu bilgileri kullanmayı mümkün kılabilmektedir (Bektaş Şeker, 2005, s. 67).

2.1.3.2.1 İnternetin Ortaya Çıkışı ve Gelişimi

İnternetin kökenleri 1960 yılında Amerikan Federal Hükümeti Savunma Bakanlığına bağlı araştırma ve geliştirme birimi olan DARPA[1]' ya dayandırılmaktadır (Çağıltay, 1997, s. 5).

1950 yıllarında SSCB'nin ilk yapay uydusu Sputnik'i uzaya göndermesine karşılık, ABD Savunma Bakanlığına bağlı ARPA isminde bir birim kurmuştur. ABD ve SSCB

[1]Savunma İleri Düzey Araştırma Projeleri Kurumu

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 vermişlerdir (Budak, 2015, s. 4).

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, University College, BBN ve London ile farklı bilgisayarların birbirlerini anlamak için protokol seti geliştirmek amacı internet working projesi başlatmıştır. 1978 yılına kadar farklı bilgisayarın birbirlerini anlayabileceği "İletim Kontrol Protokolü" (TCP) geliştirilmiştir. 1980 yılında bu protokol sabitleştirildi ve ARPANET'e bağlı bilgisayarlar arasındaki iletişim kolaylaştırıldı. 1983 yılında ise tüm ARPANET kullanıcıları yeni bir protokol olan İletim Kontrol Protokolü/İnternet Protokolü (TCP/IP) geçiş yapılmıştır. Daha sonra ARPANET 1990 yılında kullanımdan kaldırılmıştır. Ancak ARPANET ortadan kaldırılmış ise de TCP/IP protokolünün kullanımı ve geliştirilme süreci devam etmiştir (Çağıltay, 1997, s. 6). 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. İsmi verilen konsorsiyum ile

sözleşme imzalanmıştır. Bu şekilde bilgisayarların bir diğer bilgisayara bağlanmasına yarayan bir sistem kurulmuştur (Çağıltay, 1997, s. 7-10).

1989 yılında internetin sivilleşme süreci başlamıştır. İsviçre ülkesinde TİM 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 sağlanmıştır (Bektaş Şeker, 2005, s. 68). Daha sonra dünya genelinde kullanılan milyonlarca ağın da NSFNET'e bağlanması ile 1990 yıllarının başlangıcından günümüzde kullanılan haliyle internetin temeli kurulmuştur.

2.1.3.2.2 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 (Çağıltay, 1997, s. 24).

Türkiye'de internet hazırlıkları 1991 yılında ODTÜ ve TUBİTAK 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 (İnan, 2000, s. 7). Sonraki bağlantı ise 1994 yılında Ege Üniversitesinde TUVAKA kapsamında BITNET bağlantısı amacı ile kullanılan uluslararası hat 64Kbps hız ile Bonn üzerinden internet servisi sunmaya başlanmıştır (Çağıltay, 1997, s. 24). 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 (İnan, 2000, s. 66).

TR-NET'in teknik ve idari yönetimi 1996 yılından sonra ODTÜ BİDB tarafından üstlenilmiştir. TT tarafından sunulan 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 (Çağıltay, 1997, s. 25-26).

Türkiye'de kendi omurgaları olan iki kuruluştan biri ULAKBİLİM, diğer ise TURNET'tir. Bunlardan ilki, akademik amaçlı bağlantılar amacıyla çalışmaya başlanmıştır. Diğer ise ticari amaçlı faaliyetlerini sürdürmüştür. Daha sonra 1 Haziran 1996 yılında TUBİTAK çatısında Ulusal Akademik Ağ ve Bilgi Merkezi (ULAKBIM) ismiyle Yüksek Öğretim kurulunun da yardımıyla yeni merkez kurulmuştur. TUBİTAK, ULAKBIM'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-USA bağlantısını sağlayan grubunda başlangıçta içinde olduğu bir konsorsiyum tarafından oluşturulmuştur (İnan, 2000, s. 68).

2.1.4 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 bir kavram değildir (Burkay, 2008, s. 2). Suçun; her toplumda oldukça farklı anlamları varsa da suç kavramına hukuki olarak bahsetmek gerekmektedir. Sözlük anlamında suç; "*toplum düzenini bozan, kanunlarca yasaklanan, hukuka aykırı davranışlardır*" şeklinde ifade edilmektedir (Yalçın, 1998: Aktaran, Dilber, 2014, s. 64) Başka bir tanımlamaya göre ise; *hukuk düzeninin cezai müeyyide altına aldığı insan davranışlarıdır* (Gallas, ..., s. 306).

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 olmayan olan diğerine göre suç olarak kabul gören bir davranış ortaya çıkmaktadır. Örnek vermek gerekirse teknolojinin gelişmesiyle birlikte bilgisayarlar kullanımının yaygınlaşmasıyla bilgisayar aracılığıyla suç işlemeyi getirmiş 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 (Bal, 2003: Aktaran, Burkay, 2008, s. 2).

Kanunların suç kabul ettiği cezai yaptırımlara bağladığı, hukuka aykırı eylem olarak nitelendirilen suç kavramı ve müeyyideleri 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 (Bal, 2003: Aktaran, Burkay, 2008, s. 3). Yani hukuki anlamda suçu ceza kuralı belirler. Eğer kural yoksa suç da yoktur. Yasada düzenlenmemiş olan suç ve ceza mevcut olmayacağı ceza hukukunun temel ilkelerinden biridir. Geniş anlamda suç kavramını tanımlayacak olursak, ceza tehdidi altında yasaların yapılmasını yasakladığı olumlu ve olumsuz eylemler olarak ifade edebiliriz.

2.1.5 Suçun Unsurları

Türk Ceza Kanunu'nun da suç teorisine göre maddi unsurlar, manevi unsurlar, hukuka aykırılık unsuru olmak üzere üçe ayrılmaktadır (Özgenç, 2006, s. 194).

2.1.5.1 Suçun Maddi Unsurları

Suçun meydana gelmesi için bir eylem/fiil bulunmalıdır. Bu eylem/fiil icrai veya ihmali olabilir. Bir suçtan bahsedilebilmesi için, yasanın tarifine uygun bir fiilin mevcut olması şartı, maddi unsuru da barındırmaktadır. Kanundaki suç tarifinde mutlak surette bir eyleme/fiile unsur olarak yer verilmektedir. Bu eylem/fiil, normal bir insan davranışı olmayıp, bizzat haksızlık ihtiva eden bir insan davranışıdır. Suçun maddi unsuru fiildir. Ceza hukukunda fiil denilince de eylem, sonuç ve eylemle sonuç arasındaki nedensellik bağı anlaşılmalıdır (Ergün, 2008, s. 4).

2.1.5.2 Suçun Manevi Unsurları

Suçun manevi unsuru ise kusurluluktur. Kusursuz suç olmaz. Kusurluluk taksir ve kasıt biçiminde ortaya çıkar. Kusur kişisel olduğu için ancak fertlerin sorumluluğu vardır. Manevi unsurda kastedilen, failin kusurlu bir biçimde hareket etmesidir. Manevi unsur, işlenen eylem ile insan arasındaki manevi bağı temsil etmektedir. Bu bağ kurulmadan, meydana gelen davranış fiil niteliğini barındırmaz ve bir suçun mevcudiyetinden bahsedilmez (Ergün, 2008, s. 5).

2.1.5.3 Hukuka Aykırılık Unsurları

Hukuka aykırılık, yasadaki tarife uygun bulunan ve işlenen davranışın, hukuk düzenince uygun bulunduğunun, mubah sayılmadığının bir ifadesidir. Bir eylemin suç olabilmesi için yasada belirtilmiş olması ve sonucunda bir ceza bulunması gereklidir. İşlenen eylem yasada belirtilen tanıma uygun olması gerekir (Ergün, 2008, s. 5).

2.1.6 Bilişim Suçu Kavramı

Bilişim suçları, 1960 tarihinden itibaren Amerika'da ortaya çıkmasının neticesi olarak Amerikan öğretisinde yaygın bir şekilde "bilgisayar suçları" (computer crimes) teriminin kullanıldığı, diğer devletlerin hukukçularınca da benimsenmiş olup, Amerika'da bilişim suçları yerine bilgisayara karşı suçlar, bilgisayar suçu, bilgisayar ilişkili suç yada bilgisayar yardımlı suç kavramlarının kullanıldığının görüldüğü ifade edilmektedir(Yenidünya ve Değirmenci, 2003, s. 30).

Bilişim suçları, devletlerin mevzuatlarında tanımlanmış bir suç şekli değildir (Ergün, 2008, s. 12). Bilişim teknolojilerinin kullanımı, yaygınlığı ve gelişmişliği ülkeden ülkeye değiştiğinden ve bilişim teknolojilerinin alanında sınır çizmek zor olduğundan haliyle bilişim suçu ile ilgili ortak tanımlama yapılamadığı görülmüştür (Akarslan, 2012, s. 33).

Ülkemizde de bu konuda bir kavram kargaşası mevcuttur. Bilgisayar suçu, internet suçu, siber suç, bilişim suç hukuku, 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 görülmektedir (Dülger, 2014, s. 69-70).

Yukarıda bahsettiğimiz kavramların bazılarına yönelik söz konusu alanda eleştiriler mevcuttur. Örneğin ilk olarak internet suçu kavramından bahsetmek gerekirse; internet 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 suçları işlenmesi mümkün olduğu belirtilmiştir. Bu nedenle bilişim suçlarının

işlenme ortamına göre farklı şekillerde isimlendirilmelerinin doğru olmadığı; örneğin kasten öldürme suçunu işlendiği ortama göre adam öldürme, bina içinde işlenirse bina suçu, otobanda işlenirse otoban suçu, açık alanda işlenirse açık alan suçu gibi adlandıramıyorsak, bilişim suçlarını da işlendikleri ağa göre isimlendirmek doğru olmadığı, olsa olsa internet aracılığı ile işlenen suçlar kavramının kullanılması daha uygun olduğu yönünde eleştiri getirilmiştir(Yenidünya ve Değirmenci, 2003, s. 31-32).

Siber suç kavramında ise aslında bilişim suçlarından söz edildiğini, bilişim suçlarının sadece bir bilişim sisteminde işlenen biçimi değil, bilişim sistem ağları aracılığıyla (özellikle internet) işlenen suçlar kastedildiğini, bilişim suçları, siber suçlar tanımına göre bir üst kelime olduğu ve siber suçları da ihtiva ettiği eleştirisi mevcuttur(Yenidünya ve Değirmenci, 2003, s. 32-33).

Ancak her ne kadar bilişim suçlarından, siber suç kavramına göre bir üst kavram olsa da, Avrupa Birliği ile müzakere sürecinde bulunulan, AB müktesebatında uyum adı altında yedi paket halinde yüzlerce yasada değişiklik yapıldığı, Türk Ceza Kanunu, Ceza Muhakemesi Kanunu, Medeni Kanun, Hukuk Usulü gibi 80 yıllık temel kanunların değiştirildiği, en önemlisi Avrupa Birliğine uyum sağlamak için Anayasa'nın değiştirildiği, bir dönemde Türkiye'nin üyesi olduğu Avrupa Konseyi'nin "Siber Suç" kavramını kullanması ve özellikle son zamanlarda yapılan çalışmalarda siber suç kavramının tercih sebebi olduğunu ifade edildiğini belirtmek gerekir (Ergün, Siber Suçların Cezalandırılması ve Türkiye'de Durum, 2008, s. 14). Bizde bu görüşe katılmaktayız. Ancak bilişim suçu kavramına yüklenen kültürel ve dönemsel anlam bütünlüğü de göz önüne alındığında geçmiş ve mevcut yasal düzenlemeler ışında Türk Ceza Kanunu'nda bilişim suçu kavramı hem öğreti de hem uygulamada görüş birliği halinde yerleşmiş olduğu ve tercih edildiği görülmekte, bu nedenle çalışmada ülkemizdeki durumu ifade ederken bilişim suçu kavramı, dünyadaki gelişmeleri ifade ederken siber suç kavramı kullanılacaktır.

Literatürde bilişim suçu kavramının tanımı incelendiğinde birçok tanım mevcuttur. Ancak bu tanımlamada bir uzlaşmaya varılamadığı çünkü bir tanımlama yapılırken ne tür bir eylemin bilişim suçu olarak değerlendirilip hangilerinin bu eylem dışında

bırakılacağı açıklığa kavuşmuş görünmemektedir (Dülger, 2014, s. 72). 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 (Dülger, 2014, s. 72). Yine de hukuk doktrinindeki tanımlardan birkaçına değinecek olursak; Aydın, *elektronik bilgi işlem kayıtlarına yasadışı yollarla erişilmesi veya bu katıların kanuni olmayan şekilde değiştirilmesi, silinmesi veya bu tür kayıtlara girilmesi veyahut bilgi tecavüzü için hazırlık yapılmasıdır* (Aydın, 1992, s. 27-28). Ergün; *Bilişim sistemleri ve bilişim teknolojileri kullanılarak bu sistemlerde ve bilişim ağlarında işlenen suçlardır* şeklinde tanımlama yapmıştır (Ergün, Siber Suçların Cezalandırılması ve Türkiye'de Durum, 2008, s. 16). 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 (Dülger, 2014, s. 73).

2.1.1 Bilişim Suçlarının Yapısı ve Özellikleri

Bilişim suçunun işlenebilmesi için gerekli olan bilişim ortamının temel unsurları üçe ayrılmaktadır. Bilişim suçunun unsurlarından birincisi, suçun 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 (Akarslan, 2012, s. 37).

Bilişim suçunun en temel özelliklerinden bahsetmek gerekirse bu suçun işlenmesi oldukça kolay bir o kadar da tespit edilmesi ve cezalandırılması açısından zor olmasıdır.

2.2 Siber Saldırı

2.2.1 Siber ve Siber Saldırı Kavramı

“Sibernetik” (cybernetics) sözcüğünün bir ön takısı olan “siber” kelimesinin, aynı zamanda sözcüğü kısaltmak amacıyla kullanıldığı görülmüştür (Çakmak ve Demir, 2009, s. 25). Cyber sözcüğünden dilimize siber olarak tercüme edilmiştir. Bunun en önemli sebebi, siber kelimesinin gelişim süreci içerisinde yüklenmiş olduğu dönemsel anlam ve kültürel bütünlüğüdür. Merriam-Wbster 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 (Helvacıoğlu, 2004, s. 277). 1948 yılında sibernetik ilk defa, Norbert Weiner adlı Amerikalı bir bilim insanı tarafından “makinelerde ve hayvanlarda iletişim ve hâkimiyet bilimi” manasında kullanılmıştır (Çakmak ve Demir, 2009). 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 (Helvacıoğlu, s. 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 (Çakmak ve Demir, 2009, s. 26).

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 (Çiftçi H. , 2013, s. 133).

2.2.2 Siber Saldırı Aşamaları

Siber saldırıların genellikle 6 aşamada gerçekleştiği ifade edilmektedir. 1. Sistemle ilgili bilgi toplama, 2. Sisteme Sızma, 3. Sıradan kullanıcı girişi, 4. Ayrıcalıklı kullanıcı girişi, 5. Sistem kaynaklarının ele geçirilmesi, 6. 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 güvenlik zaafları sayesinde, ayrıcalıklı kullanıcı yetkileri alınır. Dördüncü aşamada, sisteme ayrıcalıklı yetkileri elde ettikten sonra (root, superuser, administrator) kötü niyetli eylemleri gerçekleştireceği yetkilere sahip olur. 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 verilerde 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 (Çiftçi H. , 2013, s. 135-138).

2.2.3 Siber Saldırı Türleri

2.2.3.1 Kabloya Saplama Yapma (Wire Tapping)

Emniyete alınmamış iletişim ağ kablolarına, özel teçhizat kullanılarak fiziki anlamda saplama yapılması ve iletişim kurulmalıdır. Bu yöntem ile tüm trafiğin ele geçirilmesi

mümkündür. Telefon trafiği de bu yöntemle dinlenebilmektedir (Çiftçi H. , 2013, s. 139).

2.2.3.2 Tuzak Kapı (Backdoor)

Arka kapı olarak da denilen tuzak kapı yöntemi ile bir sisteme yüklenen bir yazılım sistemde kullanılan bir yazılımda bırakılan açıklık gibi çeşitli yönetimlerle, normal kimlik doğrulama mekanizmasını aşarak sisteme gizli bir şekilde erişmeyi sağlayan bir yöntemdir (Çiftçi H. , 2013, s. 140).

Arka kapılar özellikle ücretsiz yazılımlarda, paylaşımlarda veya işletim sistemlerinde bulunmaktadır. Ayrıca arka kapılar e posta ile de yayılabilir (Çakmak ve Demir, 2009, s. 73).

2.2.3.3 Hizmet Dışı Bırakma (Denial of Service, Dos)

Bilgisayarı veya bilgisayar sistemlerini hedef kullanıcı topluluğunun kullanmasını engellemek için yapılan saldırılardır. 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 (Çiftçi H. , 2013, s. 140).

2.2.3.4 Kriptografik Saldırılar

Şifrelenmiş mesaj veya verilerin şifresinin çözülmesi maksadıyla uygulanan saldırılardır. Temel prensibi güçlü bir algoritmanın güvenliği bütünüyle anahtarın içindedir; algoritmanın tasarım detaylarında değildir (Çiftçi H. , 2013, s. 141).

2.2.3.5 Zamanlama Saldırıları

Kriptografik saldırıların özel bir türüdür. Kriptografi de kripto algoritmasının çalışması için geçen sürenin analiz edilerek kripto sisteme nüfuz edilmesi amacıyla yan kanal saldırıcı yapılmasına "zamanlama saldırısı" adı verilmektedir. Bilgisayarda yapılan her işlem bir süre gerektirmektedir. Bu süre sisteme verilen girdiye bağlı olarak değişir. Hassas süre ölçümü yapılmak suretiyle kripto sistemin özelliklerine ve girdiye ulaşılması çalışılır (Çiftçi H. , 2013, s. 143).

2.2.3.6 İnternet Servis Saldırıları

Bilgisayarlar birbirleriyle iletişim ağı vasıtalıyla 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 (Çiftçi H. , 2013, s. 144).

2.2.3.7 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 (Çiftçi H. , 2013, s. 145).

2.2.3.8 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 (Çiftçi H. , 2013, s. 145).

2.2.3.9 Zararlı Yazılım Kullanımı

Bir bilişim sistemine saldırmanın yollarından biri de sisteme zararlı yazılım (virüs, solucan, Truva atı vb.) yüklemek veya yüklenmesini sağlamaktır. Zararlı yazılımlar farklı yöntemlerle hedef sisteme gönderilebilmektedir (Çiftçi H. , 2013, s. 146).

2.2.3.10 Oturum Çalma

İki bilgisayar arasındaki oturumun çeşitli yöntemlerle ele geçirilerek karşıdaki bilgisayara yetkisiz giriş yapma hakkının kazanılmasıdır. Bu saldırıda saldırgan kurban ve sunucu arasına da girip ikisi arasındaki tüm trafiği dinleyebilir (Çiftçi H. , 2013, s. 146).

2.2.3.11 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'ini oluşturduğu görülmektedir (Çiftçi H. , 2013, s. 147).

2.2.3.12 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 (Çiftçi H. , 2013, s. 147).

2.2.3.13 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 (Çiftçi H. , 2013, s. 147).

2.2.3.14 Ağ Tarama (Network Scanning)

İletişim ağından akan verilen gözlenmesi veya iletişim ağına bağlı donanımların zafiyetlerinin araştırılması eylemidir. Saldırı maksatlı olarak yapılabileceği gibi sistemin güvenlik ve performansını test etmek içinde yapılabilir (Çiftçi H. , 2013, s. 148).

2.2.3.15 Yerine Geçme (Masquerading)

Başka bir bilgisayarın yerine geçerek, yetkilerini kazanması eylemidir. Bu eylem, dahili bir ağdaki bilgisayarları bir bilgisayar üzerinden dış dünyaya bağlamak için kullanılabileceği gibi, bilgisayar sistemine saldırı yapmak içinde kullanılabilmektedir. Bu yöntemle kullanıcı hesabı ve parolası alınarak sistemdeki güvenlik açıkları kullanılarak ya da kimlik doğrulama işlemini yok ederek gerçekleştirilir (Çiftçi H. , 2013, s. 148, 149).

2.2.3.16 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 hırsızlama eylemidir. Bu yolla kullanıcıları kandırmak için popüler sosyal web siteleri, açık artırma siteleri, çevrim içi alışveriş siteleri, bankacılık 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 (Çiftçi H. , 2013, s. 149).

2.2.4 Siber Silahlar

Siber tehditler amacıyla kullanılan araçlara siber silahlar denilmektedir. En çok kullanılan siber silahlar şunlardır (Gümüş, 2008, s. 16-19):

- **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 üretilerek kullanıcıların şifre ve bilgilerini el 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 sunucu gibi 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:** Bilgisayarın verilerini bozulmasına, silinmesine ya da çalışmasını engelleyecek, yavaşlatacak ya da başka problemlere sebep olacak şekilde oluşturulan programlardır.

- **Worm:** Worm aslında bir solucandır ve virüslere benzerler. Bilgisayar korsanının açık bulduğunda bu zaafa odaklanıp kodları yayar ve makinelere kendi kendine kopyalar. Bunlarda verileri silebilir, şifreleri wormu yazana ulaştırabilir.

2.3 Siber Tehditler

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

2.3.1 Siber Suç

Siber suç kavramını yukarıda, bilişim suçu başlığı altında detaylıca açıkladığımızdan ayrıca burada karışıklığa yer vermemek için yeniden açıklamaya çalışmayacağız.[2]

2.3.1.1 Uluslararası Alanda Siber Suçlarının Sınıflandırılması

Siber suçların sınıflandırılmasında ortak bir ayırım yapılamamıştır. Birçok tasnifi mevcuttur. Strasbourg'daki 21 Kasım 2000 tarihinde Avrupa Topluluğunun 24 sayılı proje çalışmalarında siber suçları dört bölüm olarak tasnif edildiği görülmektedir. Bunlar; verilerin ve bilişim sistemlerinin kullanımına, bütünlüğüne ve güvenliğine

[2] Bknz. s, 31

ilişkin suçlar, manevi varlığa ve bununla alakalı haklara ait suçlar, bilişim suçları, muhteviyatı itibariyle suçlardır (Özkan, 2006, s. 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(Hekim ve Başıbüyük, 2013)

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 hardiskin de depolanmaması gereken bilgilerin saklanması ile suça karışılabilir (pornografik videolar, resimler vb.) (Özcan, 2004, s. 305-307).

Bir başka tasnife göre ise; kişilere karşı işlenen bilgisayar suçları, malvarlığına karşı işlenen bilgisayar suçları ve devlete karşı işlenen bilgisayar suçları şeklindedir (Balcıoğlu, 2014, s. 66-67).

