Hacktivizm ve Toplum Mühendisliği Üzerine Bir İnceleme

Necati Duran[1], Özgü Can[1]

[1] İzmir Üniversitesi, Bilgisayar Mühendisliği Bölümü, İzmir

[2] Ege Üniversitesi, Bilgisayar Mühendisliği Bölümü, İzmir

necati.duran@izmir.edu.tr, ozgu.can@ege.edu.tr

Özet: Bu çalışmada son yıllarda giderek toplumda daha fazla karşılık bulan Hacktivizm ve, aslen ne bağlam ne de teknik olarak herhangi bir benzerliği olmasına rağmen, toplum nezdinde yaratılan yanlış bilinçten dolayı Hacktivizm ile karıştırılan Toplum Mühendisliği kavramları ele alınmıştır. Hacktivizm kavramının ortaya çıkışı ve gelişiminden bahsedilmiştir. Toplum Mühendisliği yöntemleri (aldatmacalar) ve bunlara karşı alınabilecek önlemler tartışılmıştır. Aynı zamanda bu çalışmada, hack kültürünün tüm dünyada çarpıtılmış bir kavrama indirgenmesinin eleştirisi yapılmaya çalışılmış ve toplumda oluşan negatif algının değiştirilmesi hedeflenmiştir.

Anahtar Sözcükler: Hacktivizm, Toplum Mühendisliği, Sosyal Mühendislik, RedHack, Anonymous

Abstract: This study attempts to deal with Hacktivism -a concept which is gradually claiming a place in society in recent years- and Social Engineering, which is confused with Hacktivism due to the false consciousness manipulated by society. In fact, the two concepts have nothing in common, neither contextually nor technically. The emergence and development of Hacktivism are taken into consideration. Social Engineering methods (tricks) and the measures to be taken against them are discussed. Meanwhile, the study aims at evaluating the debased conceptualisation of hack culture throughout the world and adjusting the negative perception of the concept.

1. Giriş

Hacklemek kavramı bilgisayara yetkisiz erişim veya kullanımı tanımlamaktadır. Hacktivizm kavramı ise hacklemek (hacking) ve aktivizm (activism) kavramlarından oluşmuştur. Politik olarak gerekçelendirilmiş hackleme eylemine karşılık gelmektedir. Crackleme (Craking) kavramı kriminal (criminal) ve hackleme (hacking) kavramlarından oluşmuş ve kötü niyetli hacklemeyi ifade etmektedir. Toplum mühendisliği ise bunlardan farklı olarak, bilgisayar sistemleri yerine onları kullanan özneleri hedef alan aldatmaca tekniklerinin tümüne karşılık gelmektedir [1]. Akademik analizlerin ve basın raporlarının çoğunda hackleme, crackleme ve hacktivism kavramları aynı şekilde değerlendirilmiş ve siberterörizmin birer varyasyonu olarak ifade edilmiştir [2].

Toplum mühendisliği insanları bazı eylemleri yaptırmak veya güvenli bilgileri ele geçirmek için kullanılan tekniklerin bütünüdür. Dolandırıcılığa benzemekle birlikte bilgileri ele geçirmek veya bilgisayar sistemlerine erişmek için hile yapmak ve insanları kandırmaktır. Toplum mühendisleri, çoğu durumda hedef ile yüz yüze veya birebirde bir iletişim kurmaktadır. Bireyler nadir durumlarda yönlendirildiklerini fark etmişlerdir [3].

Hacklemenin karışıklığa sebebiyet veren doğasından kaynaklı 'doğrudan Ağ politika eylemi' (direct action Net politics) veya 'elektronik sivil itaatsizlik' diğer çevrimiçi politik aktivizm biçimlerinden farklıdır. Politik siteler, çevrimiçi imza kampanyaları, e-mail iletileri, çevrimiçi tartışma grupları toplumsal hareketler ve politik örgütler tarafından örgütlenme,

lobicilik ve iletişim araçları olarak kabul edilmiştir. İnternetin bu şekildeki kullanımı, politik aktivistlerden tarafından bilgisayarlı aktivizm olarak kabul edilmiştir. Hacktivizm bunlardan farklıdır. Çünkü hacktivistler interneti basitçe bir iletişim kanalı olarak görmezler. İnternetin aynı zamanda çok önemli bir eylem alanı olduğunu kabul etmişlerdir. Hacktivist hareket ortak bir amaç ekseninde ortak bir yöntemle birleşmiştir. Küreselleşmeden, şifreleme teknolojilerinin kısıtlanmasından ve Latin Amerika'daki siyasi baskıdan kürtaja, elektronik gözetim tekniklerinin yayılmasına ve çevrenin korunmasına kadar hacktivist bir eylem alanına dikkat çekmişlerdir. Hacktivistler bu nedenle internet vatandaşlarının üstlendiği tekno-özgürlükçü gündemden daha geniş politik bir tayfa yayılmaktadır [2].

Toplumda hack kültürünün bilinmiyor olması ve ana akım medyanın gerek yaptığı haberler gerekse kullandığı dil sebebiyle, hacktivistler ve toplum mühendisleri birbiri ile karıştırılmaktadır. Daha doğrusu, toplum mühendisleri hackerlar olarak bilinmektedir. Gerçekte hackerlardan bihaber olan toplum, toplum mühendislerinin saldırılarını hack eylemleri olarak bilmektedir. Çalışmanın ilerleyen bölümlerinde bu kavramlardan daha detaylı bahsedilmiştir. Genel olarak Hacktivizm kavramı ve bu kavramın alt başlıkları değerlendirilmiştir. Toplum mühendisliği tanımlanmış ve toplum mühendisliği saldırılarından bahsedilmiştir. Daha sonra bu saldırılar karşısında alınabilecek önlemler tartışılmıştır. Son olarak bu kavramların birbirinden farklı konulmaya çalışılmıştır.

2. Hacktivizm

2.1 Hacktivizm Kavramları

Hacktivizm kavramı son yıllarda daha çok duyduğumuz bir kavram olsa da, kendisi teknoloji ile ilintili olarak ortaya çıkmıştır. Dolayısıyla bu kavramın ortaya çıkışı ve gelişimi teknolojinin gelişimi ile paralel gitmektedir. Öncelikle hacktivizim'in ilk halleri olarak anılabilecek Bilgisayarlı aktivizm kavramından bahsedilmelidir. Bilgisayarlı aktivizm bir eylem biçimi olmaktan daha ziyade, varolan eylemlere yani aktivizme dijital ortamda verilen destek gibi düşünülebilir. 1980'lerde yaşanan dijital aktivizm daha çok bilgi vermek veya iletişim kurmak için kurulan haber gruplarına karşılık gelir [4]. 1990'lı yılların ortalarına doğru, şu an bizim için hayatımızın bir parçası olan, internetin viral bir etkiyle yayılması dijital aktivizm tanımını değiştirmeye başlamıştır. Artık bilgisayar becerilerine sahip aktivistler, tepkilerini ifade edecekleri yeni kanallar keşfetmeye uğraşmışlardır. Bilgisayarın sadece iletişim amaçlı değil, doğrudan eylem ve hareket yeri olarak kullanılabileceğinin farkına varmışlardır [4]. Bu zamanda, hacktivizmin ilk hali ile karşılaşılmıştır. İlk hacktivist eylemlerden biri, Meksika yerlilerinin başkaldırısına destek amaçlı olmuştur. Bir grup aktivistin hazırladığı yazılım ile hedef internet sitesi geçici olarak işlevsiz hale getirilmiştir. İsteyen herkes bu yazılımı indirerek eyleme destek olabilmiştir [2].