2.3.1.2 Siber Suç Türleri

Özcan siber suç türlerini belirtirken İnterpol'ün hazırladığı "Interpol Computer Crime Manual", Birleşmiş Milletlerin "United Nations Manual on the Preventation and Control of Computer-Related Crime" ve Avustralya Polis Teşkilatı'nın "Minimum Provizyonsa for the Investigation of Compter Based Offences" kitapçıklarından yararlanarak suç tiplerini belirtmiştir (Aktaran; Özkan, 2006, s. 71-75):

1. Bilgisayar Sistemlerine ve Servislerine Yetkisiz Erişim

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

1.2. Yetkisiz Dinleme: Yetkisiz olarak bir ağ sistemine ya da bilgisayarın teknik olarak dinlenmesidir. Teknik dinleme, iletişimin izlenerek verilerin dolaylı olarak ya da doğrudan elde edilmesi ile bağlantılıdır.

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

2. Bilgisayar Sabotajı

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

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

3. Bilgisayar Yoluyla Dolandırıcılık: Klasik suçların bilgisayar ve iletişim teknolojileri kullanılarak kullanıcıyı maddi ve manevi zarara uğratacak şekilde zarar vermektir.

3.1. 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.

3.2. 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.

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

4. Bilgisayar Yoluyla Sahtecilik: Bilişim sistemlerini kullanarak sahte kâğıt para, senet, kredi kartı vb. materyaller üreterek ya da dijital belgeler üzerinde değişiklik yapmaktır.

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

5.1. Lisanssız Sözleşme İhlali

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

5.1.2. Lisans Haklarına Aykırı Çoğaltma: Yazılımın lisans haklarına aykırı davranarak kopyalanmasıdır.

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

5.2. Taklitçilik: Lisanslı yazılımın, yasalmış gibi izlenimi verilerek kopyalanması ve satılmasıdır.

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

6. 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.

7. Diğerleri

7.1. 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.

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

7.3. 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.

2.3.1.3 Siber Suçlar Geleneksel Suçlardan Ayıran Özellikler

Siber suçların, geleneksel suçlardan ayrıştığı nokta, bilişim teknolojilerinin araç olarak kullanılarak gerçekleştirilen suç biçimidir. Bilişim suçları, klasik suçlar ile benzerlik gösterdiği gibi ayrılıkları da mevcuttur (Taşçı ve Can, 2016, s. 231)**:**

a. Siber suçun sonucu başka bir devlette meydana görülebilmekte, 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 işleyenlere bakıldığında daha önce birbirlerini tanımayan devletlerde yaşayan kişilerin ortak iş yaparak suç işlemekte, hatta suçları iş birliği içerisinde yapanların aynı dili dahi kullanmadıkları görülmektedir.

e. Siber suçun işleme şekline alınan önlemler karşısında, daha gelişmiş yöntemler geliştiği görülmektedir. Bu yöntemlerin devam çeşitlenmesinin temel nedeni ise teknolojide yaşanan hızlı ilerlemeden kaynaklanmaktadır.

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 suçlarda çoğalmaktadır.

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

i. Siber suçu işleyenler arasındaki bağlantı genellikle ekonomik ya da geçici özellikte olup, klasik bir organize suç örgütünün hiyerarşisi ve yapısı bu örgütlerde görülmemektedir

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

k. Siber suçlalar her ne kadar çok büyük tahrifat yapsalar da suçu siber alanda/sanal işlediklerinden dolayı herhangi bir sorumluluk duymamaktadırlar (Dolu, 2011: 201). Yani normalde aynı mekânda bulunularak sözlü taciz gerçek yaşamda yapılması, çok ahlaki olmazken ve toplumda büyük bir çoğunluk bu eylemi yapmaya cesaret gösteremezken, internet ortamda yapılan sohbetlerde bireyler sözlü cinsel tacizi yüzünü gizleyerek çok rahatlıkla yapabilmektedirler.

2.3.2 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 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 (Sertoğlu, 1999).

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 ülke, 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 istemektedirler. Bununla birlikte her ülke, herhangi bir şekilde otoritelerini kötü biçimde etkiyebilecek ifadelerden uzak durmuşlardır. Neticesinde, bir ülke tarafından terörist olarak yaftalanan kişi ya da kişiler, diğer bir ülke tarafında da "özgürlük savaşçısı" olarak görülmektedir (Çitlioğlu, 2008: Aktaran, Yayla, 2014, s. 195). Bu nedenle terörün tanımında uzlaşma tam olarak sağlanamamaktadır.

Terör, sosyolojik açıdan, egemenlik ilişkisini yani 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. Otoriter yönetimlerde, bu faaliyetler yada saldırılar haklı bir tepki gibi algılanmasının yanında demokratik yönetimlerde kabul edilmeyişinin nedeni, demokratik yönetimlerdeki egemenlik ilişkinin, yani yönetim felsefesinin toplumun isteğine ve kabulüne bağlı olmasından dolayıdır. Ülkeler ve toplumlararası savaşlar, doğrudan egemenlik ilişkisini dönüştürmeye ve bu ilişkiye hakim olmaya yönelik olduklarından ve insanların da ölümüne neden olduklarından, tanım gereği terörist niteliği taşımaktadırlar (Kongar, 2002, s. 73, 74)

Yinede terörün tanımını yapmak gerekirse "şiddet kullanma ya da şiddet tehididi barındırananormal yollarla siyasal davranışları etkilemek üzere tasarlanmış sembolik bir fiildir" şeklinde ifade edilebilir (Thornton, 1964: Aktaran, Çakmak ve Demir, 2009, s. 36). 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) kurbanlarından çok daha geniş bir hedefe yönlenmiştir,
- Sivilleri de içine alan sıradan ve sembolik saldırıları içerir,
- Normal dışı yöntemler kullanılır,
- Özellikle, hükümetlerin ve toplulukların siyasi davranışlarını etkilemek için kullanılır (Wilkinson, 2006: Aktaran, Çakmak ve Demir, 2009, s. 36).

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 (Çakmak ve Demir, 2009, s. 37).

Terör örgütleri siber ortamda sıklıkla internetin sağladığı kolaylıklardan faydalanırlar. İnternet, teröristler için eşi bulunmaz avantajlar sunmaktadır. 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 ortam

sağlaması, medyanın ve anonimlik yoğun ilgisi ve bu avantajlar içinde sayılabilir. Bunların dışında internet özellikle hayli küçük grupların kendilerini duyurabilmesi için de önemli fonksiyon görür (Weimann, 2006: Aktaran, Çakmak ve Demir, 2009, s. 38). Bir kısım terör eylemleri siyasi olmakla birlikte, her siyasi eylemde terör niteliği taşımamaktadır. Bir saldırının terör olarak tanımlanabilmesi için "eylem, örgüt ve ideoloji" unsurlarının bir arada bulunması elzemdir. Belirtilen unsurlardan birinin eksik olması, o eylemin terörizm eylemi dışındaki sınıflamaya sokulması gerekmektedir. Örneğin bir politik nitelik taşımayan şiddet hareketleri örgütlü görünseler dahi, bu gruplar organize suç faaliyetleri olarak değerlendirilmesi gerekmektedir (Alkan, 2002: Aktaran, Özkan, 2006, s. 6).

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 (Çakmak ve Demir, 2009, s. 39). 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 (Özcan, 2004).

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 (Dening, 2012: Aktaran,Yayla, 2014, s. 195). 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 (Andress ve Winterfeld, 2011: aktaran;Yayla, 2014, s. 195).

Siber terörizm, sadece bilgisayar ve ilgili teknolojilerin bir araç olarak kullanılmasını değil, bir hedef olarak belirlenmesini 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 dayanan 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 (Çakmak ve Demir, 2009, s. 39,40). 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.

- 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 teröristin oturduğu yerden hedef aldığı sisteme sızarak çökertebilmektedir. 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 sistemine 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 seçilmektedirler. Ancak siber terörde böyle bir sınırlama bulunmamaktadır. Çünkü bilgisayar kullanımı çocuk yaştaki birisinin bile kolaylıkla öğrenebileceği, kullanabileceği bir teknolojidir. Bu nedenle terörde

çocuklar siber terörde araç olarak kullanılabilmektedir. Ortaokul ve liseli gençlerin devlet kurumlarına macera arayışı ile bir hevesle saldırmaktadırlar.

- Son olarak klasik terörde, teröristler silah ya da bomba gibi araçlarla yapılmakta iken siber terörde ise bilgisayar ve internet eylemlerini gerçekleştirmede yeterlidir (Özcan, 2004, s. 311-313)

Siber terörizm ile ilgili karşıt görüşlerde mevcuttur. Örneğin Joshua Green, "The Myth of Cyberterroism" başlığı taşıyan makalesinde bilgisayarlar tarafından öldürülen insanların olmadığını, devletlerin çok gizli ve güvenlik gerektiren bölgelerinde internet bağlantılarının bulunmadığı ifade ederek siber terörizm kavramının abartıldığı belirtmektedir (Çakmak ve Demir, 2009, s. 35).

Akman'a göre, siber terörizm; 2002 yılında yazılan "The Next War Zone" (Geleceğin Savaş Bölgesi) adlı kitapta ortaya atıldığını, 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" yönlendirerek başka ülkelere fırlatma gücüne sahip bulundukları için bu ülkelerin yakın bir gelecekte, bir "siber terörizm" yaratacakları ileri sürüldüğünü belirtmiştir.

Siber terör uzmanları şu an için çalıntı araçların, bomba yüklü kamyonların ve biyolojik silahların siber terörizmden daha büyük bir tehlike yarattığından bahsetmektedir. Siber terör tehdidi abartılmış olarak gözlemlense de ne yok sayılabilir ne de göremezlikten gelinebilir (Altınok ve Kaya, 2009, s. 160).

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 tesislerinin yerel ağ sistemlerini genel ağ sistemlerinden ayırmaları gösterilmektedir. Ancak bu durum gelecekte böyle bir saldırı olmayacağı anlamına da gelmemektedir (Çakmak ve Demir, 2009, s. 43).

2.3.3 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 saldırıları 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 edilemeyeceği, 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, Gürcistan ve Estonya'ya 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 Sözleşmesinin 51. maddesindeki "meşru müdafaa hakkı"nın kullanılabileceği düşünülmek ve savunulmaktadır (Yayla, 2014, s. 183, 184).

Bir başka neden ise, bilgi çağı öncesi düzenlenen Birleşmiş Milletler antlaşmasında gelişen teknoloji karşısında siber ortamdaki gelişmeleri 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.

Amerika Birleşik Devletleri Başkanı George W. Bush'un siber güvenlik danışmanı olarak çalışmış olan Richard Clarke göre, siber savaş, bir ülkenin, başka bir ülkenin bilgisayar sistemlerine ya da ağlarına zarar vermek veya kesinti yapmak üzere gerçekleştirilen sızma faaliyetleri şeklinde tanımlamıştır (Çiftçi H. , 2013, s. 5). 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 Sözlüğünde, siber 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 (Yayla, 2014, s. 190, 191). 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 (Çiftçi H. , 2013, s. 5).

Siber savaşın iki amacı mevcuttur. Birinci amacı, siber savaş yönteminin nasıl uygulanacağı ve gerginliğin artırılmasından nasıl kaçınılacağını içermektedir. İkinci amacı ise, siber savaşın asıl gayesidir. Rakip gördüğü tarafa boyun eğdirmeyi, verilerini çalmayı, sistemlerine sızarak belirli bir süre etkisiz bırakmayı veya komple bozmayı içermektedir (Çiftçi H. , 2013, s. 7).

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 hedeflemezler, sadece bilgisayar kullanıcısının ulaşmış olduğu verinin doğru olup olmadığını hedef almaktadırlar. Sistem problemsiz bir biçimde çalışmasına rağmen içerdiği veriler doğru olmaktan uzaktır. Bu saldırılar, özellikle resmi internet sitelerinin veya 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 (Yayla, 2014, s. 187, 188).

Siber savaş, genelde parasal kazanç hedeflenen suça ve politik amaçlı sembolik saldırılar içeren terörizmle temelde farklılık göstermektedir. Siber savaş, 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 (Çakmak ve Demir, 2009, s. 44, 45).

2.4 Siber Suçlar ve Siber Özgürlük: Gözetleme ve Mahremiyet

Devletin güvenlik güçlerinin siber suçları engelleme veya kontrol altına alma çabalarının yanında birtakım problemler ortaya çıkmaktadır. Buradaki temel problem güvenlik güçlerinin siber suçları önleme açısından vatandaşların internet gezintilerini gözetleme ve izleme faaliyetlerinde bulunmak zorundadırlar. Aynı zamanda internet kullanıcıların mahremiyet ve gizliliklerinin de aynı kişiler tarafından korunmak zorunda olduğu gerçeğidir (Suveren, 2017, s. 159).

Devletin güvenlik güçleri ve yargı sistemi, suçluları ve işlenen suçun delillerini toplamak zorunda olmaktadır. Suçlular da kolluk kuvvetleri tarafından yakalanmamak için kimliklerini gizlemekte ve anonimleşmektedirler. Gizlenen suçluların eylemlerinin engellenmeye çalışılması ile suçluların tespit edilmesi ve yakalanması için olabildiğinde eldeki imkanlardan yararlanmak zorundadırlar. Bu ise giderek artan ölçüde insanın faaliyetlerin gözetlenmesi ve izlenmesini gerektirmekte ve kaçınılmaz olarak çevrimiçi

iletişimin mahremiyet ve gizliliğin ihlal edilmesine neden olmaktadırlar (Suveren, 2017, s. 159). Suveren'e göre, günümüzde internet gözetimi ve gizlilik ile özgürlükler arasındaki denge üzerine yoğun bir mücadeleye şahit olduğumuzu söylemektedir.

2.5 Türk Ceza Kanunu'nda Düzenlenen Bilişim Suçlarının Sınıflandırılması

5237 sayılı Türk Ceza Kanunu'nda bilişim suçlarının düzenlenmesi açısından karma bir yöntem benimsenmiştir. Bilişim suçları, ikinci kitabın üçüncü kısmında, 10. bölümde bilişim alanında suçlar başlığı altında düzenlenmiştir. (Madde 243, 246) Ayrıca klasik suç tipleri içerisinde de bilişim yoluyla işlenmesi haline nitelikli hal olarak sayılmıştır (Keskin, 2007, s. 110).

Örnek vermek gerekirse hırsızlık ve dolandırıcılık suçu geleneksel suç tipleri arasında bulunmaktadır. Ancak hırsızlık ya da dolandırıcılığın bilişim sistemleri aracılığıyla gerçekleştirdiği takdirde nitelikli hal sayılarak ceza miktarı artmaktadır (Dülger, 2014, s. 338).

Mahmutoğlu, TCK'da bilişim suçlarını**,** yalnızca bilişim sistemleriyle işlenebilen suçlar, bilişim sisteminin kullanılması ile nitelikli hal kazanan suçlar, bilişim sisteminin suçta aracı olarak kullanıldığı suçlar, biçiminde ayırıma gitmiştir (Mahmutoğlu, 2013, s. 856).

2.6 Türk Ceza Kanunu'nda Düzenlenen Bilişim Suçları

TCK'da bilişim suçları açısından öteki devletlerden farklı bir yöntem kullanılmamış, ayrı bir yasal çalışma yapılmamış ancak temel ceza kanunu içerisinde yer verilmiştir. Türk Ceza Kanunu'nda bilişim suçlarına aşağıdaki maddelerde yer verilmiştir:

2.6.1 Bilişim Sistemine Girme (m.243)

Bilişim alanında suçlar alanında TCK'da ilk olarak, 243'üncü madde olan "bilişim sistemine girme" suçu düzenlenmiştir.

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

(2) Yukarıdaki fıkrada tanımlanan fiillerin bedeli karşılığı yararlanılabilen sistemler hakkında işlenmesi halinde, verilecek ceza yarı oranına kadar indirilir.
(3) Bu fiil nedeniyle sistemin içerdiği veriler yok olur veya değişirse, altı aydan iki yıla kadar hapis cezasına hükmolunur.
(4) ***(Ek: 24/3/2016-6698/30 Md.)*** *Bir bilişim sisteminin kendi içinde veya bilişim sistemleri arasında gerçekleşen veri nakillerini, sisteme girmeksizin teknik araçlarla hukuka aykırı olarak izleyen kişi, bir yıldan üç yıla kadar hapis cezası ile cezalandırılır*."[3]

Bu kanun maddesi kapsamında, bilişim sistemin bir bölümüne ya da tamamına kanun maddesine aykırı şekilde sızma ve bir süre sistemde kalmaya devam etme eylemini suç kapsamına almıştır (Dülger, 2014, s. 340). Bu kanunda genel kast ön plandadır. Yani suçun oluşması için girdiği bilişim sisteminde kişiye zarar verme ya da fayda sağlamak için içindeki bilgileri alma durumu bakımından suçun oluşumu açısından önemli değildir. Buradaki temel esas, yasaya aykırı girdiği sitemde kalmaya devam ettiği an suç tamamlanmış sayılmaktadır. Ancak sistemde kalmayı başaramadığı takdirde teşebbüs suçunu oluşturacağı değerlendirmektedir (Satılmış, 2006, s. 123).

2.6.2 Sistemi engelleme, bozma, verileri yok etme veya değiştirme (m. 244)

TCK'da 244'üncü maddesinde bilişim sistemine veya verilere zarar verme eylemleri ayrı suç tipleri olarak düzenlenmiştir.

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

[3] http://www.mevzuat.gov.tr/MevzuatMetin/1.5.5237.pdf, Erişim Tarihi, 05.04.2021

(3) Bu fiillerin bir banka veya kredi kurumuna ya da bir kamu kurum veya kuruluşuna ait bilişim sistemi üzerinde işlenmesi halinde, verilecek ceza yarı oranında artırılır.
(4) Yukarıdaki fıkralarda tanımlanan fiillerin işlenmesi suretiyle kişinin kendisinin veya başkasının yararına haksız bir çıkar sağlamasının başka bir suç oluşturmaması halinde, iki yıldan altı yıla kadar hapis ve beşbin güne kadar adlî para cezasına hükmolunur"[4]

Birinci fıkrada bilişim sistemlerinin çalışmasını engelleyen ya da çalışmasını bozan şeklindeki eylem, suç olarak tanımlanmıştır. İkinci fıkrada ise sisteme girildikten sonra bilgi ve belgeleri bozmak, yok etmek, değiştirmek, sisteme bir daha erişilmez kılmak, bilgi ve belgeleri alıp başka bir yere göndermek şeklindeki eylemler suç olarak tanımlanmıştı (Dülger, 2014, s. 409). Buradan anlaşılacağı üzere kanun sadece soyut kısmı olan verileri değil ayrıca somut anlamda donanımları ve aygıtları da yasal koruma altına alındığı görülmektedir (Akarslan, 2012, s. 48).

2.6.3 Banka veya kredi kartlarının kötüye kullanılması (m. 245)

"(1) Başkasına ait bir banka veya kredi kartını, her ne suretle olursa olsun ele geçiren veya elinde bulunduran kimse, kart sahibinin veya kartın kendisine verilmesi gereken kişinin rızası olmaksızın bunu kullanarak veya kullandırtarak kendisine veya başkasına yarar sağlarsa, üç yıldan altı yıla kadar hapis ve beşbin güne kadar adlî para cezası ile cezalandırılır.
(2) Başkalarına ait banka hesaplarıyla ilişkilendirilerek sahte banka veya kredi kartı üreten, satan, devreden, satın alan veya kabul eden kişi üç yıldan yedi yıla kadar hapis ve onbin güne kadar adlî para cezası ile cezalandırılır.
(3) Sahte oluşturulan veya üzerinde sahtecilik yapılan bir banka veya kredi kartını kullanmak suretiyle kendisine veya başkasına yarar sağlayan kişi, fiil daha ağır cezayı gerektiren başka bir suç oluşturmadığı takdirde, dört yıldan sekiz yıla kadar hapis ve beşbin güne kadar adlî para cezası ile cezalandırılır.

[4] http://www.mevzuat.gov.tr/MevzuatMetin/1.5.5237.pdf, Erişim Tarihi, 05.04.2021

(4) Birinci fıkrada yer alan suçun;

a) Haklarında ayrılık kararı verilmemiş eşlerden birinin,

b) Üstsoy veya altsoyunun veya bu derecede kayın hısımlarından birinin veya evlat edinen veya evlâtlığın,

c) Aynı konutta beraber yaşayan kardeşlerden birinin,

Zararına olarak işlenmesi hâlinde, ilgili akraba hakkında cezaya hükmolunmaz.

(5) ***(Ek: 6/12/2006 – 5560/11 Md.)*** *Birinci fıkra kapsamına giren fiillerle ilgili olarak bu Kanunun malvarlığına karşı suçlara ilişkin etkin pişmanlık hükümleri uygulanır*."[5]

Bu madde ile, banka veya kredi kartlarının yasaya aykırı bir şekilde kullanılması ile kart sahiplerini maddi ve manevi zarara uğramasını önlemek ile yasaya aykırı hareket edenleri cezalandırılması amaçlanmıştır(Satılmış, 2006, s. 125).

[5]http://www.mevzuat.gov.tr/MevzuatMetin/1.5.5237.pdf, Erişim Tarihi, 05.04.2021

BÖLÜM 3: HACKER KÜLTÜRÜ VE HACKTİVİZM

Hack, hacker ve hacktivizm ile ilgili bilgi kaynakları taraması yapıldığında ilgili literatürün üç kısma ayrıldığı görülmektedir. İlki, hackerlar hakkında olumsuz bir algı oluşturmayı amaçlayan ve geneli bilgisayar teknolojisine yakın olmayan bireylerin kaleminden çıkan ve tarafgirlikleri düşmanlıktan öteye gitmeyen metinlerden oluşmaktadır. İkincisi, Siber Ulusal Güvenlik Politikalar çerçevesinde özel veya kamu kurumlarının kriminal suç perspektifinden ve hukuksal boyutlarının ele alındığı metinlerden oluşmaktadır. Üçüncü olarak sıraladığımız kaynaklar ise hackerlığa yakınlıkları, irtibatları ya da bu konularda tecrübesi olan bireyler tarafından kaleme alınan metinler olduğu görülmektedir. Çalışmamızın ikinci bölümünde bahsedilen siber suç, siber savaş ve terör başlıkları altındaki yazılarımız bir ve ikinci tip kaynaklardan edinilen bilgilerden oluştuğundan ve bu çalışmadaki amacımız iki bakış açısı arasında bir konum almaya çalışmakta ve daha geniş perspektiften bütünsel bakış ve objektif olarak yansıtmak olduğundan bu bölümde sadece 3. tip olarak zikrettiğimiz kaynakları veri alınmıştır.