Hacker kavramı TDK'daki anlamıyla “bilgisayar korsanı”, ”bilgisayar ve haberleşme teknolojileri konusundaki bilgisini, gizli verilere ulaşmak, ağlar üzerinde yasal olmayan zarar verici işler yapmak için kullanan kimse” olarak tanımlanmaktadır [5]. Ancak, hacker kavramının gerçek anlamını bulabilmek için, öncelikle hacker'ın kökü olan hack kavramının ortaya çıkışına değinilmiştir. MIT (Massachusetts Institute of Technology) Üniversitesi'nde öncelikle öğrencilerin yaptıkları zekice kurgulanmış şakaları ifade etmek için kullanılmıştır. Daha sonrasında buna ek olarak, üniversitedeki teknik konular üzerine toplanmış bir öğrenci kulübünün teknik problemlere getirdiği yaratıcı ve başarılı çözümler için söylenen söz olarak kullanılmıştır. Çok kısa bir süre sonra ilk anlamını kaybedip ve de kulüp içerisinde yaşanan anlaşmazlıklardan ve MIT kampüsündeki bilgisayarların kullanımına dair yapılan düzenlemelerden kaynaklı bu kavram bilişim alanına doğru bir yönelim geliştirmiştir [6].

MIT'de milyon dolarlık bilgisayarların ucuzlayıp laboratuvarlarda

üniversite öğrencileri tarafından kullanılmaya başlamasıyla öğrenciler arasında yazılı olmayan kurallar gelişmiştir. Bilgisayar kullanıcıları, aynı zamanda yazılımı yapan kişilerdir. Bu kişiler programlanan şeritlerde ihtiyaçlarına uygun programları geliştirip kullandıktan sonra, çalıştıkları yerde bırakarak başkalarının da kullanmasına olanak sağlamışlardır. Bilgisayarlarda yapılan donanımsal veya yazılımsal iyileştirmeler, geliştirmeler amaçlananı en iyi şekilde karşılıyorsa buna "hack" denmeye başlanmıştır. Yaş, cinsiyet veya herhangi bir başka şey hesaba katılmadan bu eylemi yapan kişiler "hacker" olarak tanımlanmıştır. [4]

Sisteme yetkisiz olarak erişim eylemi ise "crack" ve bunu gerçekleştiren kişi veya kişiler "cracker" olarak adlandırılmaktadır. Kelime olarak ve sonrasında da bilişim dünyasındaki karşılığına bakıldığında; kırmak, yıkmak gibi anlamları içermektedir. Bir örnek olarak, ücretli yazılımların anahtarlarının kırılması ve kullanılması eylemini tariflemektedir. [7] Hacker kavramı özellikle anaakım basın/medya tarafından sıklıkla kötüleyici bir anlamda kullanılmıştır. [8] Bazıları bunun akla yatkın olduğunu düşünse de, birtakım insanlar bunun saldırgan bir anlam olduğunu düşünmektedir. Anaakım medyada, hacker kavramı sıklıkla kötü niyetli güvenlik kırıcı (malicious security cracker) olarak kullanmaktadır. [7] Hacker ve Cracker kavramlarının ayrım noktasını, hacker tanımlaması yapılırken kullanılan "malicious security cracker" ifadesi koyabilir. Oldukça açık bir şekilde hacker kavramının tanımlanıldığı iddia edilirken, aslında cracker kavramı anlatılmaktadır.

2.2 Hacker Kültürü ve Etiği

Geçmişten günümüze kadar hackerların gerçekleştirdikleri eylemlere bakıldığında; tutkuyla merak eden, öğrenemeye doyamayan, öğrenmek ve merakını gidermek için farklı şeyler deneyen, tüm çabasını bilginin açığa çıkması ve insanlara ulaşması için harcayan insanları görebiliriz. Hackerlar genel olarak bilgiyi deşifre etmeye çalışırlar. Tüm eylemleri bilginin birilerinin tekelinde kalmaması ve insanlara ulaşması amacıyla gerçekleştirilmektedir. Hackerların kriminalize edilmesi, bu bilgilerin açığa çıkmasından rahatsızlık duyan güç odaklarının çabasıdır [4].

Hackerlara bir hareketin veya sıradan bireylerin ötesinde bakmamızın sebebi, bu eylemleri yapan insanların yaptıklarıyla bizlere sıradan insanlar olmadıklarını göstermeleridir. Eğer sadece bir hareket veya bir eylem olsaydı, yaptıkları sadece o anlık ve hayatlarına etki etmeyen birer eylemden öte olmazdı. Fakat bir kültür sadece bir anlık davranışta değil, bireylerin hayat felsefesinde kendini göstermektedir. Yaptıkları bir bakıma kendilerini ifade etmenin bir biçimi olmaktadır. Hacker kültürünü anlamak için öncelikle ilk hacker manifestolarına göz atmakta fayda var. İlk olarak The Mentor'un meşhur Hacker Manifestosu'ndan [4] bir ifade:

> *Evet, bir suçluyum. Suçum meraklı oluşum. Suçum insanları nasıl göründükleri yerine söyledikleri ve düşündükleriyle yargılamak. Benim suçum sizleri zekamla alt etmek, beni asla affetmeyeceğinizi bildiğim bir şey.*
>
> *...*
>
> *Bu artık bizim dünyamız...elektronun ve devre anahtarlarının dünyası... saniyede akıp giden veri birimlerinin güzelliği. Çıkar peşinde koşuşan açgözlülerin elinde olmasaydı son derece ucuz olabilecek, zaten mevcut olan bir hizmeti para ödemeden kullanıyoruz. Keşfe çıkıyoruz... ve sen bize suçlu diyorsun. Bilgiyi arıyoruz... ve sen bize suçlu diyorsun. Bizim ten rengimiz, milliyetimiz, dinsel bağlantılarımız yok... ve sen bize suçlu diyorsun. Sen atom bombaları yapıyor, para için savaşlar çıkarıyor, öldürüyor, hile yapıyor ve bizi bütün bunları kendi iyiliğimiz için yaptığına inandırmaya çalışarak yalan söylüyorsun... hala biz suçluyuz. Evet ben*

suçluyum. Suçum merak.

İkinci olarak Richard Stallman'ın On Hacking [9] yazısından:

> *Hacklemek olarak adlandırdığımız şeye basit bir tanım koymak çok zor, ancak bence bu eylemlerin ortak noktası oyunculuk, zekayı kullanmak ve araştırmacılık. Bundan yola çıkarsak, hacklemek mümkün olanın limitlerini oyuncu bir zekayla sınamaktır diyebiliriz. Bu oyuncu zekayı gösteren eylemlerin hepsi "hack değeri" taşır.*

Son olarak Linus Torvalds'tan [10]:

> *Hacker, bilgisayarını hayatta kalmak için kullanmaktan, diğer iki aşamaya geçmiş kişidir.*

Son alıntıdan başlayacak olursak; burada Torvalds'ın ifade ettiği *diğer iki aşama* yazısında tanımlamış olduğu Linus yasasında mevcuttur. Torvalds, insan yaşamının hayatta kalmak, toplumsallaşma ve eğlence şeklinde üç aşamadan oluştuğunu söyler. Stallman'dan yapılan alınıtıya baktığımızda yapılan eylemin sıradan, basit veya kötü niyetli bir eylemden çok keşfetme dürtüsünden yola çıktığı görülebilir. Ve son olarak, ilk verilen alıntıya değinilirse; The Mentor, bilgi açlığı ve zekanın ötesinde bir yere gönderme yapmaktadır. Hacklemenin asıl amacına, yani bilginin özgürleşmesi ve bu sayede toplumsal olan bilginin tekrar topluma iade edilmesine değinmektedir.