Konu ile ilgili bahsedilen kaynak metinleri incelediğimizde karşımıza genellikle hack, crack, hacker, cracker ve buna bağlı toplumsal hareketler bağlamında, aktivizim, hacktivizm vs. gibi kavramları önümüze çıkmaktadır. Günümüz dünyasından 40-50 yıl öncesine gittiğimizde aslında ilk olarak bilgisayar sistemlerine sızmanın bir tür hacking olarak nitelendirilmekteydi. Ancak zamanla gelişen teknoloji ile internete bağlanan bilgisayarların vazgeçilmez olması kötü niyetli bilgisayar kullanıcılarını da cezbetti. Bu gelişim, hacking diye nitelendirilen eylemi daha korkunç boyutlara taşıdı ve az önce yukarıda bahsettiğimiz kavramların türemesine ve anlam karmaşasına dönüşmesine neden olmuştur.

Günümüzde toplumsal algı açısından hacker kelimesine olumsuz anlamlar yüklenmektedir ve yine olumsuz bir çağrıştırma içermektedir. Ayrıca ülkemizde ve dünyada da resmi görüşün bu yönde olduğu söylenebilir. Peki hacker kavramının gerçekten de resmi görüşü yansıtan kişi veya topluluklardan mı oluşmakta yoksa kavramın bu hale gelmesinin altında başka sebepler mi vardır? Bunun daha iyi

kavranabilmesi için bu kavramların tarihsel süreç içinde ilk ortaya çıktıkları zamandan şimdiye kadar geçirmiş oldukları anlam değişiminin nasıl gerçekleştiği ve dışsal faktörlerin neler olduğu bilinmesi gerekmektedir.

Popüler algının ötesine geçildiğinde bambaşka bir gerçeklikle karşılaştığımızı söyleyebiliriz. Bu gerçeklik, hackerlerin azılı birer suçlu, menfaat ve para peşinde koşan ya da basit bir hareket, duruş olarak değil, yaşam tarzları, dünyaya bakışları ve temel etik kuralları olduğunu yani bir kültürü temsil ettiğini hatta sadece kültür olarak değil alt/karşı kültür olarak nitelendirildiğini görmekteyiz. Bir karşı kültür olarak ele almadan önce yukarıda anlam karmaşasına neden olan kavramları sırasıyla açıklamaya çalışacağız.

3.1 Hack Kültürü

3.1.1 Hack ve Hacker Kavramlarına Giriş

Hacker kelimesinin anlamı günümüze kadar değişerek gelmiştir. Hem iyi hem de kötü anlamları barındıran tanımları mevcuttur. Tanımlayan kişinin siyasi ve ideolojik görüşü, toplumsal konumu, bilişim sistemleri ve hackerlığa karşı bakış açısına göre bu tanım değişmektedir.

Hacker kavramının günümüzdeki tanımına değinmeden önce hack kelimesinin nereden geldiği ve bu kavrama atfedilen anlamın ne olduğu açıklamak gereklidir. Hack kavramı ilk olarak ABD'deki Massachusetts Institute of Technology Üniversitesinde, 1960'lı yıllarda bu üniversite bünyesinde bulunan öğrencilerinin kendi aralarında yapmış oldukları eşek şakalarına verdikleri isimdir. Bu akıllıca şakaları yapanlara da hacker denilmekteydi. Tabi bu hack ve hacker kavramları bilgisayar ile ilgili olmadan atfedilen anlamlardı.

Eriş, hack kavramının bilgisayarlarla alakalı kullanımı Tech Model Railroad adlı kulübün Digital Equipment Corporation adlı üreticinin geliştirmiş olduğu PDP-1 isimli bilgisayarla çalışılması sırasında, yerel demiryolu jargonun bilgisayarlara uygulanmasıyla ortaya çıktığını söylemektedir. Bu terimin ilk kez günümüzdeki

kullanıldığı anlamda, 20 Kasım 1963 yılında, MIT'deki öğrenci gazetesi Tech'de şu şekilde yayınlanmıştır (aktaran; Eriş, 2009, s. 65):

...Enstitü Telefon Sistemi yöneticisi Prof. Carlton Tucker"e göre, sözde "hackerlar" yüzünden birçok telefon hizmeti aksadı. Hackerlar, Harvard ve MIT arasındaki tüm hatların meşgul edilmesi ya da ücreti yerel radar istasyonuna yazdırarak uzak mesafeli telefon görüşmeleri yapmak gibi şeyleri başardılar. PDP-1 bilgisayarını telefon sistemine bağlayıp görüşme yapma tonunun bulana kadar arama yaptırmayı da içeren bir metodun kullanıldığı bulundu. Hacking yüzünden MIT telefonlarının çoğu kullanım dışıdır.

Hacker kavramı ise, İngilizce kökenli bir sözcük olup 1950'li yıllarında dünya literatürüne girmiştir. Türkçe karşılığı "*bilgisayar korsanı*" olan bu kelime Türk Dil Kurumu'nun Güncel Türkçe Sözlük 'ünde, *bilgisayar ve haberleşme teknolojileri konusundaki bilgisini gizli verilere ulaşmak, ağlar üzerinde yasal olmayan zarar verici işler yapmak için kullanan kişi* (https://sozluk.gov.tr/)olarak tanımlamıştır.

Raymond, hackerlığı (2008) "Teknik bilgiye sahip, problem çözmekten zevk alan ve sınırları aşan kişi'dir şeklinde tanımlamaktadır. Onlara üstat demektedir. Hackerlar aslında interneti kuran kişiler olduğunu, bu kişilerin ARPANET deneylerine ve ilk zaman paylaşımlı küçük bilgisayarlara kadar giden bir toplulukları ve paydaş bir kültürleri mevcut olduğunu, "üstat" yani hacker kavramını, bu kültürün mensupları tarafından üretildiğini söylemektedir (Raymond, 2008).

Hacker, cracker vb. kavramlar sıkça birbirleri ile karıştırılmakta olup aslında anlamları birbirinden farklıdır. Kendilerini üstat ("hacker") olarak tanımlayan ancak aslında üstat olmayan bir topluluk daha vardır. Bilgisayar sistemlerini altüst eden ve telefon sistemini gizlice kullanan bu grup çoğunluklu olarak genç erkeklerden oluşmaktadır. Gerçek üstatlar ise bu tür gruplara "korsan" ("cracker-kırıcı-") adlandırmasında bulunarak onlarla iletişime dahi geçmeyi istememektedirler. Gerçek üstatlar, korsan sıfatına sahip olanların genellikle sorumsuz, güvenilmez ve tembel olduklarını ve zeki olmadıklarını savunarak güvenlik sistemini kırmanın onları üstat yapamayacağını da belirtmektedirler. Birçok yazar ve gazeteci, "üstat" ("hacker") sözcüğünü, korsanları da("cracker") içine dahil edecek şekilde kullanmaktadırlar. Raymond'a göre hacker ile cracker arasındaki

temel farkın, üstatların bir şeyleri yaptıkları, korsanların ise bunları bozdukları şeklinde anlaşılmaktadır (Raymond, 2008).

Hackerlığın günümüze doğru olumlu yönden olumsuz bir yöne doğru anlam kayması olduğunu görmekteyiz. O halde hacker kavramı tarihsellik içerisinde nasıl böyle bir anlama evrilmiştir? Yine üçüncü bölümün başında ifade ettiğimiz gibi etik ilkelerin düzenlendiği, ilk zamanlardan itibaren manifestosu olan bir alt kültürün yalnızca "sivilceli ergenler", "korsanlar", "teröristler" ve "suçlular"a şeklinde tanımlamak problemli görünmektedir. Hackerların birçoğu elde etmiş oldukları ileri seviye teknoloji bilgi ve birikimlerini kullanarak bilişim çağına etki etme gücüne sahip olmaları sebebiyle günümüzün en önemli karşıt kültürlerden biri olarak değerlendirilmesi daha isabetli bir yaklaşım olabileceği değerlendirilmektedir (Ferligül Çakılcı, 2014).

3.1.2 Hacker Kültürün Ortaya Çıkışı ve Tarihsel Gelişimi

Hack kültürünün ortaya çıkışı 1960'lardan itibaren başlamakta olup 1990'lara kadar devam etmiştir. Walleij, hack kültürünün hippilerin, yippilerin, anarşistlerin, klasik sosyalistlerin, liberallerin ve en önemlisi genç insanların gayreti, bilgisayar programları, bilim adamlarının içinde olduğu bir ideoloji karışımından alt kültür yığınına evrilen bir hikaye olduğunu ifade etmiştir (aktaran; Eriş, 2009, s. 71).

Bu kültür ABD'deki Massachusetts Institute of Technology Üniversitesinde doğmuştur. Çünkü ilk bilgisayar ağları burada kurulmuştur. Burada kurulan bilgisayar ağları ile bilgisayar ile ilgilenen üniversite bünyesindeki kulüp öğrencilerine özgürlük tanınarak bağımsız çalışmalara izin verilmiş ve bir kültürün ve etiğin doğmasına neden olmuştur.

Hackerlığın bir hareketten veya duruştan ziyade neden bir kültürü temsil ettiğini Sabancı (2013) şöyle açıklamaktadır; hareket sadece bir mevzuyu esas alır ve o mevzu üzerinden çalışarak devam eder ve katıldığı toplumsal hareket onun hayatına etki etmez. Bir duruşu da temsil etmez; çünkü hayatında gerektirdiği zamanda belirli yerlerde bunu yansıtır. Çok az bir değişimden de söz edilebilir. Ancak kültür, hayatın hemen hemen her noktasında kendisini göstermektedir. Kültürü benimsemekle, onun bir parçası olarak kendisini görür ve kişi de bunları yaşamına tatbik eder. Birey yaşamının her noktasında

benimsediği kültüre göre eylemlerde bulunarak ve bu eylemleri de gizleme gereği hissetmez. Hackerlara bakıldığında, benimsenmiş temel etik ilkeleri, çağa bakışları ve hayat tarzlarıyla güçlü bir temele sahip olmaktadırlar. Bu temel aynı zamanda bir kültürün karşı kültürü olmasını da ifade etmektedir (Sabancı, 2013, s. 15-16).

Bu kültürün ortaya çıkışındaki yer ve zaman çok önem taşımaktadır. Hackerları anlayabilmek için açık akademi modeli olan ilk yuvalarından başlamak gereklidir. Bu model hackerların öğrenme, öğretme ve çalışma üzerine fikirlerin en büyük kaynaklarıdır. Sabancı açık akademik modelini "… araştırma sürecinin katkıda bulunmak isteyen herkese açık olduğu ve en başından itibaren ilgili veya bu konuda tutkulu olan herkesin katkı sunabileceği, test edebileceği ve elde ettiği sonuçlarla sürece müdahale edebileceği yöntemdir" şeklinde ifade etmektedir (Sabancı, 2013, s. 17).

MIT'in içerisinde bulunan Tech Model Railroad adlı kulübün rakip olarak gördükleri fakültelerde yaptıkları eşek şakalarını ifade etmek için hack, bunu yapanlara ise hacker kelimesinin kullanıldığını belirtmiştik. Tech Model Railroad adlı kulüp, üniversitedeki tek elektro-mekanik kumanda düzeneği ile yönetilen demiryolu bağlantılarına sahiptir. Kulüp bünyesinde elektronik araçlara merak duyan birçok öğrenciyi kendine çekmiştir. Bu öğrenciler düzenledikleri etkinliklerde demiryolu ağı üzerinde yapılan düzenlemelerin etkisi ve basit olması temelinden değerlendirilmiştir. Bu manzaranın başarılı ve beğenildiğini ifade eden hack kavramı ile kullanılmaya başlanmıştır (Akdeniz, 2013, s. 9).

Buna göre artık hack kavramı hem eşek şakalarını hem de beceri kabiliyetini gösterme gibi her iki anlamda da kullanılmaya başlanmıştır. MIT, kampüsündeki Tech Model Railroad Club üyelerinin bazıları kampüste bulunan bilgisayarlar ile uğraşmaya başlamıştır ve bu bilgisayarlar MIT içindeki yapay zekâ laboratuvarındaki (MIT Al Lab) mesaileri için emek edilmeye başlanmıştır. Böylelikle hack ve hacker kelimelerinin kulüp içerisindeki organizasyonlardan bilişim alanına doğru evrilmesine sebep olmuştur.

3.1.2.1 İlk Kuşak (1970-1980)

Micro bilgisayarların ortaya çıkışı ve ilk çıktıklarındaki yüksek rakamlara nazaran fiyatlarının oldukça düşmesi ile MIT kampüsündeki öğrencilerin bilgisayarları kullanmalarına izin verilmiştir.

MIT kampüsündeki mikro bilgisayarlarda çalışan programlar, delikli kâğıt şeritlerin bilgisayara takılması suretiyle şeritlerin okunması ve işlenmesiyle gerçekleştirilmekteydi. O dönemlerde yazılımlar yani programlar uzmanlar tarafından değil de kullanıcılar tarafından geliştiriliyordu. Bu öğrenciler bilgisayar odasında çekmece içindeki kodların bulunduğu bandı alarak kullanabilmekteydiler. Yine yeni kodlar yazıp başka öğrencilerin kullanması için çekmeceye koymaktaydılar. Ayrıca bu kodlarla ilgili birbirlerine öneride bulunmakta ve oluşturdukları kodlar üzerine tartışarak birbirlerinin yanlışlarını düzeltmekteydiler (Sabancı, 2013, s. 18).

Bu nedenle bilgisayarlar, yapılabilecek her türlü düzenleme ve geliştirme işini iyi yapıyor ve yerine getiriyorsa bu bir hacktir. Bunu yapan kişi de üyelerin saygısını kazanır ve hacker olarak nitelendirilir. Ancak grup içerisinde bir üye kendisini hacker olarak tanıtamamaktadır (Akdeniz, 2013, s. 10).

1970-1980 yılları arasında bilgisayar ile ilgili gelişmelerden biri bilgisayarın tek kullanıcısı olan ve tek görev yapabilen özelliği yerine çok kullanıcılı çok görevli işlemler yapılabilecek seviyeye doğru geliştirilmesidir. Bundan dolayı bilgisayarın kaynaklarını paylaşmaya çok kullanıcının aynı bilgisayar üzerinden yapılmaya başlanmıştır. Bu nedenle kullanıcılar birbirlerinin süreçlerine, yazdıkları programa erişebilmesi, karışabilmesi ve düzenlemesi mümkün hale gelmiştir. Bir MIT öğrencisinin çalışmasını sürdürdüğü terminal ekranında bir anda çıkan böceğin ortaya çıkması şaka yapıldığını göstermektedir. Bu şakayı yapan kişinin mesajı için şu şekildedir: “Kodların hatalı!”. Hacker bakış açısıyla gösterilen zararsız, eğlenceli ve yapan kişinin becerisini ve zekasını gösteren bu resimde diğer öğrenciler için bu tablo olumsuz algılanmış ve hack, hacker kavramları olumsuz bir anlama doğru evirilmiştir (Akdeniz, 2013, s. 11).

3.1.2.2 İkinci Kuşak (1980-1990)

1980 dönemi sonrasında ise hacker kültürü bir değişime uğradı. Teknolojinin gelişmesiyle birlikte bilgisayar her alana girmiş ve kişisel bilgisayarlar yaygınlaşmıştır. Bilgisayar ağları uluslararası boyuta ulaşmıştır. Bu nedenle artık hacker kültürü MIT üyelerinden oluşmuyordu. İnternet sayesinde birçok topluluklar yani sanal cemaatler oluşmuş, kişiler ve topluluklar birbirleri ile iletişim halinde olmuşlardır. Böylelikle bilgi daha fazla yayılmaya başlamıştır. Bir yandan da bu dönemdeki bilgisayar ağlarındaki zayıflıklarında farkına varılması ile birçok kişi tarafından istismar edilmiştir. Yani uzak sistemlere erişme imkânı ve bunu paylaşma imkânı doğmuştur. İkinci kuşak hackerlar, ilk kuşak hackerların etik değerlerini kendi içlerinde bulundurmakla birlikte başka değerleri de benimsemişlerdir. Yani uzak sistemlere erişimden, bunu paylaşmaktan zarar gelmez düşüncelerini barındırmaktadırlar.

Bununla birlikte sınırı kestirilemeyen bu yeni alanda devletlerde panik havası oluşturmuş ve kontrol altına almak için baskıcı tavır sergilemiştir. Bir yandan da şirketler interneti ve teknolojiyi metalaştırmaya çalışması ile devlet ve şirketler ilk kuşak hacker kültürü ile çatışma içine girmiştir.

Sonuç olarak; çok sayıda insanın destek verdiği geniş tabanlı alt kültür ortaya çıkmıştır. Fakat bu alt kültür bazı konularla ilgili önceki nesilden biraz farklı ögeler barındırmaktadır. Örneğin interneti yalnızca bir laboratuvar ya da cemaatçi söylemin bir mekânı olarak değil, marjinalliğin, karaborsanın ve suçun da mekânı olarak tanımlanmaktadır. Üstatların değerleri kabul edilse bile artık değişen bilişim dünyasında yeni, sert ve daha güçlü bir etik ilkelere ihtiyaç olduğu kanaati hakimdir. Bu sebeplerden ötürü yukarda bahsi geçen devletin otoriter tavrı ve ticarileşme nedeniyle de yaptıkları birçok eylem suç kapsamında değerlendirilmiş ve bu kültüre eklemlenmiştir (Eriş, 2009, s. 83).

3.1.2.3 Üçüncü Kuşak (1990 ve sonrası)

1990lı yıllardan sonra gelen ve üçüncü kuşak olarak anılan bu grup, özgür yazılım ve açık kaynak kod gibi hareketlerden etkilenmişlerdir. Bu etkilenmenin ardından

bilgisayar teknolojilerinin yaygınlaşması, UNIX işletim sisteminin başarısı ve ilk kuşak hack/ hacker kavramlarının halen varlığını sürdürmesinde yatmaktadır.

Ticari şirketlerin internet ve teknolojiyi metalaştırması ile geliştirdikleri bilgisayarlar ile beraberinde birçok sorunlar getirmiştir. Ayrıca bazı yazılımcıların üretmiş oldukları programlarının kodlarını gizlemeye başlamaları akabinde bu kodlara hackerlar tarafından ulaşmaları ya da bunlar üzerinde değişiklik yapmaları nedeniyle hackerların cezalandırma yollarına başvurmaları, hackerların tepkisini almıştır (Sabancı, 2013, s. 18).

Richard Stallman tarafından yaratmış olduğu GNU-GNU's Not Unix adlı özgür yazılım ve açık kaynak kodlu yazılım projesinin kendi bünyesinde hem sosyal hem teknik ve hem de ticari olarak ortaya koyduğu ilkeler üçüncü kuşak hacker ve hack kavramının sınırlarını çizmiştir (Akdeniz, 2013, s. 13).

Üçüncü kuşak hacker toplulukları bir süre sonra yaptıklarından para kazanabilecekleri ticari mekanizmaları kurmuştur. İlk kuşak etik değerlerini, pratikler ile birleştirip önceki etik değerlerini korumaya çalışan ve bunun yanında bir sonraki kuşağın da kendilerini takip edebilecekleri bir rol modeli de kurmuşlardır. İkinci kuşağın güvenlik konusundaki adımları ve test etmek ilkesiyle yapılan işlemler, ilk kuşak çerçevesinden bakan kişiler için, yapılan faaliyetlerin bir hack değil kırma (crack) işi olduğunu, üçüncü kuşağında ilk kuşağın etik değerlerinin geçerliliğini korumuştur (Akdeniz, 2013, s. 14).

3.1.3 Hacker Kültürünün Beslendiği Kaynaklar

Hofstadter'in kitabı olan *Gödel, Escher, Bach: an Eternal Golden Braid* 'in hackerların hayat görüşüne hizmet ettiği söylenmektedir. Birçok hackerın başucu kitabı olan bu eser, konunun uzmanları tarafından bir başyapıt olduğu değerlendirilmektedir. Kültürlerinin felsefi altyapısını Hofstadter'in eserinden çıkarsadıklarını belirtmektedir. Bu eserde var olan birçok konu, antik filozofların paradoksları benzerinde işlenmiş ve aralarında benzerlikler çizilmiştir (Eriş, 2009, s. 83).

Hackerlar, bilginin kısıtlanmasını asla kabul etmezler. Bu nedenle bilginin özgürlüğü için ellerinden geleni yapmışlardır. İnternet ise, bu bilgiye ulaşmada sınırsız özgürlükler tanımlamaktadır. İnternetin böyle bir özelliğinin mevcut olmasında iki önemli unsur etkendir. Birincisi hackerların bilginin özgürlüğe olan tutkularıdır. Bu tutkuları olmasaydı, belki de internet olmazdı veya bu kadar gelişemezdi. İkincisi ise Hakim Bey[6] ve onun teorisi olan *Geçici Otonom Bölge*dir. Hakim Bey, post-anarşizm temelinde isyana teşvik eden, iktidar karşısında gizliliği savunan bir muhalefet anlayışını savunmaktadır (Eriş, 2009, s. 103). Hakim Bey'in The Net& The Web kısmındaki düşünceleri ile WWW'e doğru giden yolda siber uzayda gerçekleşme imkânı olduğu fark edilmiştir. Ayrıca hackerlar, Hakim Bey'in şiirsel terörizm tezinden etkilenmiştir. Bu tez aslında bir yöntemi ifade etmektedir. Beklenilmeyen bir zamanda ve beklenmedik bir yola mesaj iletmek, şok yaratmak hep söylemek istenileni ulaştırmanın etkileyici bir yöntem olduğu düşüncesi savunulur (Sabancı, 2013, s. 20).

Hackerlar üzerinde Wiliam S. Burroughs'ta etkili olmuştur. Kaos aşığı ve Beat kuşağının dâhisi bir yazardır. Yaşarken daima dille arasını düzeltememiş, devamlı onunla savaş halinde olan birisi olmuştur. Dilin uzaylılarca insanoğluna gönderilmiş bir virüs olduğunu söyleyerek virüse hakim olmaya, hakim olamaz ise yok etmeye çalışmıştır. Dili kendisi için bir eğlence aracı olarak görmüş ama asla onunla tatmin olmamış; parçalara bölmeye, kafasına göre biçimini değiştirmeye veya yapılamayacak şeyleri yapmaya uğraşmıştır (Sabancı, 2013).

Hackerlar da kodları birer dil olarak görerek onun gibi davranmaya başlamıştır. Kodları olduğu gibi bırakmıyorlar. Onları bozup yeniden inşa ediyorlar. Ayrıca ne kadar açığı ve zayıf noktaları mevcut ise de onları bulmaya çalışıyorlar. Bu itibarla Burroughs'un dil ile kurduğu ilişkiden etkilenen ve onun izinden giden hackerların da kodlarla

[6]Peter Lambert Wilson, Hakim takma adıyla tanınan Amerikalı anarşist yazar. "bir yaşam edinin, yaşam tarzı değil" ilkesiyle geçici otonom bölgeler oluşturma fikriyle bir tür ontolojik anarşizmin savunucusu olmuştur

arasında kurdukları ilişki bilişim dünyasına çok katkı sağlamıştır. Birçok farklı dillerde yazılımlar geliştirilmiştir.