İlk hackerlar ABD'nin akademik ortamlarını tanımış üniversite öğrencileri olmuştur. Burada benimsenmiş bir Açık Akademi Modeli'nden bahsedilebilir. Bu model araştırmada bulunmak isteyen herkesin katılımına açık, tutkulu olan herkesin katkı sunabileceği, test edebileceği ve sürece müdahale edebileceği günümüz bilimsel araştırma yöntemine benzer bir yapıyı ifade edilmektedir. Bu tarz bir yöntemle yetişmiş insanların bilginin kısıtlanmasına, sadece seçilmişlerin erişimine açık olmasına sessiz kalabileceklerini düşünmek büyük bir hayal kırıklığı olurdu.

Bu yetişmiş kültüre bakıldığında, hackerlık bazı etik kuralları beraberinde getirmektedir. Hacker etiğini 3 farklı aşamada incelenmiştir. Birinci kuşak hackerlar, ikinci kuşak hackerlar ve üçüncü kuşak hackerlar. İlk kuşak hacker etiği, ilk hackerların ortaya çıktığı MIT bünyesinde, hackerların birbirleri arasındaki ilişkiyi düzenleyen değerler olarak görülebilir. Bu değerler [6] listelelendiğinde;

1. *Bireyler sistemlerin nasıl işlediğini bilmelidir.*
2. *Bilgi özgürdür.*
3. *Otoritenin getireceği baskıdan korunmak için bilgi gayri merkezi bir yapıda olmalıdır.*

gibi ifadeleri içermektedir. Bu kuşak bilginin toplumsallaşmasını merkezine almış ve bu bağlamda eylemlerde bulunmuştur. İkinci kuşak hackerlar ilk kuşağın etiğini benimsemiş ve buna ek olarak başka değerleri eklemişlerdir. Fakat bu kuşakta ilk kuşak etiği çok belirgin olmamıştır. Bu grup 1980'li yıllarda kişisel bilgisayarların, mikro bilgisayarların yerini aldığı zamanlarda ortaya çıkmaktadır [6].

1. *Hiçbir koşulda zarar verme.*
2. *Kişisel bilgisayarlar özel yaşamlara ait bilgi barındırıyor olabilir. Bu bilgi kesinlikle korunmalı.*
3. *Sınırları zorlayın, keşfedin.*
4. *İletişim temel bir haktır.*
5. *Elde ettiklerinizi paylaşın.*
6. *Kendinizi koruyun.*
7. *Hack sistemlerin güvenliklerini iyileştirir.*

İkinci kuşağın etik değerlerine baktığımızda değişen teknoloji, kişisel bilgisayarlara yönelim beraberinde değişen bir toplumu ve değişen bir anlayışı getirmektedir. Bunun tersi de geçerlidir, toplum ve teknolojinin değişimi arasında diyalektik bir süreç işlemektedir [6]. Bu değişim ilk kuşaktan başlamış ikinci kuşakta çok daha belirgin hale gelmiştir. Üçüncü kuşak ise özgür yazılım ve açık kaynak hareketinden oldukça etkilenmiştir [6]. Bu hareketler ile ilk kuşak etiğinin geri döndüğü kabul edilebilir. Bu gelişimde internetin etkisi göz ardı edilemez.

Bu kuşağın hareketi şirketlerce geliştirilen teknolojinin yarattığı sorunlara yanıt olarak da düşünülebilir. Richard Stallman'ın GNU - GNU's not Unix[11] hareketinin içerisinde tanımlanan prensipler üçüncü kuşak etiğin yazılı hali olmuştur. Bu üçüncü kuşakta etik değerler birinci kuşağı barındırmış ve ikinci kuşağın aksine pratikleriyle buluşturmuştur. Bunlarla birlikte kendilerinden sonra gelecekler için bir model oluşturmuşlardır. Günümüz iş dünyasında kendine yer edinmeye çalışan bir kısım için de "etik hack" [6] kavramını eklemekte fayda vardır. Bu, ikinci kuşağın prensiplerinin iş dünyasında uygulayarak yapılan eyleme gönderme yapmaktadır. Aslında yapılan şey "etik crack" olmaktadır.

2.3 RedHack ve Anonymous Örnekleri için Değerlendirme

Anonymous ve RedHack gibi isimleri sık sık duymaya başladık. Peki hacktivizm denilen şeyden ne kadar haberdarız ve bu isimlerle hack eylemleri yapanlar neyi amaçlıyor? Bunlar kim? İşin aslı, sorulacak çok fazla soru vardır. Çalışmanın bu kısmında bu örnekler üzerinden hacktivizm kavramı tartışılmıştır.

Daha önce de belirttiğimiz gibi, hacktivizm bilgisayarlı aktivizmin bir türü olarak karşımıza çıkmaktadır. Düşüncelerini paylaşmak için sokağın yetmediğini düşünen birilerinin gerçekleştirdiği, sokağı ve dijital dünyayı birleştiren bir eylem biçimi olarak anılmaktadır [8]. Anonymous örneğinde görülebileceği gibi; bu grup başta eğlence amaçlı eylemler yapmak için bir araya gelmiş insanlardan oluştuğunu ifade etmiştir. Şu anki haline bakıldığında artık eğlenceden daha öte, toplumsal ve politik bir yanı olduğunu söyleyebiliriz. Yapılan eylemlerde hedeflenen şey toplumsal bir olaya dikkat çekmek olduğu için internetin etkin bir şekilde kullanılması gerekmektedir. Bu etkin kullanım ile kamoyu yaratılması sağlanmaktadır. Bu noktada hacktivizmi; bilgisayarların, programalama becerisinin ve internetin toplumsal bir soruna yönelik tepki gösterilmesi için kullanılması olarak tanımlayabiliriz. Anonymous kendini hacktivist bir grup olarak tanımlamamaktadır. Ve bir lideri yoktur. Daha çok bir fikir etrafında gelen insanlardan oluşmaktadır. Bu oluşum uzun süreli bir yapıdan ziyade bir toplumsal sorun karşısında din, dil, ırk, yaş, cinsiyet gibi herhangi bir şey göz etmeksizin bir araya gelen insanların birlikte bir eylem yapması olarak düşünülebilir. Bunu Anonymous'un kendi tanıtımından [12] bir kesit ile daha iyi ifade edebiliriz:

> *Anonymous aslında birlikte kısa bir yolculuğa çıkan insan topluluğu denilebilir - işe giderken otobüste veya trende tanışan kişiler gibi: Kısa süreliğine hepimiz aynı rotadayızdır, aynı amacı, hedefi veya beğenmeme durumunu paylaşırız. Ve birlikte çıktığımız bu kısa yolculukta belki dünyayı değiştirebiliriz.*

Bu bireyler yaptıkları kısa yolculuktan sonra dağılıp belki bir daha tekrar bir araya gelmeyeceklerdir. Geldiklerinde bile yine anonim kimlikleri ile hareket edeceklerdir. Anonymous, Scientology'nin [13] yayınlanan bir videoyu telif hakları sebebiyle kaldırtması üzerine, birkaç kişinin Scientology'ye eğlence amaçlı sataşmasıyla başlayan bir akımdır [14]. Bu akım her geçen gün daha fazla kişinin katılımı ile eğlenceden daha toplumsal ve politik olaylara yönelik eylemler düzenlemeye doğru ivme kazanmıştır. Aynı anda farklı yerlerde farklı toplumsal sorunlar için bir araya gelen ve eylem yapan Anonymous'lar olabilmektedir. Anonymous'un özü de işte tam burada kendini göstermektedir. Teknolojinin gelişmesine rağmen ilk yapılan hack eylemlerinde kullanılan DDos [15] (distributed denial of service -dağıtık hizmet akstama) saldırıları gerek çok teknik bilgiyi ihtiyaç duyulmaması gerekse sivil itaatsizliğin internet ortamında uygulanabilir hali olması bakımından halen rağbet görmektedir.