Ayrıca hacker kültürü ile cyberpunk kültürü arasında karşılıklı etkileşim söz konusu olmuştur. Onlar bilimkurgu hayranıdırlar. Hacker kültürü cyberpunk kültüründen etkilendiği gibi, cyberpunk kültürünüde beslemiştir.

Son olarak *Jargon File*den bahsetmemiz gerekmektedir. Bu kültürün ortak mirası olan Jargon File, hacker kültürünün maddi ürünlerini barındırmaktadır. Kültüre katılanların katkılarını maddi beklentisi olmayan editörlere göndermeleri ve onların da mantıklı, düzenlenmiş yeni sürümleriyle üretmesiyle gelişmiştir. Jargon File, hackerların kullandıkları argo kelimelerinden oluşmaktadır. Bu jargonda teknik ifadeler mevcut olsa da teknik bir sözlük olarak değerlendirilmemektedir. Buradan yola çıkarak Jargon File bir anlamda hackerların aralarında iletişim kurmak, teknik tartışmalar yapmak ve eğlenmek için kullandıkları dil şeklidir (Eriş, 2009, s. 74). Bu anlamda Jargon File hacker kültürü için ortak kültürel mirası ifade ettiği gibi, tarihsel bağlamda kuşakların bu kültürden beslenerek ilerlediği söylenebilir.

3.1.4 Hackerların Motivasyonu (Linus Yasası)

Burada hackerlar ile mücadele eden yorumcuların hackerların hacking eylemlerini neden yaptıklarına ilişkin değerlendirmeleri içermemektedir. Daha çok kendileri tarafından yazılmış metin ve dokümanlar dikkate alınmıştır.

“Hackarlığın dürtüsü nereden gelir?” diye sorar Linus Torvalds. Bunun için genel insan dürtüleri bağlamında açıklamaya çalışır ve adını Linus Yasası ile kavramlaştırır. Linus yasası der ki insanların tüm motivasyonları 3 kategori altında toplanır. Bunlar sırasıyla hayatta kalabilme, toplumsal hayat ve eğlencedir.

En alt kademede *hayatta kalma* dürtüsü mevcuttur. Bu dürtü, diğer iki dürtünün gerçekleşmesi için gerekli olmaktadır. Daha sonra *Toplumsal hayat* gelmektedir. Toplumsal yaşam ise, kabul görme, ait olma ve sevgi ihtiyacını bünyesine alır. İster psikolojik isterse de sosyolojik anlamda olsun, her bir birey onaylandığını hissettiği bir

topluluğa ait olmak istemektedir. Ancak sadece onaylanmak yetmeyebilir. Birey eylemleri vasıtasıyla kabul görmek de isteriz ve bunun için daha derin bir tecrübeye ihtiyaç duymaktadır. Diğer bir ifadeyle, insanlar diğerleriyle birlikte bir bizin parçası olma, bir topluluk içinde saygı duyulan bir kadın veya erkek olma ve bir başkasıyla birlikte özel bir ben olma tecrübesine ihtiyaç duymaktadır. En son mertebe *eğlence* dürtüsüdür. Eğlencede anlatılmak istenen kendi başına keyifli ilginç ve cazip olan bir şeyle motive olma durumunu yansıtır. Bazı insanlar sonsuza dek sıkılmaktansa ölmeyi tercih eder (Himanen, 2005, s. 61).

Linus Yasası, yukarıda açıklanan bu üç durumun bireyleri motive ettiği anlatımından çok, gelişimimizin hayatta kalabilmekten toplumsal yaşama ve buradan da eğlenceye giden tüm bu mesafeleri kat etme sürecini sürdürmekle alakalı olduğuna ilişkindir (Himanen, 2005, s. 16).

Hackerlarda asıl maksat hayatta kalmak değildir. Ellerinde bir bilgisayar var ise ilk endişeleri ne yiyecekleri veya nerde kalacakları ve hayatlarına nasıl devam edecekleri değildir. Hayatta kalmak motivasyonu devam ederken diğer iki dürtüleri saf dışı bırakacak türden baskınlığı söz konusu değildir.

Aslında hackerlar bilgisayarlarını hayatta kalmak için kullanmaktan, diğer iki basamağa atlamış olandır. Bilgisayarı toplumsal hayat için kullanmaktadırlar. Aynı zamanda bilgisayar onlar için eğlencedir. Yani hackerlar bilgisayar ile kodlarla yeni bir şey yaratarak hem eğlenirler hem de toplumsallaşmış olurlar. Birçok hackerın bir arada çalışması durumu temelde network oluşturma etkisi ortaya çıkar. Bu nedenle bundan daha ileri düzeyde bir motivasyonun olmadığına inanmaktadırlar (Himanen, 2005, s. 17).

Buradan da anlaşıldığı üzere hackerların kendi söylemleri üzerinde durulduğunda motivasyonlarının şu şekilde olduğu görülmektedir: entelektüel ilgi, bilginin olabildiğinde sınırlarını genişletme isteği, özgür bir biçimde bilgi transferi ve akışına yönelik bağlılık, hakim otoriteye, şirketlerin kontrollerine karşı direniş ve gizli verileri

korumakla memur olanların savsaklamalarını ve maharetsizliklerini göstererek bilgisayar güvenliğinin iyileştirilmesi olarak anılmaktadır.

3.1.5 Hacker Etiği

Steven Levy'nin "Bilgisayar Devriminin Kahramanları" adlı eserinde hacker kültürünün ortaya çıktığı MIT'deki Model Trenyolu Kulübün temelleri attığını ifade etmiş ve ardından genel kabul gören hacker etiği kodlarını sıralamaktadır (aktaran; Eriş, 2009, s. 80). Ayrıca Sabancı (2013) ve Akdeniz'in (2013) de yine hackerların etik değerlerini anlatmışlardır. Bu kaynakların hepsinde etik değerlerin aynı olduğu görülmüş ise de tüm hackerların bu sayılan etik değerlere uyduğu söylenemez. Temel olarak hacker etiği 6 madde halinde sıralanmıştır:

1. Bilgisayarlara, sistemlere ve donanıma erişim kısıtlanamaz. Şahıslar, bir sistemin veya bir teknolojinin nasıl işlediğini öğrenmekte özgürdüler.
2. Bilgi özgürdür ve öyle kalmalıdır.
3. Otoriteye asla güvenilmemelidir. Güç tek bir noktada toplanmamalıdır.
4. Hackerlar yaptıkları işlerle değerlendirilmelidir.
5. Bilgisayarlar yaşamı olumlu yönde geliştirir.
6. Bilgisayarlar aracılığı ile iyi ve güzel işler yapılmalıdır.

Hackerlar için bilgi ve bilgiyiye özgürce, sınırsızca erişim en değerli şeylerden biridir. Çünkü birşeyi her yönüyle bilebilmek ve yeniden birşeyler yaratmak için o bilgiye özgürce ulaşılmalı ve muhafazası sağlanmalıdır. Bilgi kimsenin tekelinde olmaması gereklidir. Bilginin sadece bir kesimde olması demek gücün onda bulunması demektir. Bu nedenle hackerlar bilginin özgür kalmasını savunmasından başka bu bilgininin korunmasına yönelik her türlü mücadeleyi sergilemektedirler.

Hackerlara göre devletlerin ve girişimcilerin toplumu kontrol edebilmek için bilginin özgürlüğünü kısıtlama arsuzu ve merakı engelleme çabası içindedir. Bu nedenle daima otoriteye karşı bir duruş sergilemişlerdir. Çünkü kendilerine karşı bir engel olarak görmektedirler.

Hackerlar, insanları cinsiyet, yaş, din, dil ve ırklara göre sınıflandırmamaktadır. Onlara göre kişileri görünüşlere göre değil , gösterdiği beceri ve zekası ile takdir edilmesi gereklidir. Çünkü başarının arka planında zeka, beceri ve yaratıcılık olduğuna inanmaktadırlar.

Bilgisayarların kötü ve zararlı olduğu tezini asla kabul etmezler. O fikri çürütmek için ellerinden geleni yaparlar. Ayrıca bilgisayarda yapılacak işin estetik boyutunu da gözardı etmezler. Zaten hackerların birbirlerinden etkilendikleri şeyde kodların arkasındaki estetiktir.

Ayrıca hackerlara göre dünya bilgisayarlar ile daha iyi bir yer haline getirilebilir. Bu nedenle yarattıkları kodlarla ve geliştirdikleri yazılımlarla insanların yaşamlarına etki ederek kolaylıklar için çalışmaktadırlar.

Hackerların etiğine farklı bir bakış açısı da Pekka Himanen'den gelmiştir. Hackerların düşünce, yaşam biçimleri , çalışma şekli ve eylemleriniMax Weber'in protestan çalışma ahlakına bir direniş olarak nitelendirir. Bu şekilde hacker etiği; çalışma etiği, para etiği ve network(netik) olarak sınıflandırmıştır (Himanen, 2005).

3.1.5.1 Çalışma Etiği

Weber, kapitalizmin ruhunun özünde dinden arındırılmış protestan çalışma etiğinin kendi kanunlarına göre işlemeye başlama halidir olduğunu ifade etmiştir. Himanen'e göre kapitalizmin protesten çalışma etiği halen günümüzde kuvvetli bir güç olarak hakimiyetini sürdürmektedir. Bu anlamda günümüz ağ toplumu, sanayi toplumundan pek çok açıdan ayrıldığıhalde klasik kapitalizimden kopuş anlamında anlaşılmaması gerektiği, sadece yeni bir tür kapitalizm olduğu ifade edilmiştir.

Himanen, Protestanlıkta çalışma insanın özü olarak ön plana çıktığını vurgulamış ve manastırlardan örnekler vererek açıklamıştır. Çalışmak bu hayatta en önemli şeydir ve eğer yaşadığımız dünyada doğru şekilde davranılmazsa sonraki yaşamda bile çalışmaya mahkum olunmaktadır. Bu tema ile protestan etiği, ideolojiyi çok güçlü bir biçimde kendisine uyarlayarak cennet ve cehennemi bile tersyüz etmiştir. Dünya yaşamında iş,

kendi içerisinde mutlak bir hedef olarak görüldüğünden dolayı rahipler, cenneti sadece vakit öldürülen bir yer olarak tahayyül etmekte zorlandı. Çok çalışmak bundan sebep, şeytani bir ceza olmaktan çıkarılmıştır. Ağ toplumunun da bu çalışmamerkezli yaklaşım biçimini sorgulamak bir yana halen hakim olmayı sürdürdüğünü söylemektedir (Himanen, 2005, s. 32-33).

Protestan çalışma etiğinde çalışma ve zaman arasında organik bir bağ mevcuttur. Benjamin Franklin'in "vakit nakittir" sözü protestan çalışma etiğinde yer bulmuştur. Bu etik anlayış aynı şekilde ağ topulumun da hakimiyetini sürdürür (Himanen, 2005, s. 37-38). Bu şekilde zaman parasal bir değere sahip olunca zamanın en iyi şekilde değerlendirilmesi gerektiği fikri iş yaşamında *optimizasyon* kavramını ön plana çıkarır ve bir zaman sonra optimizasyon yalnızca çalışma hayatında değil işin dışında kalan gündelik yaşam üzerinde de etkisi altına almaya başlar. Himanen, bu durumu pazarın cumalaştırılması adıyla kavramsallaştırmaktadır. Zamanın optimizasyonu tüm süreçlere yayılmıştır dolayısıyla anne ve babalar bile artık evlerinde çocuklarına karşı ilgi ve alaka için ayırdıklarını zamanlarını optimize etmekte ve boş vakit (leisure time) geçirmek yerine kaliteli vakit geçirmek olarak tanımlanan başı ve sonu kesin olarak bilinecek bir şekilde biçimlendirilmiştir (Eriş, 2009, s. 78).

Hacker'ın çalışma etiği ise, otoriteye karşı oluşuyla bireye her zaman saygı duymuştur. Bireyin değer ve özgürlüğünün "çalışmak" adına böylesine sınırlandırılışın ortasında insanlara, yaşamımızın şimdi ve burada olduğunu hatırlatmaktadır. Onlar için, çalışmak, sürekli bir biçimde devam eden ve içinde diğer tutkulara da yer olması gereken yaşamın sadece bir parçasıdır. Çalışma biçimlerinde köklü değişikliklere gitmek, sadece çalışanlara değil, insana da insan oldukları için saygı gösterme meselesidir. Dolayısıyla bu anlamda hackerlar "vakit nakittir" sözü yerine "bu benim hayatım" görüşünü benimsemektedirler.

3.1.5.2 Para Etiği

Protestan para etiğinde, "daha fazla para kazanmak" dürtüsü mevcuttur. Çalışma ve para kazanma hayatın en önemli amaçlarından biridir. Neden yaşıyorsun sorusunun

cevabıdır. Ancak modern dünyada bu iki dürtü biraz gelişerek ve güçlenerek değişime uğramıştır. Çalışma ve para protestan ahlakında(kapitalizm) hayatın gayesi iken, modern dünyada yani yeni ekonomide iş ve para arasındaki denge, "para kazanmak" dürtüsü birazdan daha ağır basarak en yüce değer olarak kabul edilmiş, çalışma dürtüsü ikinci plana atılmıştır. Artık çalışmak, para kazanmanın aracı haline gelmiştir.

Kapitalizm 'in mülkiyet fikri yine modern dünyada daha da güçlenerek bilgi alanında yayılmıştır. Artık şirketler ticari amaçlarını, ticari markalar, telif hakları, patentler, patent hakkı bildirimi olmayan sözleşme ve bilgiye farklı yollardan sahip olmaya çalışarak gerçekleştirmişlerdir. Bilgi öyle yoğun bir biçimde korunma altına alınmıştır ki hapishaneye benzer hale getirdiği izleniminden sıyrılamamıştır (Himanen, 2005, s. 59).

Modern dünyada toplumsallaşmanın aracı iş (çalışmak)tir. İnsanlar iş yerinde dedikodu yapabilir, hayat koşullarını tartışabilir ve aktüalite hakkında yorum yapabilir, âşık olabilir. Daha iyi bir iş çıkararak da kabul görebilir. Kişinin bu güdülerinin tatmin edebilmesi için çalışmaya ihtiyaç duymaktadır.

Hacker para etiğinde ise; hackerlar için toplumsallaşma ve eğlenceyi(tutku), para kazanmaktan daha önemli olduğunu düşünürler. Onlar için para kazanmak sadece hayatta kalma gibi temel dürtü seviyesinden ibarettir. Hackerların dünyasında toplumsallaşma modern dünyanın süreçlerinden farklı olarak ilerler. Boş zamanlarını başkalarına verdikleri kodları, yazılımları(paylaşma) geliştirmek için çaba sarf etme eylemlerinde kuvvetli toplumsal dürtüler vardır. Onlar için benzerlerinden kabul görmenin etkisiyle motive olurlar. Tutkularını (eğlenerek yarattıkları yazılımlar) paylaşan bir toplulukta görmek, paradan önemli tatmin hissi vermektedir. Bu tatmin para kazanmaktan daha önemlidir. Görüldüğü üzere Protestan etiğindeki yaşam motivasyonu; çalışmanın kendisi bir tutkuyu gerçekleştirmeyi hedeflerken, yani hem toplumsallaşmanın hem de eğlencenin amacı görülürken, hackerlar da ise tutku ile toplumsal değeri olan bir şey yaratma, paylaşma ve benzerlerinden kabul görme düşüncesi motivasyon kaynaklarını oluşturur. Bu nedenle hackerların birçoğu yazdıkları

yazılımların lisanslarını çıkarmak yerine (copyright) onları copyleft (bedava) olarak sunmaktadır.

Ayrıca üretmiş bulundukları ürünler konusunda da para kazanmanın ötesinde amaçlara sahip olan hackerlardan Stallman, GNU projesi ile ilgili olarak buradaki (free software) free kelimesinin ücretsiz yerine serbest olarak düşünülmesini istemektedir. Bu bağımsız ürün üzerinde bilgilenmek için en kolay ifadesiyle içine görebilme, değişiklik yapabilme, paylaşabilme ve dağıtabilme özgürlüğünü amaçlamaktadır (Eriş, 2009, s. 79).

3.1.5.3 Netik (Network Etiği)

Hackeların network etiğinde ön plana çıkan iki önemli unsur ön plana çıkmaktadır. Bunlar "Özgürlük ve Mahremiyet" kavramları. Eskiden insanların, çoğunlukla deneysel bir iletişim ortamı olması sebebiyle rahatlıkla paylaşım yapabildikleri ve kendileri bu yapabildikleri adına mahremiyetleri hususunda şüphelenmedikleri bir zamanda artık hem hakim otoritenin gözetim ve denetim anlayışı hem de ekonomi alanında internetin gün geçtikçe daha fazla ticarileştirmesi nedeniyle ortaya çıkan problemlere karşın 1990'lı yıllarda "Electronik Frontiers Foundation" kurulmuştur. Bu kuruluş bu konular hakkında çeşitli çalışmalar yapmakta olup bunun yanı sıra konferans ve eylemler düzenlemektedir. Ayrıca bu kurum dünyadaki tek örnek de değildir. Hollanda'da menşeili XS4ALL (acces for all) kurumu etik konularla ilgili olarak ismini pek çok yerde duyurmuştur. Sonuçta internet teknolojisi kısıtlamadan ziyade paylaşımı doğa olarak bünyesinde barındıran bir alandır. Onu üreten bilim insanları ve hackerlarında yaklaşımları bu eğilimdedir. Ancak gerek hükümetlerin kısıtlayıcı baskıları gerekse şirketlerin interneti bir paylaşma alanı yerine bir ekonomik pazar olarak görmeleri hackerların tepkilerini de beraberinde getirmiştir.

Devletin kısıtlayıcı baskısı, bu tarz bir zihniyete sahip olunca basın ve medyayı özellikle de radyo ve televizyon gibi hem geleneksel hem de merkezi olanları kontrol etme gayreti içindeydiler. Ayrıca internetin içeriği ile ilgili de denetim kurmaya çalışmaktaydılar ancak uygulamada internetin merkezsiz olmasından dolayı bunu

yapmakta oldukça zorlandılar. Bu sebeple internet, baskıcı toplumlarda özgür ve bireysel söylemler için önemli bir araç haline gelmiştir. Bilgi ve iletişim araçlarını inşa eden hackerlar da dünyanın çeşitli bölgelerindeki muhaliflere kullanım konusunda destek olmuşlardır (Himanen, 2005, s. 95).

3.1.6 Hacker Etiğinin Değeri

Himanen, hackerların yedi etik değerinin mevcut olduğunu ifade etmektedir. Fakat yedi değerin hepsine birden katılmamaktadır. Hackerların ilişkileri incelendiğinde yine de hepsinin söylenmesinde zorunluluk olduğunu söylemektedir (Himanen, 2005, s. 133).

Hackerlar için ilk esas etik değer, onu eyleme geçiren güdü ile bu güdü sonucu gerçekleştirdiği programla mutlu olan ve içinde enteresanlığı barındıran *tutkudur*. İkinci etik değer *özgürlüktür*. Hackerlar monotonlaşmış yaşam ve düzenlenmiş (optimize)zaman ve çalışma yerine, yaratıcılığı temel alarak tutkularına yer vererek yaşamlarını aktif bir sürece göre yönetirler. Üçüncü etik değer ise; kodlarını, programlarını paylaşarak, bu paylaşımları neticesinde toplumda kabul görmek istemektedirler. Bu durum kendileri için *toplumsal değer* ifade etmektedir. Aynı zamanda yazılımlarının diğerleriyle paylaşılmasını, kontrol edilmesini ve geliştirilmesini istemektedirler. Bu durum da dördüncü etik değer olan *açıklık* ile ifade edilmektedir. Beşinci etik değerleri *etkinliktir*; bireysel yaşamak ve faaliyetleri ile alakalı özgürlüklerini korumak için her türlü dayatmayı reddetmektedirler. Altıncı etik değer ise *duyarlıktır;* "başkalarına alaka göstermenin kendi içinde bir amaç olması ve network toplumunu, kendi mantığının kolaylıkla yol açtığı hayatta kalma zihniyetinden kurtarma arzusunu" ifade etmektedir. Yedinci etik değer ise *yaratıcılıktır*. Kişinin becerilerine hayal gücünü eklemleyerek kullanması ve daima kendisini geçmesi, insanoğluna değeri olan bir çalışmada bulunmasını ifade etmektedir (Himanen, 2005, s. 134,135).

Himanen, gerçek hacker bu değerleri benimsemekle olabileceğini, yedinci etik değeri olan yaratıcılığı başardığında "gerçek bir kahraman" olacağını ifade etmektedir (Himanen, 2005, s. 135)

3.1.7 Hacker Çeşitleri

Halk arasında veya haberlerde bilişim sistemine sızan, zarar veren, sistemin çalışmasına engel olan, web sitelerini hackleyen, politik olarak devlet kurumlarının sitelerine siber saldırı düzenleyen ve bilinçli/bilinçsiz onlara katılan tüm kişilere hacker olarak lanse edilse de aslında eylemlerini kim için yaptıklarına, bu eylemlerin amaçları ve araçları yani saldırı çeşitlerine göre birden çok hackerler türü olduğunu söyleyebiliriz. Çalışmamızda sayısal anlamda kesin olarak türlerini belirtmekten kaçınılmıştır. Çünkü bazı kaynaklarda hackerlığın çeşidi olarak belirtilmiş ise de bazı kaynaklarda hacker türü olarak ele alınmadığı görülmüştür. Biz ise taradığımız tüm kaynaklarda gördüğümüz tüm çeşitleri burada açıklamaya çalışacağız.

Hackerlığın genel anlamda 3 başlık altında sınıflandırıldığı görülmüştür. Bunlar; beyaz, kırmızı, siyah ve gri/siyah şapkalı hackerlardır. Çoğunlukla şapka renklerine göre niyetleri belli olan hackerlar, iyi ya da kötü huylu olarak değerlendirilmektedir. Beyaz rengi masumiyeti, siyah rengi kötülüğü ve gri rengi ise kesinliği belli olmayan niyetler olarak belirtilmektedir. Kırmızı renkli şapkalılar ise kendilerini diğer hackerlardan ayırmaktadır. Bunların dışında kalan hacker çeşitleri ise bu sayılan 3 sınıflandırmadan birine de dahil edilebilmektedir.

Beyaz şapkalı hackerlar, kötü niyetli hackerların, firmaların veya devlet kurumlarına ait bilişim sistemlerine sızmaya çalışmasını engellemeye çalışmaktadırlar. Bu nedenle bilişim sistemindeki temel açıkları bularak kötü niyetli hackerların sisteme sızmadan önce açığı kapatmaya çalıştıkları gibi açıkları raporlayarak bu tarz durumlardan nasıl kurtulabileceklerine yönelik ilgili kişilere yardımcı olmaya çalışmaktadırlar. Beyaz şapkalı hackerlara örnek olarak World Wide Web (www)'i kuran Tim Berners-Lee'yi, Linux'un mucidi olan Linus Torvalds'ı verebiliriz.

Siyah şapkalı hackerlar, şahısların, şirketlerin veya devlet kurumlarının bilgisayarlarına sızmak için açık arayarak bu açığı tespit ettikten sonra içerisine sızıp sistemin çalışmasını bozarak zarar veren, çalışmasını engelleyen ve içerisindeki gizli bilgileri alarak bu bilgileri kendi çıkarları doğrultusunda (şantaj, tehdit, para vb.)

kullanan kişilerdir. Bu kişilere örnek olarak verilebilecek kişilerden biri Kevin Paulsen'dir. Yarışma tertipleyen radyo istasyonunun telefon hattına girip, kendisini 102. arayan kişi olarak göstererek Porche araba kazanmıştır. Gary Mckinnon ise, ABD'nin askeri kuvvetleri ve NASA'nın sistemine sızmıştır.

Gri şapkalı hackerlar, mevcut koşullara göre siyah veya beyaz şapkalı hackerlara dönüşebilenlerdir. Elde ettikleri bilgi ve belgeleri pazarlayarak hayatını kazanan kimselerdir. Çıkarları doğrultusunda değişiklik gösterebilmektedirler. Bu sebeple dikkat edilmesi gereken hackerlardır.

Kırmızı şapkalı hacker olarak nitelendirilen bu grup beyaz veya siyah şapkalı hacker özelliği taşımamaktadırlar. Bu grup genellikle hactivizm eylemlerinde kendilerini göstermektedirler. Redhack grubu kendisini kırmızı şapkalı hacker olarak tanımladığı görülmektedir (Kara, 2013, s. 14).

Eriş (Eriş, 2009), hackerları üçe ayırmaktadır: üstat, korsan ve hacktivisttir. Bunlardan birincisi teknolojiden etkilenmiş "***üstat***" diye tanımlanan kişilerdir. Marx'ın yabancılaşmış işgücü kavramına göndermede bulunarak, üstatların da iyi bir ressam, marangoz gibi yabancılaşmış iş gücü olduğunu ifade etmektedir. İkinci grupta anılan hackerlar ise "**korsan**"lardır. Yani suçlular. İnternetin ticarileşmesi ve bilgisayarların özel bir gruptan çıkıp tüm kesimlerde yaygınlaşması ile devletlerin toplumu kontrol kaygısı güderek otoriteryan şekilde baskı altına almak istemesi, girişimcilerin interneti metalaştırmaya çalışmasıyla ile bu ortamdan faydalanan ve yeni düzene karşı çıkan kişilerin üstatların değerlerini kabul eden ancak yaptıkları suç kabul edilen ve davranışları suça yönelen kişilerden oluşmaktadır. Üçüncü grup "***hacktivist"***lerdir. Hacktivistler aslında aktivistlerdir. Haktivistler (aktivistler), siber alanda bilişim sistemlerini kullanarak, internetin muhalif bir tavrı internete taşıma alanı olduğunu keşfederek protestolarını bu alanda sergileyen kişilerdir. Üstatlardan farkları bilişim sistemlerini kullanma becerileri ve hayranlıkları daha azdır. Üstatlar ise bir sistemin kimin yaptığının önemi yoktur onu yapan zekâ onları büyülemiştir.

Rorgers ise, (aktaran, Gökdemir, Eylül 2013, s. 35), tüm hackerları aynı sınıflandırmada zikretmenin doğru olmadığını ifade ederek hackerları dörde ayırmaktadır:

1. **Eski okul hackerları:** 1960 tarihlerinde M.I.T. ve Stanford üniversitesinde eğitimini alan bilgisayar programcıları olarak bilinmektedir. O zamanlarda hack etmek bir beceri ve zekâ ürünü olarak görüldüğü için bu topluluğa dahil olan hackerlar sistemlerin kodlarını analiz etmekle ilgilenmektedir. Ancak ilginç bir biçimde işin suç boyutu onları pek ilgilendirmemektedir. Kötü niyetli değillerdir. Sadece internetin herkese açık, erişilebilir bir sistem olduğunu düşünmektedirler. Hacking eylemleri onlar için sadece sistemi anlama, çözme ve öğrenme amacını taşımaktadır. Ufuk Eriş'in "üstat" diye tabir edilen kişilere denk düşmektedir.
2. **Zeki çocuklar:** Medya ve basında hacker olarak adlandırılan bu isimler çoğunlukla bu gruba dahil edilmektedir. İnternette gerçekleştirdikleri hack eylemlerini aleni bir şekilde anlatıp övündükleri için kolluk kuvvetine yakalanmaktadırlar. En ünlüleri Mafyaboy'dur. Mafyaboy grubu 12 ile 30 yaş arasında olup erkeklerden oluşmaktadır. Okulu sevmeyen ve eğlenceyi bilgisayar sistemlerinde arayan bu gençler, internet sitelerine girip, bilişim sistemlerine zarar vermektedirler.
3. **Profesyonel hackerlar:** Bu grubun üyeleri kazançlarını sistem kırarak kazanırlar. Belli bir ücret karşılığında bilgisayar sistemlerine girip veri hırsızlığı yapan bu hackerların amacı çoğunlukla şirketlerin ve devletin sistemlerine sızmaktır. Bu grupta organize suç örgütlerine çalışan hackerlar da yer almaktadır.
4. **Virüs yazarları:** Kendilerini hackerlardan ayrı tutarak elit bir grupta görmektedirler. Yazdıkları kodları internette yaymaktadırlar. Bu kişiler hakkında detaylı bir araştırma yapılmamıştır.

Ayrıca hackerların yukarıda açıkladıklarımızdan farklı türleri olduğunu da görmekteyiz. Bunlar ile ilgili fazla araştırma yapılmadığından sınırlı tanımlama ve değerlendirmelere ulaşmaktayız. Bu nedenle tanımları kısa tutulmuştur. Ayrıca tanımlamaları birbirine çok benzer olup aralarında çok ufak farklılıklar vardır:

5. Cracker: Medyanın "hacker**"** kelimesini doğru kullanmadığından, hackerlar tarafından tarif ettikleri bilgisayar korsanlarını ifade etmek için 1985 yılında oluşturulan

bir terimdir. Bu kişiler bilişim sistemlerine sızarak zarar vermekten hoşlanmaktadırlar. Geneli genç erkek bireylerden oluşan bu grup kendilerine toplum içerisinde "hacker" demeyi sevmektedirler. Cracker kavramı, orta seviyede bir yeteneğe sahip ve etik sınırları olmayan kişileri tanımlamak için kullanılmaktadır. Ancak cracker kavramının net bir karşılığı olmamakla birlikte anlamı kişiden kişiye değişebilmektedir Cracker'lar sızdıkları sistemlerde izlerini silmeyi ve herhangi bir sisteme bağlanırken farklı yönlendirmeler ya da proxy sunucuları kullanmaktadırlar. Buradan da anlaşılacağı üzere, cracker'lar suç işlediklerinin farkındadır ve kimliklerini mutlak surette gizlemeye çalışmaktadırlar. Cracker'lar bir sisteme girdikten sonra kendilerine yarayabilecek her türlü veriyi alırlar ve imkan varsa o sisteme başka bir zamanda girebilmesini sağlayacak bir "rootkit" yerleştirmektedirler (Hacker Sırları, 2009, s. 6).

6. Script Kiddie: Bu bireyler çoğunlukla bilişim sistemlerine saldırarak, zarar vermeye ve elde etmiş oldukları verileri kötü amaçlarla kullanmaya çalışmaktadırlar. Özellikle internet sitelerinde rahatça ulaşılabilen çeşitli hazır yazılımları nasıl yapılacağını adım adım anlatan belgeleri okuyarak kullanmaktadırlar (Turak, 2014, s. 6).Script kiddie'ler ile cracker'lar arasında temel ve en belirgin fark, cracker'ların yaptıklarının arkasındaki teknolojiyi bir seviyeye kadar anlamaktadırlar. Oysaki script kiddie'ler bu tarz bilgilere sahip değildir. Ellerindeki cihazlar script kiddie'lerinkinden daha ileri düzeyde olmayabilir ancak cracker'lar bu cihazları kullanmayı ve nasıl çalıştıkları hususunda bilgiye sahiptirler. Cracker'ların saldırıları, script kiddie'ler kadar yankı uyandırmaz, çünkü cracker'lar sızdıkları sistemden izlerini silmeyi ve sisteme girerken çeşitli protokol yönlendirmeleri ve proxy sunucularını kullanmaktadırlar (Hacker Sırları, 2009, s. 6).

7. Lamer: Cracking, Hacking gibi mevzularda bilgisi olmadan ya da üstün körü anlamadan öğrendiği bilgilerle hacker gibi hareket etmeye çalışan kişilerdir. Lamer'lar, script kiddie'lerin bir alt versiyonu olarak ele alınabilir (Hacker Sırları, 2009).

8. Devlet Destekli Hacker: Devletlerin siber orduları içerisinde yer alan, devletin kritik alt yapılarını koruyan ve gerektiği taktirde ülkenin hedef ve çıkarları doğrultusunda diğer bilişim sistemlerine giren ya da engelleyen kişiler olmaktadır (Turak, 2014, s. 6).

9. Ajan Hacker: Şirketler tarafından rakip gördükleri şirketlerin gizli verilerini ve ticari sırlarını elde etmek için belirli ücret mukabilinde anlaştıkları kişilerdir (Turak, 2014).

10. Siber Teröristler: Siyasi açıdan kendi motivasyonlarını sağlayarak, bilişim sistemlerine yaptıkları saldırılar ile toplumlar içerisinde korku yaratmaya ve kaos ortamı oluşturma gayreti içinde olan kişilerdir (Turak, 2014).

11. Warez-d00d: Bilgisayar programlarının güvenliklerini kırarak internette ücretsiz bir şekilde paylaşan cracker gruplarıdır.

12. Samurai: Yasal cracking işleri için tutulan hackerlardır.

13. Phreaker: Kablo-TV, Telefon, smartcard, bankamatik gibi diğer sistemleri kıran kişilerdir.

14. Wannabee: Hacker, cracker gibi olmaya uğraşan ancak henüz öğrenme aşamasındaki kişilerdir.

3.1.8 Ünlü Hackerlar

3.1.8.1 Dennis Ritchie& Ken Thampson (dmr&ken)

Dennis MacAlistair Ritchie 1941, Newyork doğumludur. New Jersey'de büyümüştür. Harvard Üniversitesi Fizik bölümünü dereceyle bitirip, aynı üniversitede yüksek lisans yapmıştır. Üniversite yıllarında bilgisayara olan muazzam ilgisi nedeniyle MIT laboratuvarlarında vakit geçirmiştir. 1967 yılında Bell laboratuvarında Bilgisayar Bilimleri Araştırma Merkezine girmiştir. Burada bir süre sonra kader arkadaşı olan Ken Thompson ile tanışmıştır.

Ken Thompson 1943 yılında New Orleans doğumludur. Elektrik mühendisliği alanında lisans ve yüksek lisans yapmıştır. C programlama dilinin öncüsü niteliğindeki B programlama dilini yazmıştır. Ayrıca UTF-8 karakter sınıflandırılmasını da Thompson'a borçluyuz.

Bel Laboratuvarlarında Ritchie ve Thompson ikilisinin önderliğinde, çok görevli ve çok kullanıcılı bir işletim sistemi olan UNIX'i geliştirmişlerdir. 1973'te IBM organizeli İşletim Sistemleri sempozyumunda, UNIX işletim sistemi tüm bilişim camiasına

duyurulmuştur. Bu başarılarından ötürü birçok ödüle layık görülmüşlerdir (Hamza, 2011, s. 14-16).

3.1.8.2 Richard Stallman (RMS)

Richard Matthew Stallman, 1953 Newyork doğumludur. Sistem uzmanı ve yazılım geliştiricisidir. 1971'den beri MIT'in yapay zeka laboratuvarlarında (AI) çalışmış olup, GNU[7] projesini hayata geçirmek için AI laboratuvarlarından ayrılmış ve çalışmalara başlamıştır. GNU projesini var eden, hayata geçiren liderdir veya babasıdır. GNU Emaxs Editörü, GNU Compiler Collection, GNU Binary Utilities, GDB Hata Bulucusu, Gmake program düzenleyicisi ve daha birçok yazılım Stallman'in üründür.

Richard Stallman, açık kaynak kod yazılıma verdiği önemi aynı zamanda emek verilerek üretilen yazılımların lisans altına alınması için GPL (GNU General Public Licence) projesinin lisans altyapısını piyasaya sürmüştür. Bu şekilde hem özgür yazılım açısından hem kullanıcılar açısından hem de yazılımcılar açısında en ideal ortamı sağlamıştır. Şu an kullandığımız teknolojiyi ona borçluyuz. Free Software Foundation tarafından yaygınlaştırılan GPL, internetin omurgası olan TCP/IP gibi Internet protokol yazılımlarını ticari tekelleşmeden kurtarıp kullanıcılara "özgür yazılım" sloganıyla ulaştırılmasında büyük etken olmuştur (Hamza, 2011, s. 17-18).

3.1.8.3 Kevin Mitnick (Condor)

Kevin Mitnick birçok otorite tarafından dünyanın en ünlü hacker'ı olarak kabul edilmektedir. ABD Adalet Bakanlığı kendisini ABD tarihinin en çok aranan bilişim suçlusu olarak tanımlamaktadır. Mitnick'in yaşantısı Freedom Downtime ve Takedown adlı iki filme konu olmuştur. Mitnick'in eylemleri arasında bilgisayar sistemlerine girme, kurumsal sırları çalma, telefon ağlarını karıştırma ve ulusal güvenlik uyarı

[7] GNU açık kaynak kod işledim sistemidir ve özgür yazılımıdır. UNIX'e benzerliği olmasına karşın, çekirdeğinde UNIX'e ait kod barındırmamaktadır.

sistemine girme vb. suçlar yer alır. Önemli bir astrofizikçi olan Tsutomu Shimomura'nın bilgisayarına girmesi sonucunda yakayı ele vermiş ve beş yıl hapis yatmış ve cezası 2000 tarihinde bitmiştir. Ayrıca, bilgisayarlara yaklaşma yasağı 2003 tarihinde bitmiştir. Günümüzde, beyaz şapkalı bir bilgisayar hackeri olarak güvenlik danışmanlığı yapmaktadır. Yine dünya çapında kongrelere katılmaktadır (Hacker Sırları, 2009, s. 8).

3.1.8.4 John Draper (Captain Crunch)

1944 doğumlu olan John Draper Phreaker'ların atası olarak bilinmektedir ayrıca telefon sistemlerini ilk kıran kişidir. John T. Drapler'ı, bugünlere taşıyan görme engelli bir arkadaşı olan Joybubles takma isimli Joe Engressiadır. 7yaşında iken çıkarmış olduğu ıslık sesiyle, telefon sinyallerini taklit ederek ücretsiz görüşme yapabileceğini keşfetmiştir. Sonraki zamanlarda ise Cap'ın Crunch mısır gevreği ambalajından çıkan bir oyuncak düdüğün, 2600 Hertz'lik sinyale eşdeğer olduğunu görmüştür. Bu ayrıca AT&T'nin uzak mesafe iletişiminde kullandığı ton sesidir. Bu bilgiyi John Drape ile paylaşmış ve J. Draper bundan ilham alarak Blue Box'ı geliştirmiştir. Geliştirilen Blue Box'lar, telefon servislerinin görüşme konsollarını taklit ederek çalışmakta ve bu sebeple uzun mesafe telefon aramalarını ücretsiz hale getirmiştir.

Apple I olan ilk el yapımı bilgisayar için gerekli sözcükler, John T. Draper tarafından ilk el yapımı bilgisayar olan Apple I için gerekli kelime işlemeci yazmıştır. 1980'li yıllarda IBM, yeni bilgisayarları tüm ülkelere yayılırken, kelime işlemci programlar için Draper'a teklif götürür. Draper'da Easy Writer adını verdiği kelime işlemci programlar için IBM ile anlaşmıştır.

Ayrıca J. Draper, Captain Crunch olarak bilinmektedir. Ayrıca o zamanın en ünlü gruplarından Homebrew Bilgisayar Kulübü üyesinden olmuştur. (Hamza, 2011, s. 22-23).

3.1.8.5 Peiter Zatko (Mudge)

Peiter C. Zatko 1970 doğumlu olup, Mudge kod adıyla tanınmıştır. Berklee okulundan mezun olmuştur. Buffer Overflow adlı güvenlik açığını ilk araştıranlardan biridir. Bu araştırmalarla ilgili makaleler yayınlamış ve UNIX işletim sistemi güvenliği için birçok öneri ve tavsiyelerde bulunmuştur. Ancak Mudge'nin ünlü olmasında en önemli etken NT şifre denetleme aracı olarak tanınanL0pht-Crack'tir. Ayrıca, AntiSniff ve L0pht watch gibi programlarda kendisine aittir.

Mudge, bu kadar hacker grubu ve hackerlar arasında devlet ve şirketlerle arası iyi olan tek kişidir. Talep ve randevu doğrultusunda resmi kişilerle görüşmekte, DEFCON gibi bir hacker organizasyonuna konuşmacı olarak katılmakta bunun yanında Usenix gibi akademik konferanslar da yer edinmekteydi. Ayrıca kendisi cDc üyesidir. (Hamza, 2011, s. 24)Mudge, 2010 yılında DARPA'da siber güvenlik araştırmalarını denetledi. 2013 yılında Mudge, İleri Teknoloji ve Projeler bölümünde Google için çalışmaya başlamıştır.

3.1.8.6 Robert Moris

Morris, 1965 doğumlu bir Amerikandır. Babası Amerikan Ulusal Güvenlik (NSA) bölümüne bağlı Bilgisayar Güvenliği Merkezi'nde çalışmaktadır. Morris, internette yayılan ilk bilgisayar solucanı (worm) olarak bilinen Morris solucanı'nın yaratıcısıdır. Bu suçun neticesinde 1986 Bilgisayar Dolandırıcılığı ve Suistimali Yasasından hüküm giyen il kişi olmuştur. Morris, Solucanın kodlarını Cornell Üniversitesi'nde öğrenciyken yazmıştır. Amacının internetin ne kadar büyük olduğunu görmek olduğunu iddia etmektir. Ancak solucan Morris'in beklentisinin dışına çıkarak kendini aşırı biçimde yaymış ve ulaştığı bilgisayarları yavaşlatmaya başlamıştır. Solucanın yaklaşık 60,000 bilgisayara bulaştığı söylenmektedir (Hacker Sırları, 2009, s. 12). Morris günümüzde MIT Bilgisayar Bilimleri ve Yapay Zekâ Laboratuvarında öğretim görevlisi olarak çalışmaktadır.2019 yılında Ulusal Mühendislik Akademisi'ne seçilmiştir.

3.1.8.7 Mark Abene (Phiber Optik)

Masters of Deception' isimli hacker grubunun kurucu üyelerindendir. 'Phiber Optical' kod adını kullanarak ABD'de on binlerce genci telefon sistemlerinin çalışma özelliklerini araştırmaya teşvik etmiştir. Amerikan Federal Mahkemesi, ibret olması için Mark Abene'yi 1 yıl süre ile mahkumiyet hükmü almıştır. Daha sonralarda ise New York adlı Magazin dergisi tarafından "New York'un en zeki 100 kişisinden biri" olarak gösterilmiştir.[8]

Phiber, hep yeraltı dünyasında kalmadı. Az önce belirttiğim gibi Newyork Times, Washington Post, Wall Street Journal vs. gibi birçok büyük gazete ve dergilerle röportajlar yaptı, güvenlik konferanslarına konuşmacı olarak katılmıştır. American Express, Sun Microsysstems, IBM ve İsviçre bankası gibi yerlerde güvenliğin sağlanması için görev aldı (Hamza, 2011, s. 27). Silikon vadisinde hayatını devam etmektedir.

3.1.8.8 Gordon Lyon (Fyodor)

Fyodor kod adını kullanmakta olan Gordon Lyon güvenlik camiasında tanınan ve önem verilen bir isimdir. Ağ güvenliği konusunda alanında otorite sahibidir. En popüler yazılımlardan en ünlü olanı Nmap Security Scanner Lyon ürünüdür. Bu ürün ağ haritası çıkarmak taranan bilgisayarın işletim sistemini ve portların durumunu öğrenmek için kullanılmıştır.

Güvenlik üzerine birçok kitabı olup aynı zamanda Honeynet Projesi'nin de kurucularındandır. Honeynet, 1999 yılında hiçbir kâr amacı gütmeksizin, internet güvenliği alanında faaliyet yürütmek amacıyla kurulan bir organizasyondur. Kendisi aynı zamanda Computer Professsionals for Security Responsibilitiy organizasyonun da başkanlığını yürütmüştür. (Hamza, 2011, s. 28)

---

[8] https://www.hurriyet.com.tr/gundem/hacker-romantizmi-23613096, Erişim Tarihi, 15.03.2021

3.1.8.9 Kevin Poulsen

Dark Dante kod adıyla tanınan Poulsen'in uzmanlık alanı telefonlardır. KISS-FM adlı radyo istasyonunun telefon hatlarını hackleyerek bir Porche ve çeşitli hediyeler kazanmasıyla ün kazanmıştır. Kendisi bilgisayar suçlarının Hannibal Lecter'i olarak anılmaktadır. Federal bir soruşturma veri tabanını hackledikten sonra yetkililer tarafından aranmaya başlanmıştır. Aranması sırasında federal bilgisayarlara girip bilgi çalarak yetkililerin tepesini daha da attırmıştır. Kevin'in fotoğrafı Unsolved Mysteries adlı bir televizyon programında yayınlandıktan sonra kanlın telefon hatları kilitlenmiş ve sonunda Poulsen bir süpermarkette yakalanarak beş yıl hapis yatmıştır. Poulsen günümüzde gazeteci olarak çalışmaktadır (Hacker Sırları, 2009, s. 10).

3.1.9 Ünlü Hacker Grupları

Öncelikle belirtmemiz gerekir ki bu başlık altında zikredilecek gruplar kimilerine göre hacktivist gruplara, kimilerine göre ise terör örgütü kapsamına sokulmaktadır.

Son zamanlarda tüm ülkeleri, toplumları ciddi ölçüde ilgilendiren hacker gruplarının hactivist amaçlı toplumsal hareketleri veya siber eylemleri, bireysel veya gruplar halinde çalışmalar göstermeye başlamışlardır. Bu faaliyetlerin amacı artık, hackerlar bireysel çıkarlarından ziyade kamu yararını düşünerek faaliyette bulunduklarını savunarak, hacker grupları oluşturmaktadırlar. Ancak bunun yanında ülkenin güvenliği ve bütünlüğü açısından tehlike oluşturan tehdit unsuru olarak da değerlendirilebilmektedir.

3.1.9.1 Anonymous

Anonymous 2003 yılında 4chan forum sitesinde yayılmaya başlamıştır. Metin yerine imgeleri kullanarak bir tür online tahtaya ileti bırakma sistemi olan "Imageboard" mantığının İngilizceye uyarlanmış hali ile anarşist ve aktivist ruhlu kişiler forumda kendi alt kültürünü kurmuşlardır (Uçkan, 2013, s. 63).