Anonymous gibi yapılarda hacktivist eylemleri gerçekleşirenlerin tüm zamanını bilgisayar başında geçiren ve bilgisayardan başka uğraşı olmayan 'sivilceli ergen' tanımıyla hiç uyuşmayan bireyler olduğuna dikkat çekmek gerekiyor. Tüm bireylerin üst düzey programlama becerisine sahip olması gerektiği düşüncesi de büyük bir

yanılsamadır. Bu bireyleri birkaç grup altında toplayabiliriz. İlk grup, gerçekten de sayısı çok fazla olmayan ileri seviye programlama becerisine sahip bireylerden oluşmaktadır. Bu bireyler siber uzayın öncüleri kaşifleri olarak da anılabilir. İkinci grup, hacker kategorisinde olmayıp hacktivist eylemlerde görsel tasarım gibi desteklerle katkıda bulunan ve 'geek' olarak anılan kategoridir. Son grup, bilgisi ve fikri olmadan bu sürece dahil olmaya çalışan bireyleri ifade eder ve kendilerini geliştirmeleri için diğer bireylerin yardımı ile 'geek' kategorisine dahil olabilirler. 'Lamer' denilen grup ise nasıl çalıştığını anlamadan an az direktif ile bir şeyler yapmaya çalışan kesimi ifade eder. [6]

The Mentor'un 1986 yılında yayınladığı Hacker Manifestosu dünyanın her yerinde duyulmuş ve yavaş yavaş etkisini göstermiştir. Bu manifesto Türkiye'de o zamanlardan itibaren karşılık bulmaya başlamıştır ve bu karşılıklardan biri de, yakın zamanda yaptığı eylemlerle adını duyuran RedHack olmuştur. RedHack, benzer eylemleri ve benzer tutumları olsa da, Anonymous'un aksine farklı bir yapı olarak hareket etmektedir. Uzun süredir hacktivist eylemlerde bulunuyor olmalarına rağmen, son yıllarda çok daha fazla tanınır hale gelmiştir. Bu durumun iki açıdan açıklaması yapabilir. Birincisi, yapılan eylemlerin toplumda daha çok yer edinir olmasıdır. İkinci olarak da, toplumun hacker algısı daha pozitif bir yöne doğru kaymaya başlamasıdır. Bu durum diyalektik bir süreç olduğundan, bu sebepler birbirinden ayrı düşünülemez.

Toplum tarafından destek görecek eylemler, hem tanınırlığı hem de toplum algısını olumlu yönde değiştirmektedir. Toplumdaki bu pozitif yöndeki kırılmanın İçişleri Bakanlığı'nın hacklenmesi ile gerçekleştiği söylenebilir [8]. Her ne kadar teknik olarak basit bir eylem olsa da, hem hedef alınan kişi/kurumlar hem de elde edinilen bilgiler sebebiyle toplum tarafından epey destek görmüştür. Bu kabul görmüşlük sosyal medyada yazılanlardan rahatlıkla okunabilir. Bu durum RedHack'ten istek eylemlere kadar gitmektedir. Gerek söylemlerinde aldıkları nükteli tutum gerekse dillendirdikleri toplumsal sorunlar sebebiyle giderek daha da tanınır hale gelmektedir. İyi bir sosyal medya yönetimine sahip olduklarının hakkını vermek gerekmektedir. Tanınırlıklarını bir nebze de sosyal medyayı iyi kullanıyor olmaları sağlamaktadır. Yaptıkları eylemleri takip edenler biliyordur, yakın zamanda yaptıkları iki eylem örneğini verebiliriz. Bu sayede eylem tarzlarının ve amaçlarının neler olduğu daha iyi anlaşılabilir. Bunlarda ilki, son günlerde yaşanan döviz yükselişi karşısında Merkez Bankası'nın sitesini (tcmb.gov.tr) hacklemeleridir. Ve bunu nükteli bir şekilde Twitter ortamında duyurmuşlardır [16]. Bu eylemde hem toplumsal soruna dikkat çekmek için yapılmış eylemi hem de toplumla kurulan iletişim şeklini görebiliriz. İkinci olarak, son günlerde haberlerde daha çok duymaya başladığımız “çocuk gelin” veya diğer bir ifadeyle çocuk tecavüzü olarak adlandırılan toplumsal soruna dikkat çekmek için Aile ve Sosyal Politikalar Bakanlığının sitesinin hacklenmesidir. Sitede bu toplumsal soruna değinen açıklamalar [17] yayınlamalarıdır. Bu örnekte de göreceğiniz üzere yine toplumsal bir meseleye dikkat çekme çabaları olmuştur.