Faaliyetlerini, kendilerini anonim olarak kimliklerini gizleyerek yapmaktadırlar. Grup manifestosunda, netin özgür ve kısıtlamasız bir alan olması için çabaladıklarını ancak

son zamanlarda devletlerin internetteki serbestlikleri sınırlamak için yoğun uğraşlar verdiklerini belirtmişlerdir (Gökdemir, Eylül 2013, s. 177).

2008 yılından sonra grubun politik eylemleri artmıştır. İlk kurbanları ünlü ABD'li film oyuncusu Tom Cruise ve üyesi olduğu Scientology Tarikatı olmuştur. Cruise'un tarikatla ilgili bir videosu internette paylaşılır ve tarikat, videonun lisans hakkının kendisine ait olduğunu öne sürerek video içerik sağlayıcı olan YouTube platformundan kaldırılmasını talep etmiştir. Ancak Anonymous grubu böyle bir durumu ifade özgürlüğüne bir taarruz olarak değerlendirmiş ve tarikata ait internet sitelerine saldırı düzenlemiştir. Anonymous'un herkesçe bilinen mottosuda bu zamanda şu cümlelerle ortaya çıkmaktadır: "Biz Anonim'iz, Biz Lejyonuz. Bağışlamayız. Unutmayız. Bizi bekleyin" (Uçkan, 2013, s. 64).

Anonymous ismini ilk defa *Sony* saldırısı ile duyurmuştur. Amerika askeri ordusuna çalışan Lockheed Mart'e ait şirketin enformasyon ağına siber saldırıda bulunmuştur. 2011 yılında İrlanda seçimlerinde partinin internet sitesine sızarak, siteye mesaj bırakmıştır. Arap Baharı olaylarında, Tunus ülkesinde yaşanan devrimde Tunus'lu hackerlarla ortak saldırı düzenleyerek hükümete ait 8 web sitesini çökertmiştir. İlk sansasyonel saldırısını ise Wikileaks ve Bradley Manning olayının patlak vermesinden sonra hükümetin Wikileaks'ten dokümanları yayınlamasını durdurmasını istemiştir. Ancak dokümanları yayınlamayı sürdürmüştür. Anonymous, Wikileaks ile iş yapmak istemeyen ve köşeye sıkıştırmaya çalışan Paypal, Mastercard ve Visa'ya karşı savaş açmış ve 2010 yılı, aralık ayının 8. gününde Mastercard ve Visa'nın web sitelerine saldırı düzenlemiş ve çökertmiştir (Kara, 2013, s. 19).

Anonymous, bazı çevreler tarafından aslında bir örgüt veya grup olmadığı, bir fikir olduğunu belirtmişlerdir. Bir lideri veya hiyerarşisi mevcut değildir. Merkezi istihbaratı yoktur. Bir tür "franchise" olarak düşünülebilir. Bir fikrin paydaşları, kimliklerini ortaya çıkarmadan, açık bir sistem içerisine, benzer düşüncelere sahip diğer kişilerle bir araya gelip geçici gruplar oluşturarak bu düşünceler adına birtakım faaliyetlere girişebileceği bir ağ yapılanmasıdır (Uçkan, 2013, s. 64).

3.1.9.2 Lulzsec

Lulzsec aslında Lulz Security'nin kısaltılmış halidir. İddiaya göre Anonymous grubu ile rekabet halinde olan İnternet Fedosu adlı grubun altı üyesi Lulzsec grubunu kurmuştur. İdeolojisi aslında eğlenmek amaçlı saldırılar düzenlediği belirtilmiştir. Zaman zaman da politik mesajlarda verdiği olmuştur.[9]

LulzSec'te eylemlerini, "Halk ya da tüketiciler aleyhine çalışmalar yaptığı" iddiasıyla ülke ve şirketlerin önemli sitelerine saldırılarda bulunarak göstermiştir. 50 gün boyunca devam eden faaliyetlerinin ardından kendilerini feshettiklerini duyurmuştur. Ardından 2011 senesinde eylemlerine ara veren grup, 2012 yılından itibaren LulzSec Reborn adıyla eylemlerine devam etmiştir. Amerika ve İngiltere'de itibarlı hükümet ve özel sektör internet sitelerini hedef almıştır. Saldırılarında çoğunlukla DDoS saldırıları düzenlemiştir.

LulzSec adlı hacker grubu Nintendo, SonyPictures, Paypal, MasterCard, Century Fox gibi devlet kurumlarının ve özel sektörlerin internet sitelerine saldırıları ve özellikle Sony Playstation ağına yaptığı saldırı siber saldırı sonucu, 77 milyon kullanıcının verilerini aldıklarını duyurmasıyla tanınmaktadır. CIA'in web sitesine saldıran grup, siteyi kapatmıştır. CIA'in internet sitesini kapattığını kabul eden 24 yaşındaki grup lideri Glen McEwen, Avutralya kolluk kuvveti tarafından 24 Nisan 2013 yılında yakalanarak tutuklanmıştır (Kara, 2013, s. 22).

3.1.9.3 Suriye Elektronik Ordusu (SEA)

Suriye Elektronik Ordusu 2011 yılında açtıkları web sitesi üzerinden kendilerini tanıtmışlardır. Ana gayeleri Suriye'de çıkan iç çatışmalarda yaşanan gerçekleri çarpıtmaya çalışan, mezhep çatışmalarını başlatarak nefreti yaymaya çalışan medya kuruluşları ile sosyal ağları hedef almaktır. Hacktivist grup olarak kendilerini

[9] https://en.wikipedia.org/wiki/LulzSec, Erişim Tarihi, 25.03.2021

tanıtmışlardır. Her ne kadar hükümet yanlısı politikalar sergilemiş ve Beşşar Esed'te "Sanal alemin gerçek orduları" şeklinde söz söyleyerek onları desteklediğini beyan etmiş ise de hükümet tarafından resmi kurulan bir hacker grubu değildir.

Suriye Elektronik Ordusu, Amerikan Associated Press isimli haber temsilcisinin twitter hesabını hackleyerek sanayi endeksinde maddi zarara neden olduğu gibi bu saldırıdan sonra da Suriye karşıtlığı haberi yapan NPR, BBC, CBS News gibi haber sitelerini, bazı insani kuruluşların web sitelerini hacklemiştir.

3.1.10 Ünlü Türk Hacker Grupları

3.1.10.1 RedHack (Kızıl Hackerlar)

Redhack (Kızıl Hackerlar, Kızıl Hackerlar Birliği), 1997 yılının mayıs ayında Türkiye'de kurulmuştur. Hacking ve programlama bilgisi dışında bir dünya görüşü mevcut olduğunu bu nedenle kendilerini marksist ve sosyalist olarak tanımlamışlardır.

Bir tüzük ile yapılanması bulunan grup bünyesinde; üyelik kabul şartları, hedef ve amaçları, grup üyelerinin sahip olduğu görev ve sorumluluklar, üyelerin sahip olduğu haklar, mali kaynaklar ve üyelikten ayrılmaktan söz edilmektedir (Turak, 2014, s. 7).Şirinler isimli çizgi filmin, karakterleri olan Şirin Baba, şirine, isyankar şirin, çalışkan şirin, Doğrucu şirin gibi iyi niyetli kahramanlarının adlarını takma adı olarak kullanmaktadırlar. Böylelikle grup üyeleri sevimli ve zararsız oldukları izlenimi vermektedir (Kara, 2013, s. 20).

Serkan Ocak'ın 2012 tarihi nisan ayında Radikal gazetesine RedHack ile ilgili verdiği röportajında; devrimin bir kızıl ordunun neferi olduklarını, köylülerin, emekçilerin işçilerin, katılanların, öğrencilerin her türden ezilen dünya toplum ve uluslarının ajanı olduklarını ifade ederek, gizli ajan oldukları iddialarını reddetmişlerdir. Ayrıca hiçbir sol örgütle doğrudan veya dolaylı bir bağlantılarının olmadığını, PKK'lı oldukları söylentilerinin, bu gruba desteğin engellenmesine yönelik uydurulmuş iddialar olduklarını belirtmişlerdir (Gökdemir, Eylül 2013, s. 31).

Grubun çekirdek üye sayısının 12 olduğu söylenmektedir. “Halk için hack” sloganını şiar edinmiş olan RedHack grubunun gelirlerini temelde illegal olmak üzere, “devrimci duruşun rehberlik ettiği bir şekilde” yeteneklerinden yararlanarak elde etmektedir. Ayrıca gruba dahil olan kişilerin hünerlerine göre Merkez Komite, Siyasal Büro, Basın ve Enformasyon Bürosu, Teknik Büro, Enternasyonal Büro, Hack Bürosu, Askeri Komite, Alt Grup Komitesi şeklinde çeşitli komite ve bürolar yer almaktadır (Turak, 2014, s. 7-8).

Redhack hangi eylemi yapacağına, kendi ifadeleriyle “halkın ihtiyaçları doğrultusunda belirlemeye” çalışmaktadır. Bu nedenle, iki grup çalışma sistemi geliştirmişlerdir. İlk grubun, sisteminin zayıf noktasını aradığını, açığını gördüğü sistemlere sızarak, sistemi hacklediğini, ikinci grubun ise, faaliyetlerinin belirli bir siyasi çizgide olduğundan gireceği sistemin zayıf noktasını aramak biçiminde çalışma sürdürmektedir. Türkiye’de hayatını sürdüren ve bu sebeple gündemi takip eden grup üyeleri, yalnızca internette takılan asosyal kişilerden olmayıp sokaklarda takıldıklarını söylemektedirler. Hacker olarak tanınmak istemediklerini, devrimci olarak tanınmak istediklerini ifade etmektedirler. Siyasi bir anlayışa sahip olduklarını bu minvalde açıklayacakları dokümanların da siyasi amaca hizmet edeceğini söylemektedirler (Kara, 2013, s. 20).

3.1.10.2 Ayyıldız TIM

Ayyıldız Tim adlı hacker grubu bir Türk hacker grubudur. 2002 yılında kurulmuştur. Bir web sitesi bulunmakta olup bu web sitesinde kendilerini Türkiye’ye yönelik düşmanlar tarafından yapılabilecek herhangi bir siber saldırılara karşı gönüllü olarak hizmet veren topluluk olarak tanıtmışlardır. Kuruluş amaçlarının en öne çıkan ögelerden biri devletçiliktir. Devlet adamlarına ve devlet kurumlarına, her türlü değerlerimize

yapılan kabalıkları devletin bütünlüğüne yapılan bir saldırı olarak görmekte ve duruma göre saldırı hedef ve yöntemlerini seçtiklerini söylemektedirler[10].

Ayyıldız Tim, Anonymous tarafından Telekomünikasyon İletişim Başkanlığı'na karşı düzenlenmiş saldırıyı karşı cevap vererek engellemiştir. Ayrıca Pentagon'un internet sitesini sekiz saat süreyle erişimsiz kılmıştır (Kara, 2013, s. 25).

3.1.10.3 Cyber-Warrior

Bir Türk hacker grubu olan Cyber-Warrior 2001 yılından beri faaliyetini kesintisiz bir biçimde sürdürmektedir. Bilişim güvenliği alanına hakim yüzlerce beyaz şapkalı hacker yetiştirmiştir. Kendilerini, inanç ve ahlaki değerlere yapılan saldırılar, Türkiye'ye yapılan saldırılar ve kamu vicdanını kötü etkileyen hadiseler karşısında sanal dünya üzerinde eylemlerini sürdüren hacktivist grup olarak tanıtmaktadırlar. Yine kendi kurmuş oldukları internet sitesinde misyonlarını açıklarken *internet üzerinden İnanç ve Ahlaki değerlerimize saldırı yapan, Saf beyinleri bulandırmaya yönelik içerikler bulunduran, Satanist ve Pornografik içerikli yayınlarla mücadeledir* şeklinde belirtmişlerdir[11].

Cyber Warrior adlı hacker grubu herhangi bir kuruma, örgüte, derneğe, partiye ideolojik görüş veya siyasal anlamda kimseyle bir bağı bulunmadığını söylemektedirler Gruba katılmak isteyenler, bilgi ve becerilerine göre toplulukta görev verilir (Kara, 2013, s. 24).

04/07/2003tarihinde Türk askerlerinin başına çuval geçirilmesi hadisesine karşılık binlerce ABD web sitesini hacklemişlerdir. Hackledikleri web sitelere "BİR TÜRK AMERİCA'YA BEDELDİR 11 TÜRK İÇİN DÜNYAYI FETHEDERİZ" ve "Şimdilik

[10]https://www.ayyildiz.org/ayyildiz-tim-tarihi.html, Erişim Tarihi, 04/03/2020
[11]https://www.cyber-warrior.org, Erişim Tarihi, 03.04.2020

1.500 tane sitenizi topraklarımıza dâhil ediyoruz İP/Cyber Warrior Team Akıncılar Grubu" şeklinde mesaj bırakmışlardır[12].

3.1.10.4 Türk Hack Team

Kendilerini milliyetçi, muhafazakar ve Atatürkçü olarak tanımlayan ve genel itibariyle Uluslararası hack gruplarından Türkiye'ye dönük yapılan hack operasyonlarına karşı koymak üzere kendini tasarlamış bir grup, Türkiye de yeterince bilinmese de Uluslararası alanda en çok bilinen gruplardan biri diyebiliriz, bundan birkaç ay önce softpedia adlı otoriter bir sitede Dünya 'nın en etkili 2. Hack grubu olarak seçilmiş, 1. sırada olan grup ise sizlere çok tanıdık gelecek olan Anonymous adlı hacker grubu. Uluslararası basına da bakıldığında bu grup Washington Post, New York Times, LeFigaro gibi birçok uluslararası basın organında makalelerine rastlamaktayız

3.2 Dijital Aktivizmin Bir Türü Olarak Hacktivizm

Dijital aktivizm, aktivizmin bilişim teknolojilerini kullanarak eylemlerini siber ortamda yani dijital dünyada gerçekleştirilmesidir. Dijital aktivizm; slaktivizim, kliktivizm, hacktivizm gibi türler ile kendisini göstermektedir. Bu durumda dijital aktivizm farklı aktivizim türlerinin genel bir ifade biçimidir. Aktivist faaliyetler, bilişim teknolojilerin gelişmesiyle hızlı, etkili, ulaşılabilirlik düzeyi ve eş zamanlı olarak kendini göstermiştir. Hacktivizm de hacker etiğini benimseyen aktivislerin politik gerekçelerle hedef haline gelen kurum ve kuruluşların internet sitelerine hacking eylemi yapılıyor olması gerekçesiyle dijital aktivizmin başka bir türü olarak faaliyeti gerçekleşmektedir. Hacktivizmi açıklamadan önce aktivizm ve dijital aktivizmin ne olduğunu açıklamaya çalışacağız.

[12]http://www.cyber-warrior.org/Hacked/index.htmErişim Tarihi, 03/04/2020

3.2.1 Aktivizm ve Dijital Aktivizm

Türk Dil Kurumu aktivizmi, eylemcilik olarak açıklamaktadır. TDK'ya göre; aktivizm, bir araya gelmiş insanların kurum ve kuruluşlar üzerinde baskı yaratarak problemli gördükleri siyasetleri, durumları ya da uygulamaları düzenleme çabasını ifade etmektedir. Aktivizm çoğunlukla toplumu oluşturan bir kısım üyelerin sorunlu bir uygulama görmeleri halinde ortaya çıkmaktadır. Aktivizm ile ilgili sosyolojik açıklamalar cinsiyet, ırk, ekonomik farklılıklar tarzında sosyal ayrıcalıklar ve ayrışmalar, aktivizmin meydana çıkmasında esas koşul olarak kabul edilmektedir. Ayrıca bu düşünce siyasi, ekonomik dini ve ideolojik ayrımları da aktivistler için ideolojik motivasyon kaynakları olarak görmektedir (Yılmaz, Dündar ve Oskay, 2015, s. 486)

Bir başka tanımda; *bireylerin, kurumların ya da hükümetlerin sergilediği yanlış, hatalı ya da zararlı sonuçları olduğuna inanılan davranışlara karşı gerçekleştirilen eylemlere aktivizm, bu eylemlerde bulunan kişilere aktivist denilmekte*dir (John ve Thomson, 2003, aktaran; Sert, 2012, s. 128).

Aktivistler genelde insan hakları, çocuk hakları, hayvan hakları, yaşama hakkı gibi konular üzerinde yoğunlaşmaktadırlar. Sert, bu tanımlamalardan çıkarsamada bulunarak aktivizmin, problemli veya haksızlıklarla ilgili olumlu yönde bir değişim yapmak hedefiyle gönüllü olarak bir arada olan insanların ortak mücadele verdikleri sonucuna ulaşmıştır (Sert, 2012, s. 129).

Clarke ve Wilson, insanların gönüllülük icap eden topluluklara dahil olmanın nedenini 3 farklı teşvike bağlamaktadır. Bunlar maddiyata yönelik teşvikler, dayanışma duygusuna yönelik teşvikler, hedefe yönelik teşvikler (Sert, 2012, s. 129)

Dijital aktivizm ise, aktivist çalışmaların, sosyal medya da olmak üzere kitlelere anlık bilgi akışı ile ulaşmayı mümkün kılan alanlarda ya da podcast, vlog, blog, fotoğraf ve video paylaşım siteleri ve benzeri yerlerde gerçekleştirilmesidir (Akmeşe ve Deniz, s. 498).

Görüldüğü üzere aktivistlerin olan biteni mümkün olduğunca geniş kitlelere, en hız bir şekilde ve topyekün olarak anlatma gayreti içerisinde olduğundan teknolojiden faydalanmaktadır. Bu itibarla temelini internetten alan yeni bir faaliyet alanı ortaya çıkmıştır. Bunun adı da dijital aktivizmdir.

Dijital aktivizmin etkin ve yoğun kullanılmasının sebebi internetin sunmuş olduğu zengin imkânlardır. Toplumu ilgilendiren konuların alternatif kaynaklardan ve daha demokratik bir şekilde paylaşılması ile kolektif hareketlerin organize olması açısından internetin sunmuş olduğu avantajların önemi gün yüzüne çıkmaktadır (aktaran; Sert, 2012, s. 129).

Dijital aktivizmin sosyolojik anlamda bir destek veya tepki faaliyetleri bakımından iki biçimde kendisini göstermektedir. Birincisi, internet ve sosyal medya uygulamaları aracılılığıyla bir konu ile ilgili örgütlenmek şeklinde seyretmek, ikincisi de internetle alakalı olarak kötü biçimde yorumlanan bir olay ya da düzenlemeye tepki vermek için sosyal medya uygulamaları ile bir mesaj yayınlamasıyla kısa bir süre için ekranlarını karartmaları şeklinde seyretmektedir. Bu şekilde eylemsel ya da düşünsel olan tepki de dijital bir şekilde gösterilmektedir (Yegen, 2014, s. 123).

Dijital aktivizm, 2010 yılında meydana gelen ABD Dışişleri Bakanlığı ile konsoloslukları arasındaki iletilerin ifşa olması hadisesi ile ortaya çıktığı (Wikileaks olayları) ifade edilir (Yegen, 2014, s. 122). Ardından sosyal medyanın etkisi ve bu mecralardan destekler alarak gerçekleşen ve hızlı yayılan Arap Baharı, daha sonra İspanya (Demokrasi Hemen Şimdi adlı manifesto), Yunanistan, İsrail'deki "öfkeliler hareketi, hemen ardından küresel ekonomik krizin ortaya çıkarak çevreye yayılması olayına bir cevap olarak, "Wall Street'i İşgal Et" hareketi ortaya çıkmıştır (Uçkan, 2013, s. 54). Bu sayede dijital iletişim ile yeni aktivizm biçimlerinden de söz edilir olmuştur.

Dijital aktivizm; slaktivizim, kliktivizm, hacktivizm gibi türler ile kendisini göstermektedir. Hem slaktivizm yani tembel aktivizm hem de kliktivizm yani tıklama aktivizmi, aktivist hareketlere bedensel olarak değil, bilişim ve iletişim teknolojiler

aracılığı ile katılmayı ifade etmektedir (Yılmaz, Dündar, ve Oskay, 2015, s. 491). Bununla yanında kliktivizm ve slaktivizm arasında birtakım ayrılıklarda mevcuttur. Kliktivizm, yönetimsel bir özellik taşımaktadır. Kliktivistler, kampanyalar oluşturarak grup veya toplulukları bir araya getirmekte iken Slaktivizm ise kampanyalara sosyal medya aracığı ile destek vermeyi ifade etmektedir (Yegen, 2014, s. 122).

3.2.2 Hacktivizm

Hacktivizm kavram olarak hackleme ve aktivizm kelimelerin evliliğinden meydana gelmiştir. Hacktivizm, hedef aldığı bir internet sitesine yönelik büyük zararlara neden olmayı amaçlamayan ancak tepkisini ve rahatsızlığını dile getirmeyi amaçlayan faaliyetlerini kapsar (Yegen, 2014, s. 123).

Hacktivizim politik eylemlerin kurum ve kuruluşlara yönelik dijital ortamda gerçekleştirme faaliyetidir. Ayrıca Alexandra Samuel'e göre hacktivizm; "hack ve aktivizm kelimelerinin portmantosu ve yasal açıdan belirsiz araçların politik sonuçlar pesinden sessiz bir şekilde kullanılmasıdır." Dunning'e göre ise hacktivizm; "bilgisayar korsanlığının özel yazılımlar yardımı ile alışılmadık ve genelde yasa dışı yollarla, bilgisayardan faydalanılan operasyonlar olarak adlandırıldığı noktada, bilgisayar korsanlığı ve aktivizmin çakışmasıdır." Demirkıran'a göre "bilgisayar teknolojisinin veya programlama sistemlerinin toplumsal bir soruna yönelik tepki gösterme amaçlı kullanılmasıdır." şeklinde tanımlamalar mevcuttur (Demirkıran, 2013, s. 27).

Taylor'a göre, hacktivizm 1990 yılların açık bir politik duruşudur. Metalaşmış bazı politik değer ve uygulamalara karşı bir direniş veya tepki özelliğini ifade eder. Smith'e ve Yamitch'e göre ise, hacktivizm eylemi yapan hacktivist gruplar ve kişiler, kötü niyetli bir hackerlar gibi yıkıcı eylemlerde bulunmazlar, amaçları toplumsal veya politik mesajlar iletecek olan bir amaca dikkat çekmektir ve bu çoğunlukla şirket veya hükümet politikalarına karşı saldırıları kapsar. Ayrıca, hacktivizm aynı zamanda insanları önemli çok sosyal veya politik sebepler konusunda destek ya da tepki konusunda düşünmeye zorlar (Yegen, 2014, s. 123-124).

Hacktivizm köklü bir geçmişe sahiptir. Aktivizm ile ilişkili olarak hacktivizm denilemese de 1980 yılında PeaceNet adına bir haber grubu kurulmuştur. Bu teknoloji ile insanlara bilgi vermek ve iletişim amaçlı olduğu görülmüştür. Daha sonra teknolojinin gelişmesi ve internetin icadıyla aktivistler eylemlerin dijital ortamda ifade edebileceği kanallar keşfetmiştir. Bu şekilde aktivizmin çehresi değişmeye başlamıştır. Böylece günümüzü hactktivizmin ilk adımları atılmıştır.

1990 yılında Electronic Disturbance Theater (EDT) adlı aktivist grubu, Meksika yerlilerinin ayaklanmasına destek maksatlı internet üzerinden aksiyona geçerek FloodNet adlı bir program üretilmiştir. Bu yazılımla sanal oturumlar ile kindar taraftaki web sayfasını geçici bir müddet işlevsiz hale getirmiştir. Böylelikle yaşanılan olaylara karşı tepkilerini dünyaya duyurmayı başarmışlardır (Demirkıran, 2013, s. 26).

Demirkıran hacktivistlerin, sadece bir grup hacker ya da hackerlardan oluşup oluşmadığına yönelik Anonymous ile ilgili internet sitelerinde dijital etnografi incelemesi yapmıştır. Bu araştırma ile hacktivistleri teknolojik açıdan 3 grubu ayırmış olup; **birinci grup,** ileri seviye programlama becerisine sahip hackerlardr. Bu gruptaki kişi sayısı azdır. Hacktivizmin öncüleri, kâşifleridir. Hactivizmi yönlendirebilecek, dönüştürebilecek ve yeni yollar keşfedebilecek güçtedirler. **İkinci grupta ise** üstat diye tabir edilen hackerlar kadar bilgiye sahip değilseler de teknik kavramlara aşinalardır. Genel olarak görsel tasarım konusunda bilgilidirler. İletişim materyalleri hazırlama konusunda destek olabileceği belirtilmiştir. **Üçüncü grup** ise çok fazla bir bilgisi olmayan ya da hiçbir fikri olmayan kişilerdir. Bunlara hacker denilmez ancak hackerlardan destek alırlar (Demirkıran, 2013, s. 28).

Hacktivistler genelde DDos saldırıları gerçekleştirirler. Çünkü hacktivistlerin hepsi teknolojik bilgileri üst düzey olmadığından, DDos saldırıları kolay öğrenilebilir ve kullanılabilir özellikte olduğundan bu yöntemi tercih etmektedirler. Ayrıca hacktivist oluşumların genelde gençlerden oluştuğu söylenebilir. Nedeni ise Z jenerasyon (1980-1990 arası doğanlar) olarak adlandırılan bu kuşağın gözünü dijital dünya ile açmış olmalarıdır. İnternet ile kısıtlamalardan hoşlanmamaktadırlar. Bu şekilde "bilgi özgür kalmalıdır ve paylaşılmalıdır" şeklindeki ilkenin doğal olarak farkındadırlar. Bunun

sonucu olarak da gördükleri veya görecekleri engellenme kaygılarından ötürü bu platformlarda hemen yer almış, bilişim sistemlerini ve teknolojik ürünleri kolaylıkla kullanır olmuşlardır.

Online aktivizm, hacktivizm ve siber terörizm arasında kesin çizgilerle birbirinden ayrılmıştır. Online aktivizimde internet, iletişimi araç olarak kullanılır. Asıl hareket zemini gerçek dünyadır. Hacktivizm de ise eylem alanı dijital dünyadır. Protesto amaçlı eylemler ile bir probleme dikkat çekmek için tercih edilir. Ayrıca eylemlerinde yıkıcı ve yok edici özellik barındırmaz. İşte bu tam da noktada siber terörizmden ayrılır. Siber terörizmde sistemlere zarar verilir, çökertilir, yıkıcı ve yıpratıcı bir hal alır. Ancak şunu belirtmek gerekir ki her zaman hacktivizm amacıyla yapılan eylemler siber terörizme kayması muhtemeldir (Demirkıran, 2013, s. 30).

Hacktivistler, hack eylemlerin suç olduğunu kendileri de bilirler. Ancak eylemlerinin siber savaş, siber terör ile ilgili düzenlenen kanunlar kapsamında değerlendirilmesine karşıdırlar. Çünkü eylemlerin bir terör örgütünün amaçları doğrultusunda yapmadıklarını ifade ederler. Ancak eylemleri artık yıkıcı bir hal alıp terör örgütlerinin amaçları doğrultusunda yapıyorlar ise artık siber terörizmden söz edilebilir.

3.3 Türkiye'de Hack Kültürü ve Hacktivizm

Türkiye, internet ile 1990 yılların sonunda tanıştığından hack kültürü, Amerika veya Avrupa'da olduğu gibi kodlardaki üstün zeka ve becerilerine göre hacker unvanı alınır şeklinde bir algı tam olarak oturmuş değildir. Bu nedenle toplumsal algı bakımından hacker, cracker vb. kavramları medyanın da etkisiyle hep olumsuz anlamlar yüklenmiştir.

Türkiye' de hacker kültürü (kırıcı kültürü) konusunda Ufuk Eriş (2009)'in doktora tezinden başka çalışma yapılmadığı görülmüştür. Türkiye'de bu ve benzeri konular çoğunlukla suç olgusu özelde bilişim suçu perspektifinden ele alınmış, hukuki ve güvenlik politikalar bakımından çalışmalar, değerlendirmeler ve çözümler yapılmıştır. Bu tablodan bile Türkiye'de hacker kültürünün anlaşılmadığına ve bu nedenle üzerinde neden durulmadığına yönelik ipuçları barındırmaktadır.

Türkiye'de hacker kültürü ve yapısı konusunda akademik düzeyde yapılan araştırmalar neticesinde kendilerini hacker olarak tanımlayan kişiler için aşağıdaki sonuçları söyleyebiliriz (Eriş, 2009):

- Hacker olarak kendini tanımlayan kişiler çoğunlukla genç yaştaki (14-21)erkek öğrencilerden oluşmaktadır.
- Türk hackerlar, hackerlık bilgilerini forumlardan öğrenmişlerdir. Bu forumlara üyelik dâhilinde katılabilmektedirler. Üye olduktan sonra belli unvanlarım mevcuttur. Dolayısıyla belli bir hiyerarşik yapıları olduğu söylenilebilir.
- Hackerlik gibi kavramlara internet aracılığı ile karşılaştıkları, başlama sebepleri arasında, başlarına gelen bir olay, kişisel nedenler ve internetten araştırma yapma olarak sıralanabilir.
- Hackerlık ile uğraşı nedenleri arasında en belirgin olarak, eğlenmek ve ülke menfaatleri çerçevesinde milli bir duruş sergileyerek ülkeye hizmet etmektir.
- Hackerlik faaliyet amaçlarının ise uyarı amaçlı sistem açıklarını bulmak, protesto amaçlı site kırmak, öğrenmek ve merak duygusudur.
- Hacking yöntemleri arasında en çok SQL injection site kırmak, xss açıkları ve exploit kullanmaktadırlar.
- Hacking faaliyetlerini bir suç olarak algılamaktadırlar ancak bu faaliyetler bir ülke amaçlarına hizmet ediyorsa suç olarak tanımlanmaması gerektiğini düşünmektedirler.
- Hack eylemlerinden anladıkları, bilişim sistemlerine izinsiz girebilmek ve protesto amacıyla internet sitelerini hacklemek olduğudur.
- Türk hackerlar meşru olarak hedefledikleri alanlar terörist oluşumların internet siteleri ve yetişkin (+18) siteleridir.
- Siyasi görüşleri muhafazakâr ve milliyetçi temelinde olduğu görülmüştür.
- Hacker etiğinden anladıkları, ülkü dahilinde olmak, kişisel ahlak ve bir misyon olarak algılamaktadırlar.
- Kendilerini, yabancı hackerlardan daha çalışkan, meraklı ve zeki olduklarını ayrıca hareket dürtülerinin yabacılardan farklı olarak dini ve milli değerler ile hareket ettiklerini düşünmektedirler.

Yukarıdaki maddeler, bir bütün olarak değerlendirildiğinde Türkiye'deki hackerların hacker etiğinden anladıkları ile hackerların doğduğu ve büyüdüğü yerde algılanan hacker etiğinden farklı olduğunu görmekteyiz. Amerika ve Avrupa'da daha çok muhalefet biçimi olarak karşı kültürü temsil ederken, Türkiye'de muhafazakar ve milliyetçilik temelinde şekillenmiştir.

Her ne kadar hacker etiği bakımından farklılık görülmüş ise de hacker eylemlerini zevk için yaptıklarını beyan etmeleri üstatların belirlediği hacker etiği içerisinde değerlendirilebilir. Ancak hacker kelimesi ile ilgili olarak üstad anlayışını benimseyen Türk hackerları hacking faaliyeti konusunda konusun da korsan yaklaşımını benimsemektedirler. Ancak *üstat* anlayışını benimsenmesinin uzantısı olarak sistemler hakkında bilgili olmak üretmenin değerlendirilmesi beklenmektedir.
Türkiye'de hack gruplarından bahsetmek gerekirse amaç ve politik görüşleri bakımından ikiye ayrılmıştır. Birincisi, temelini milliyetçi ve muhafazakâr vb. görüşlerden alan kendilerini milli olarak tanımlayan, devlet güçlerinin desteğini alan gruplar, diğeri ise özgürlük savaşçıları olarak ifade edilen, siberpunk yaklaşımı çerçevesinde anarşist ilkelerin ön plana tutulduğu, sosyalist, Marksist temelli gibi kavramlar çerçevesinde değerlendirilebilecek, devlet güçlerinin karşısında yer alan ve devlet güçlerinde milli olmayan gruplar olarak tanımlanan gruplardır.

Devlet güçlerinde milli olarak tanımlanan ya da Eriş'in araştırmasından çıkan sonuçlara uyan gruplar olarak Turk Hack Team, Ayyıldız Tim, Cyber Warrior (akıncılar) yer almaktadırlar. İkinci gruba örnek olarak Redhack ve coldhackers verilebilir.

Yukarıdaki değerlendirmenin yanında Türkiye'deki hacktivizm grupları arasında ön plana çıkan Redhack grubunun ayrı tutulması gerekmektedir. Özgür Uçan'a göre bu grup hacker etiğine uygun eylemlerde bulunmaktadır (Uçkan, 2013, s. 66).

Örnek vermek gerekirse birinci gruptaki tanımlanan grup Ermeni soykırım yasasını gündeme getiren Fransız milletvekilinin sitesine saldırıp hacklemek yada internetin güvenli internet olması bakımından filtreleme sistemini getiren Bilgi Teknoloji

Kurumun sitesine tepki amacıyla saldıran Anonymous'un iletişim forumlarından birini hacklemek devletçi eylemler olarak değerlendirilirken, otorite karşı eylemlerde bulunan, hedeflerini devlet kurumlarından ve ana akım medyadan seçen grup, ikinci gruplardan değerlendirilmektedir (Uçkan, 2013, s. 66).

Bu nedenle Uçkan'a göre Redhack Türkiye politik panoramasının bir parçası olduğunu söylemektedir.

SONUÇ

Enformasyon teknolojilerin gelişmesi, internetin buluşu ile mekân ve zamanda bir dönüşüm yaşanmış, devletler arası sınırlar ortadan kalkmış, doğu bloğunun yıkılmasıyla mal ve hizmetler tüm dünyaya yayılmış, uluslararası kuruluşlar ortaya çıkmış ve tüm dünyayı etkisi altına alan, siyasi, kültürel, ekonomik ve sağlık alanda değişimler yaşatan ve dünyayı köy haline gelmesini ifade eden küreselleşme kavramı ortaya çıkmıştır.

Çalışmamızda küreselleşmeye dair sunduğumuz bu bilgiler doğrultusunda ve Manuel Castels'in kuramını merkeze alarak, günümüzde toplumların yeniden şekillendiğini görmekteyiz.

Castells'e göre toplumların yeniden şekillenmesinde ise birbirinden bağımsız 3 sürecin bir araya gelmesi ile oluşmaktadır. Bu üç süreç; yeni teknolojilerin gelişmesi, kapitalizmin ve ulus devletlerin kendini yeniden yapılandırması ve yeni toplumsal hareketlerin ortaya çıkmasıdır. Bu süreçlerin birbirleri ile olan etkileşimi ile yeni bir toplumu; ağ toplumunu meydana getirmiştir.

Küreselleşme ile birlikte bu yeni toplumsal yapı, kapitalizmin oluşturduğu kurumları yerinden oynatmakta, kültürleri evrimleştirmekte, ulus mantığı ile kurulan devletlerin alanları daraltmakta, sınırları kaldırmaktadır.

Castels'e göre ağ toplumunda, sınıf ve kimlikler parçalanmış, kaybolmuş, ağ toplumuna uyum sağlayan sadece ağ işçileri ortaya çıkmıştır. Geri kalanı ise toplumun paryasını oluşturmaktadır. Ağ toplumunda eşitsizlikler, kutuplaşma ve dışlama üzerine kurulu düzen, gezegene yayılmıştır. Giderek parçalanmış olan bu kimlikler, yeniden inşası için bir araya gelmesine kolektif kimliklerin ortaya çıkmasına neden olmaktadır. Dolayısıyla kolektif kimlikler beraberinde birtakım talepleri, isyanları birlikte getirmektedirler. Devletlerin bu taleplere karşı karşılık vermemekten ötürü meşruiyet krizi ortaya çıkmasına neden olmaktadır. Meşruiyet krizi derinleştikçe değerler üzerinde birleşen direniş kimlikleri temelinde örgütler/cemaatler oluştuğu söylenebilir.

Bu örgütler devletlere ve toplumun yıkıcı mantığına karşı eski klasik yöntemlerle savaşmamakta, gelişen teknolojik gelişmeler neticesindeki araç ve gereçlerden yararlanmaktadırlar.

Bunun sonucunda yeni bir dünya; siber dünya, yeni bir kültür; hacker kültürü, sanallaştırılmış gerçek kültür(gerçek sanal kültürü) 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

Çalışmamızın odak noktası, yaşanan toplumsal değişimde ve ortaya çıkan toplumsal hareketler bağlamında oluşan hack kültürü incelenmiştir. Ancak hack kültürünün doğru bir şekilde incelenmesi için siber dünyadaki diğer kavramların, aktörlerin ve eylemlerin de tanımlanması yapılmıştır.

Araştırmanın sonucuna göre, siber dünyadaki hacker kültürünün aktörleri ve eylemleri ile suç kültürünün aktörleri ve eylemleri birbirlerinden farklı olduğu kadar aynı olabildiği görülmüştür. Bu durum, tanımlayan kişinin konumu, hayata bakış açısı, siyasi düşüncesi, konu hakkındaki bilgi ve tecrübesi ile eylem sahibinin niyeti, kendini nasıl konumlandırdığı ve doğurduğu toplumsal sonuç ile değişkenlik göstermektedir. Çalışmamızda bu aktörlerin kimler olduğunu, eylemlerin nelerden ibaret olduğu, kendilerini nasıl tanımladıkları ve dışardan nasıl tanımlandıkları hangi kavramlar ile ifade edilmeye çalışıldığını keskin çizgiler olmasa da belirgin bir şekilde ayrıştırmaya çalışıldı.

Siber dünyada işlenen suçlar; bilgisayar suçu, internet suçu, siber suç, bilişim suç hukuku, 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 savaş kavramlarının saldırı yöntemleri her ne kadar benzerlik gösterse de motivasyon ve amaçları bakımında ayrıldıkları görülmüştür. Buna göre siber suç, bilişim sistemlerinin kullanılmak sureyle kişiden kişiye işlenen suçlar olduğu değerlendirilmektedir. Burada herhangi bir örgütsel eylemin olmadığı anlaşılmaktadır. Bireysel eylem söz konusu olmaktadır. Bilişim suçu, bilişim sistemlerine geçici veya kalıcı zarar vermek, verileri elde etmek veya yok etmek ifade edilmektedir. Ancak bu saldırılar örgütlü bir şekilde ideolojik, devlete karşı olduğunda ya da toplumları paniğe sokmak, korkutmak ve karışıklık meydana getirmeye çalışıldığında devletler bunu siber terörizm kapsamına soktuğu görülmüştür. Yine bu saldırılar devletten, devlete ister doğrudan ister dolaylı yoldan olduğu vakit siber savaş kapsamına alınmaktadır.

Bilişim suçları kapsamında değerlendirilen siber saldırılar vatandaşların hayatlarını etkilemekte, ekonomi alanında şirketlere büyük kayıplara uğratmakta ve devletlerin güvenliğini tehdit etmektedirler. 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.

Ülkemizde bilişim suçları ile yapılan mücadele yasal altyapımızda bir takım önemli eksiklikleri bulunmaktadır. Örneğin siber dünyaya ilişkin kavramların kanunlarımızda net tanımlanmadığından ve bazı kavramlara yer verilmediğinden, her görünen siber eylemlerin terörizm etrafında değerlendirilmekte, her örgütsel eylemlerin terörist grupları sınıfına sokulmaktadır. RedHack ve benzer davalarda bu eksiklikler görülmüştür. Bu nedenle Türk Ceza Kanunu'nda ve Ceza Muhakemesi Kanunu'nda siber suç, siber saldırı, siber savaş gibi benzer kavramlara ve yaptırımlarına ilişin yeni düzenlemelerin yapılması gereklidir. Örneğin siber teröre ilişkin halen ilgili mevzuatlarda tanımının yapılmamış olması büyük bir eksiklik olduğu değerlendirilmektedir. Ya da 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 halen netlik kazanmamıştır.

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.

Hacker kültürünün anlaşılması bakımından birkaç önemli nedenleri mevcut olduğunu görmekteyiz. İlk olarak suç eğilimi gözetmeksizin değişen toplumsal yapıya ayak uydurarak pratikte demokratik yoldan nasıl sisteme başkaldırdıklarını görebilmekteyiz. Diğer bir hususta teknolojilerin demokrasi yolunda nasıl kullanılabileceği hakkında topluma bir resim çizebilmiştir.

Araştırmanın sonucuna göre, hacker eylemlerinin ağ toplumu ile olan ilişkisi dikkate alındığında, siber suç, siber terörizmden farklı yorumlar yapmayı mümkün kılmıştır. Her ne kadar bir bilgisayara sızmanın suça dönüşebileceği gözler önüne serilmiş ise de hacker kültürünün fikir ve eylem pratiğinde ağ toplumunun eleştirisi olarak değerlendirmekte mümkün olmaktadır.

Castells' göre, ağ toplumunun kapitalist toplum olduğunu, ancak yeniden dönüşerek güçlendiğini hâkim anlayışının ise Protestan etiği olduğunu ifade etmiştir.

Araştırmanın sonucuna göre, Protestan etiğinde çalışma hayatının ve çok para kazanmanın ulvi olduğu, zamanın ve çalışma biçiminin optimize edildiği, bilginin meta haline getirildiği, himaye edildiği ve tekelleşmesini sağladığı görülmektedir. Ancak hackerların kültürü incelendiği zaman, onlar için çalışma hayatı, minimum geçim kaynağından fazla önem taşımamaktadır. Arzularına göre çalışmakta, yine arzularına göre oturmaktadırlar. Burada çalışma hayatlarının ve zamanlarının optimize edilmediği görülmektedir. Onlar için eğlence ve sosyalleşme daha ön plandadır. Bu nedenle yazılımlarını paylaşmaktan hoşlanmaktadırlar. Ayrıca diğer topluluklar tarafından kabul görmekten zevk duymaktadırlar. Bilginin serbest/özgür dolaşımını savunmaktadırlar. Aynı zamanda mahremiyet konusunu da görmezden gelmemektedirler. Bu anlamda hacker etiği, Protestan etiğinin tutumundan ayrıldığı değerIendirilmiştir.

Çalışmanın sonucuna göre ağ toplumu ve Protestan etiğine baskın olan yedi etik değer "iş, para, esneklik, optimumu sağlama, belirleyicilik, neticenin muhasebesini yapma ve istikrar" olduğu, hacker kültüründe ise baskın olan etik değerinin "özgürlük, tutku, toplumsal değer, şeffaflık, duyarlık, etkinlik ve yaratıcı olma" olduğu görülmektedir.

Castells göre, ağ toplumu iki mantık sistemi içerisinde çalışmaktadır. Bunlar Kapsama ve dışlama. Yani düğümler faydasız hale dönüştüğünde ağlar, düğümleri bozarak ve verimli, yeni olanlarını eklemleyerek kendilerini yeniden dönüştürmeye yönelmektedir (Castells, 2005, s. 153).

Araştırmamızı bu doğrultuda değerlendirecek olursak, ortaya çıkan teknolojik gelişmelerden ötürü enformasyon çağı insanlığa "Ağ Toplumu" nu ortaya çıkarmıştır.

Enformasyonel devrimlerin meydana gelmesindeki alt yapı internet ve bilgisayar olmaktadır. Enformasyonel devrimlerdeki ticari boyut ise yeni iş türleri alanı, yeni güçlü ve büyük şirketler olarak karşımıza çıkmıştır. Başka bir ifadeyle enformasyonel devrimler, kendini yeniden üreten ve büyük şirketlere (Apple, Microsoft, Dell Compter, Cisco Systems, oracle, Sun Microsystems, vs.) evrilenler sayesinde olmuştur. Bu temel unsurun hem yenilikçi hem de yaratıcı hacker kültürünü temsil eden bir kültürün kaynağı üzerine yapılandırıldığını görülmüştür. Ancak süreç ilerlediğinde kapitalist sistemin kuvvetlenmesi ile bir anlamda ağ toplumunun yaratıcısını "Ağ" dışına itmiş ve dışlamıştır. Bunun nedeni ise, hacker kültürünün etik anlayışı, ağ toplumundaki egemen anlayışından (dönüşen, gelişen ve güçlenen Protestan etiği) farklılık arz etmekle kimyalarının uyuşmadığı anlaşılmaktadır. Bu sebeple ağ toplumunun yarattığı eşitsizliğe, baskın olmaya çalışan egemen anlayışa karşı direniş kimliği çevresinde örgütlenerek toplumsal hareketlere katılmışlardır. Bu direniş biçimlerini, yaşamdaki pratiklerinde "özgür yazılım" "açık öğrenme modeli" ve "açık kaynak kod" organizasyonları ile günümüz çağına meydan okuyarak muhalif bir tavır gösterdikleri değerlendirilmiştir (Sandilaç, 2020, s. 72).

Hackerların açık öğrenim modelinin geniş perspektifte değerlendirmeye çalıştığımızda, tüm çalışma ve iş alanlarında örnek olabileceği düşünülmektedir. Bu doğrultuda, bu mantalite etrafında "net akademisi" kurmak için kullanılabilir. Bu şekilde etik anlayış ve bu öğrenim modeliyle ağa yeni düğümler eklemlenerek yaratıcı kaynaklar üretilebilir.

Pratikte "Özgür yazılım" ve "Açık Kaynaklı Kod" biçiminde hayata yansıyan eylemlerin aslında ağ toplumunda farklı alanlarda da nasıl uygulanabileceği hususunda düşünmeye iterek yol haritası çizmiştir. Bu doğrultuda hackerların zarar vermeden yaptıkları etkili ve güçlü muhalif pratiklerine bakıldığında sadece terörist, siber suçlu ve tüm görülen siber suçların, tek sorumlusunun hackerlar olduğu düşüncesine indirgenemeyeceği değerlendirilmektedir.

Günümüzde hackerların niyetleri şapka renklerine göre sınıflandırıldığı görülmüştür. Bu anlamda araştırmamıza konu hacker kültürü ve etiğinin aslında beyaz şapkalı hacker kategorisinde değerlendirilmektedir.

Hacker gruplarını aynı kategoride değerlendirmek mümkün olmamıştır. Kimileri ideolojiden, kimileri hacker etik ilkelerinden, kimileri de devlet yanlısı gruplardan oluştukları görülmüştür. Örneğin Anonymous, Redhack gibi grupların merkeziyetsiz, örgüt lideri olmayan ideolojilerden beslendiği görülürken, Ayyıldız TIM gibi grupların devlet yanlısı, milliyetçi bir tavır sergiledikleri görülmüştür. Ancak şunu da belirtmek gerekir ki hacker grupların hangi tarafta bulunurlarsa bulunsunlar kim için yaptıklarına göre suç/suç olmayan şeklinde bir değerlendirilmeye tabi tutulmamalıdır.

Aktivizmi, internet ve bilişim teknolojileri ile evrimleştiren ve siber alana yerleştiren dijital aktivizmin günümüzde her formu ile kendini hayatımızda gösterdiği görülmektedir. Bu anlamda dijital aktivizmin bir şekli olan hacktivizm de tüm devletlerde olduğu gibi Türkiye'de de yeni bir kavram olarak gündeme oturmuştur. Siyasi sebepler ile internet üzerinden siber protesto veya siber saldırı eylem şeklinde yapılan hacktivizm, bireysel tepkinin siber biçimine dönüştüğü görülmektedir.

Sonuç olarak ister bireysel siber suç ister örgütsel siber terörizm suçu, isterse de hackerlerın pratiğe dökülmüş eylemleri olsun teknolojik devrimler toplumsal yapıyı dönüştürmüş, zaman ve mekanı aşan, sanallık kültürü inşa eden ağ toplumu ortaya çıkmıştır. Hem devletler yönünden hem de kapital sistem yönünden her ne kadar yapılanma gayreti içerisinde girmiş iseler de istikrarsızlıkla baş edilememiş ve toplumsal eşitsizlikler nedeniyle gruplar, toplumlar bir nevi dördüncü dünyaya hapsedilmişlerdir. Bu nedenle ağ toplumundaki meşruiyet savaşları toplumsal meydan okumalar yeniden yapılanan kimlikler üzerinden ifade edilmesi öne çıkmıştır. Bu anlamda suç ve terörizm boyut değiştirmiş, dünyanın iktidar erklerine karşı yapılan bu savaşlar kullandıkları silah, metot ve elde edilen sonuçlara göre kimileri siber suçlu, siber terörist kapsamında değerlendirilmiş kimileri de hacker kültürünün bir parçası olmuştur.

Çalışmamızda tüm hackerların birer günahsız olarak nitelendirilmesi ya da tüm eylemlerinin bilişim suçları kapsamının dışında tutulması gerektiği anlaşılmamalıdır. Bu çalışmamızda enformasyon toplum biçimlerine karşı bir eleştiriyi beraberinde getirdiğine dikkat çekmiştir.

Hacker kültürü, demokratik eylemleri bakımından siber suç ve siber terörizmden ayrılarak, bu yeni etik anlayışı, günümüzdeki topluma hakim olan etik anlayışına karşı güçlü bir meydan okuma olarak değerlendirilmiştir. Bu çerçeveden bakıldığında hacker kültürü, karşı kültür açısından toplumsal yapının temeline karşı ciddi bir direniş kimliğini temsil etmektedir.

KAYNAKÇA

Akarslan, H. (2012). *Bilişim Suçları.* Ankara: Seçkin Yayıncılık.

Akdeniz, G. (2013). Hacker Etiği. A. R. Keleş, Y. Sal, & (der) içinde, *Hack Kültürü ve Hacktivizim: Yeni Bir Siyaset Biçimi.* İstanbul: Alternatif Bilişim.

Akman, T. (2003). *Sibernetik: Dünü, Bugünü, Yarını.* İstanbul: Kaknüs Yayınları.

Akmeşe, Z., & Deniz, K. (tarih yok). Dijital Aktivizm olarak Video Aktivizm: Redhack Belgeselleri. Yeni Medya Çalışmaları II. Ulusal Kongre. https://www.academia.edu/11425974/D%C4%B0J%C4%B0TAL_AKT%C4%B0V%C4%B0ZM_OLARAK_V%C4%B0DEO_AKT%C4%B0V%C4%B0ZM_REDHACK_BELGESELLER%C4%B0 adresinden alındı

Altınok, T., & Kaya, Z. (2009). Siber Tehditlerle Mücadele. H. Çakmak, & T. Altunok içinde, *Suç, Terör ve Savaş Üçgeninde Siber Dünya.* Ankara: Barış Platin Kitabevi.

Altunok, E., & Vural, A. F. (2011). Bilişim Suçları. *Denetişim*(8).

Arseven, C. (2013, 06 29). *Hacker romantizmi*. 03 15, 2020 tarihinde www.hurriyet.com.tr: https://www.hurriyet.com.tr/ adresinden alındı

Avşar, Z., & Öngören, G. (2010). *Bilişim Hukuku.* İstanbul: Türkiye Bankalar Birliği Yayınları.

Aydın, E. D. (1992). *Bilişim Suçları ve Hukukuna Giriş.* İstanbul: Doruk Yayınları.

Ayyıldız TIM Tarihi. (tarih yok). www.ayyildiz.org: https://www.ayyildiz.org/ayyildiz-tim-tarihi.html adresinden alındı

Balcıoğlu, İ. (2014). İnternet Kullanımı ve Getirip Götürdükleri. *Somuncubaba Dergisi*, 66-67.

Bauman, Z. (2018). *Küreselleşme Toplumsal Sonuçları.* (A. Yılmaz, Çev.) İstanbul: Ayrıntı Yayınları.

Bektaş Şeker, T. (2005). *İnternet ve Bilgi Açığı.* Konya: Çizgi Kitapevi Yayınları.

Biber, A. (2000/8). Küresel Dünyada Gelişen İnternet ve Değişen Halkla İlişkiler. *G.Ü. İletişim Dergisi*.

Bilton, T., Bonnett, K., Jones, P., Lawson, T., Skinner, D., Stanworth, M., & Webster, A. (2009). *Sosyoloji.* (K. İnan, Y. Kartal, N. Özkale, K. Toroman, Y. Özkan, & A. Güngen, Çev.) Ankara: Siyasal Kitabevi.

Bozkurt, A. (2014). Ağ Toplumu ve Bilgi. *Türk Kütüphaneciliği Dergisi, 18*(4).

Bozkurt, V. (2000). *Küreselleşmenin İnsani Yüzü.* İstanbul: Alfa Yayınları.

Budak, Ö. S. (2015). Bilişim Öğrencilerinin Siber Suç Farkındalığı: Erzurum İli Mesleki ve Teknik Liseler Örneği. *Yüksek Lisans Tezi*. Erzurum.

Burkay, S. (2008, Ekim). Teorik Çerçevede Suç. *ETHOS: Felsefe ve Toplumsal Bilimlerde Diyaloglar*(2/4).

Castells, M. (2004). Ağda Küreselleşme, Kimlik ve Toplum-Calhoun, Lyon ve Touraine'e Cevap! M. Armağan (Dü.) içinde, *Küresel Kuşatma Karşısında İnsan* (Ş. Yalçın, Çev.). İstanbul: Ufuk Kitap Yayınları.

Castells, M. (2005). *Enformasyon Çağı: Ekonomi, Toplum ve Kültür - Ağ Toplumunun Yükselişi.* İstanbul: İsanbul Bilgi Üniversitesi Yayınları.

Castells, M. (2005). Enformasyonculuk ve Network Toplumu. H. Pekka içinde, *Hacker Etiği, İş Hayatına Yıkıcı Bir Yaklaşım* (Ş. Kaptan, Çev.). İstanbul: Ayrıntı Yayınları.

Castells, M. (2007). *Enformasyon Çağı: Ekonomi, Toplum ve Kültür - Binyılın Sonu.* İstanbul: İstanbul Bilgi Üniversitesi Yayınları.

Castells, M. (2008). *Enformasyon Çağı: Ekonomi, Toplum ve Kültür - Kimliğin Gücü.* İstanbul: İstanbul Bilgi Üniversitesi Yayınları.

Castells, M. (2008a). *Enformasyon Çağı: Ekonomi, Toplum ve Kültür - Ağ Toplumunun Yükselişi* (2 b., Cilt 1). İstanbul: İsanbul Bilgi Üniversitesi Yayınları.

Castells, M. (2008b). *Enformasyon Çağı: Ekonomi, Toplum ve Kültür - Kimliğin Gücü* (2 b., Cilt 2). İstanbul: İstanbul Bilgi Üniversitesi Yayınları.

Çağıltay, K. (1997). *İnternet.* Ankara: METU PRESS.

Çakmak, H., & Demir, C. K. (2009). Siber Dünyadaki Tehditler ve Kavramlar. H. Çakmak, & T. Altunok içinde, *Suç, Terör ve Savaş Üçgeninde Siber Dünya.* Ankara: Barış Platin Kitabevi.

Çeler, Z. (2012). Manuel Castells ve Ağ Toplumu İdeoloji Olarak Enformasyon. *İleti-ş-im, 0*(17).

Çiftçi, H. (2013). *Her Yönüyle Siber Savaş.* Ankara: Tubitak Popiler Bilim Kitapları.

Çiftçi, İ. (2015). *Avuçlarımızda Titreyen Dünya: Küreselleşme.* İstanbul: Vadi Yayınları.

Demirkıran, P. (2013). Hacktivizm. A. R. Keleş, Y. Sal, & (der) içinde, *Hack Kültürü ve Hactivizm: Yeni Bir Siyaset Biçimi.* İstanbul: Alternatif Bilişim .

Dilber, F. (2014). Kitle İletisim Araçları ve Suç Olgusu. *KMÜ Sosyal ve Ekonomik Arastırmalar Dergisi*(Özel Sayı 1).

Dülger, M. V. (2014). *Bilişim Suçları ve İnternet İletişim Hukuku.* Ankara: Seçkin Yayınları.

Erbay, Y. (2011, Bahar). Küreselleşme Sürecini Anlamaya Yardımcı Bazı Kavramlar. *İletişim ve, Kuram ve Araştırma Dergisi*(32).

Erdağ, A. İ. (2010). Bilişim Alanında Suçlar (Türk ve Alman Ceza Hukukunda). *GÜHF Dergisi Doç. Dr. Mustafa Yıldız'ın Anısına Armağan, XIV*(2).

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

Ergün, İ. (2008). *Siber Suçların Cezalandırılması ve Türkiye'de Durum.* Ankara: Adalet Yayınevi.

Ergün, İ. (2008). *Siber Suçların Cezalandırılması ve Türkiye'de Durum.* Ankara: Adalet Yayınevi.

Eriş, U. (2009). Türkiye'de Kırıcı (Hacker) Kültürü. *Doktora Tezi*. Eskişehir.

Ferligül Çakılcı, E. (2014). Sanal Uzamda Bir Direniş Pratiği: Hacktivizm. https://www.academia.edu/9047530/Sanal_Uzamda_Bir_Direni%C5%9F_Prati%C4%9Fi_Hacktivism_Eda_Ferlig%C3%BCl_%C3%87ak%C4%B1lc%C4%B1 adresinden alındı

Friedman, T. (2002). *Lexus ve Zeytin Ağacı Küreselleşmenin Geleceği.* (E. Özsayar, Çev.) İstanbul: Boyner Yayınları.

Gallas, W. (...). Cezalandırılabilirliğin Temelleri ve Sınırları (Suç Kavramı Üzerine Düşünceler). (İ. ÖZGENÇ, Çev.) *Selçuk Üniversitesi Hukuk Fakültesi Dergisi, 4*(1-2).

Giddens, A. (2000). *Elimizden Kaçıp Giden Dünya.* (O. Akınhay, Çev.) İstanbul, İstanbul: Alfa Yayınları.

Giddens, A. (2018). *Modernliğin Sonuçları.* (E. Kuşdil, Çev.) İstanbul: Ayrıntı Yayınları.

Gökdemir, O. (Eylül 2013). *RedHack Sanal Alemin Klavyeli Asileri* (7 b.). İstanbul: Destek Yyaınevi.

Göker, G., & Doğan, A. (2011). Ağ Toplumunda Örgütlenme: Facebook'ta Çevrimiçi Tekel Eylemi. *Balıkesir Üniversitesi Sosyal Bilimler Enstitüsü Dergisi, 14*(25).

Güçdemir, Y. (tarih yok). Enformasyon Toplumu ve Küreselleşme. *İletişim Fakültesi Dergisi*.

Gümüş, Ç. (2008). Bilişim Suçlarıyla Mücadelede Polisin Eğitimi. *Doktora Tezi*. Elazığ.

Hacker Sırları. (2009). *PCnet, Bilgisar ve İnternet Dergisi*.

Hamza, E. (2011). *Hacking İnterface.* İstanbul: KODLAB.

Harford, T. (2008). *Görünmeyen Ekonomist.* (S. Demirel, Çev.) İstanbul: Pegasus Yayınları.

Hekim, H., & Başıbüyük, O. (2013). Siber Suçlar ve Türkiye'nin Siber Güvenlik Politikaları. *Uluslararası Güvenlik ve Terörizm Dergisi*(4), 137.

Held, D., & McGrew, A. (2008). *Küresel Dönüşümler: Büyük Küreselleşme Tartışması.* Ankara: Phoenix Yayınları.

Helvacıoğlu, A. D. (2004). İnternet ve Hukuk. Y. M. Atamer içinde, *İnternet ve Hukuk.* İstanbul: İstanbul Bilgi Üniversitesi Yayınları.

Himanen, P. (2005). *Hacker Etiği, İş Hayatına Yıkıcı Bir Yaklaşım.* (Ş. Kaptan, Çev.) İstanbul: Ayrıntı.

Hirst, P., & Thompson, G. (2007). *Küreselleşme Sorgulanıyor.* (E. Yücel, & Ç. Erdem, Çev.) Ankara: Dost Kitabevi.

https://sozluk.gov.tr/. (tarih yok).

İnan, A. (2000). *INTERNET El Kitabı.* İstanbul: Sistem Yayıncılık.

Jargon File Version 4.4.6. (2003). http://jargon-file.org/archive/ adresinden alındı

Kara, M. (2013). Siber Saldırılar-Siber Savaş ve Etkileri. *Yüksek Lisans Tezi*. İstanbul.

Kaya Erdem, B. (2010, Aralık). Siber Sığınak "Ağ Toplumunun Yalnızlaşan Bireyinin Kendini İfade Etme Mecraları ve Biçimleri "Farmville Örneği". *Akdeniz İletişim Dergisi*(14).

Kaypak, Ş., & Haytoğlu, M. (2016). Küreselleşme Sürecinde Toplumsal Hareketler ve Kente Yansıması. *Süleyman Demirel Üniversitesi Sosyal Bilimler Enstitüsü Dergisi*(CİEP Özel Sayısı).

Kazgan, G. (2000). *Küreselleşme ve Ulus-Devlet.* İstanbul: Bilgi Üniversitesi Yayınları.

Keskin, İ. (2007). Bilişim Suçları. *Adalet Dergisi*(29).

Kongar, E. (2002). *Küresel Terör ve Türkiye.* İstanbul: Remzi Kitapevi.

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

LulzSec. (tarih yok). wikipedia: https://en.wikipedia.org/wiki/LulzSec adresinden alındı

Mahmutoğlu, F. S. (2013). Türk Ceza Kanununda Yer Alan Bilişim Alanındaki Suçlar ve Karşılaşılan Sorunların Yargı Kararları Işığında Değerlendirilmesi. *Prof. Dr. Füsun Sokullu - Akıncı' ya Armağan - İstanbul Üniversitesi Hukuk Fakültesi Mecmuası,, LXXI*(1).

Malkoç, İ. (2007). *Açıklamalı İçtihatlı Yeni Türk Ceza Kanunu* (Cilt 2). Ankara: Malkoç Kitapevi.

Özcan, M. (2004). Siber Terörizm ve Ulusal Güvenlik. Y. M. Atamer içinde, *İnternet ve Hukuk.* İstanbul: İstanbul Bilgi Üniversitesi Yayınları.

Özgenç, İ. (2006). *Türk Ceza Kanunu Gazi Şerhi (Genel Hükümler)* (3 b.). Adalet Bakanlığı Yayını.

Özkan, T. (2006, Ağustos). Siber Terörizm Bağlamında Türkiye'ye Yönelik Faaliyet Yürüten Terör Örgütlerinin İnternet Sitelerine Yönelik Bir İçerik Analizi. *Yüksek Lisans Tezi*. Anadolu Üniversitesi Sosyal Bilimler Enstitüsü.

Özkışlalı, G. (2008). Küreselleşme, İnternet ve Terörizmin Değişen Yüzü; Siber Terörizm. *Yüksek Lisans Tezi*. Ankara.

Özkul, D. (2002, Ocak-Haziran). Bilişim Sistemi Kavramı ve Bilişim Sistemlerinin Denetimi. *Sayıştay Dergisi*(44-45), 14.

Raymond, E. (2008). *Nasıl Hacker Olunur?* (Y. Şentürk, Y. Kolukısa, & N. Yücel, Çev.) http://docs.comu.edu.tr/howto/hacker-howto.html adresinden alındı

Robertson, R. (1999). *Küreselleşme toplum kuramı ve küresel kültür.* (Ü. H. Yolsal, Çev.) Ankara: Bilim ve Sanat Yayınları.

Sabancı, A. (2013). Hackerlara bir karşı kültür olarak bakmak. A. R. Keleş, Y. Sal, & (der) içinde, *Hack Kültürü ve Hactivizim: Yeni Bir Siyaset Biçimi.* İstanbul: Alternatif Bilişim.

Sandilaç, N. (2020). Ağ Toplumunda "Ağ" Dışı Kalan Hackerların Muhalefet Biçimi: Hacker Etiği ve Özgür Yazılım. *Sosyal ve Kültürel Araştırmalar Dergisi, 6*(12).

Satılmış, E. (2006). TCK'da Yer Alan Bilişim Suçları. *İstanbul Barosu Dergisi, Ceza Hukuku, Özel Sayı*(1).

Sert, N. Y. (2012). Online Aktivizm Araçları Yoluyla Oluşturulan Etkilerin Metafor Kullanılarak Açıklanması Örnek Olay İncelemesi: "İnternetime Dokunma" Eylemi. *Akdeniz Üniversitesi İletişim Fakültesi Dergisi*(17).

Sertoğlu, S. (1999, Aralık 6). Temmuz 7, 2018 tarihinde Sabah: http://arsiv.sabah.com.tr/1999/12/06/y11.html adresinden alındı

sitemizin çizgisi. (tarih yok). https://www.cyber-warrior.org/: https://www.cyber-warrior.org/ adresinden alındı

Suveren, Y. (2017). Küreselleşme, İnternet ve Yeni Suçlar: Siber Dünya ve Siber Suçlar. *SUÇ SOSYOLOJİSİ* (s. 160-195). içinde Eskişehir: Anadolu Üniversitesi Basımevi.

Taş, O. (2007). Şebeke Toplumunda Direniş: Hacker Kültürü ve Teknoloji Etiği. M. Binark içinde, *Yeni Medya Çalışmaları.* Ankara: Dipnot Yayınları.

Taşçı, U., & Can, A. (2016). Türkiye'de Polisin Siber Suçlarla Mücadele Politikası: 1997-2014. *Fırat Üniversitesi Sosyal Bilimler Dergisi, 25*(2).

Turak, Y. (2014, 02 08). RedHack Özelinde Siber Olaylar ve Siber Suçlar. *Türk Hukukunda Bilişim Suçları ve Uygulaması Dersi Projesi*. İstanbul: İSTANBUL BİLGİ ÜNİVERSİTESİ.

Uçkan, Ö. (2013). Dijital Aktivizimin Sınır Boyunda Hactivizm:Anonymous ve RedHack Örnekleri. A. R. Keleş, Y. Sal, & (der) içinde, *Hack Kültürü ve Hacktivizm: Yeni Bir Siyaset Biçimi.* İstanbul: Alternatif Bilişim.

Yayla, M. (2014). Siber Savaş ve Siber Ortamdaki Kötü Niyetli Hareketlerden Farkı. *Hacettepe Hukuk Fakültesi Dergisi, 4*(2).

Yazıcıoğlu, R. Y. (1997). *Bilgisayar Suçları: Kriminolojik, Sosyolojik ve Hukuksal Boyutları ile.* İstanbul: Alfa Yayınevi.

Yegen, C. (2014). Dijital Aktivizmin Bir Türü Olarak Hactivizm ve "RedHack". *E-Journal of Intermedia, 1*(1).

Yenidünya, A. C., & Değirmenci, O. (2003). *Mukayeseli Hukukta ve Türk Hukukunda Bilişim Suçları.* İstanbul: Legal Yayıncılık.

Yıldırım, A., & Şimşek, H. (2011). *Sosyal Bilimlerde Nitel Araştırma Yöntemleri.* Ankara: Seçkin Yayıncılık.

Yılmaz, B., Dündar, G., & Oskay, T. (2015). Dijital Ortamda Aktivizm: Online İmza Kampanyalarına Katılım Davranışlarının İncelenmesi (Kocaeli Üniversitesi İletişim Fakültesi Öğrencileri Üzerine Bir Araştırma). *Intermedia International E-journal, 2*(2).

Yüksel, H. (2014). Şaşı Bakıp Şaşırmak: Enformasyon Toplumu Kuram ve Politikaların Toplumsal Barış ve Adalet Açısından Eksiklikleri. *4. Uluslararası Gazimağusa'da İletişim ve Medya Çalışmaları Konferansı.* Kuzey Kıbrıs.

ÖZGEÇMİŞ

Nurullah Sandilaç lisans öğrenimini ise Sakarya Üniversitesi Fen-Edebiyat Fakültesi Sosyoloji bölümünde tamamlamış ve aynı üniversitenin Eğitim Fakültesi'nden Pedagojik Formasyon Eğitimi belgesini almıştır. Yüksek Lisans eğitimini ise Sakarya Üniversitesi Sosyal Bilimler Enstitüsü Sosyoloji Anabilim Dalı'nda Dr. Yaşar SUVEREN danışmanlığında tezli olarak gerçekleştirmiştir.