3. Toplum Mühendisliği

3.1 Toplum Mühendisliği Kavramları

Toplum mühendisliği kavramı 1800'lü yılların sonunda modern çalışanlar yaratma düşüncesi ile ortaya çıkmıştır. Daha sonrasında toplumu yeniden inşa etmek, toplumsal sorunlara yönelik çözümler getirmek veya tam aksi bir düşünceyle, kitlesel hareketlerin yoğunlaştığı zamanlarda kitlenin manipule edilmesi gibi amaçlarla iki farklı doğrultuda ABD (Amerika Birleşik Devletleri) ve SSCB (Sovyet Sosyalist Cumhuriyetler Birliği)'de ortaya çıkmıştır. ABD'de kitleleri savaşın gerekliliğine ve özgürlüğün savaş sonrası kazanılacağına inandırmak için yapılan çalışmaları kapsamıştır [18]. SSCB'de ise Çarlık Rusyasının toplumsal yapısı yerine Sovyet devrimi ile oluşturulmak istenen yeni toplumsal yapının inşası sırasında ortaya çıkan çalışmalardır [19].

Toplum mühendisliği sosyal bir

disiplin olup devletler veya herhangi bir özel yapı/kurum/kimse tarafından uygulanan; toplumsal davranışları, tutumları ve kaynakları geniş çapta etkilemek için sarf edilen çabaların tümü olarak ifade edilebilir. Toplum mühendisliği, bilimsel yöntemleri sosyal konular üzerinde uygulama olarak da anılabilir. Toplum mühendisleri bu yöntemleri toplumu anlamak ve analiz etmek için kullanan kimselerdir. En güvenilir ve anlamlı çıktıları alabilmek için güvenilir istatistiksel verilerle ve en gelişmiş tekniklerle ile çalışılması gerekmektedir. Toplum mühendisliği, toplumların refah ve özgürlük düzeylerini arttırmak için toplumsal yapının yönetimine uygun tasarımlar geliştiren veri tabanlı bilimsel bir sistem olarak düşünülebilir.

Kavram, çok çeşitli sebeplerden dolayı kötü anlamlarıyla anılır olmuştur. Bunun da temel sebepleri gerek devletlerce gerek özel veya resmi kurumlar gerekse kişiler tarafından başka amaçlar için kullanılmasıdır. Bunların en başında toplumun istenildiği gibi yönetilmesi veya başka bir ifade ile, ABD örneğinde olduğu gibi, devletlerin topluma meşrulaştırmak istedikleri konularda toplumun belleğini ve kararını etkilemek için kullanılmıştır. Toplum mühendisliğinin belirli bir aracı yoktur. Probleme özgü araçlar kullanılabilir. Bunlar gazete veya internet gibi herhangi bir iletişim aracı olabilir. Bir başka toplum mühendisliği, reklam şirketleri gibi yerlerde kimi şirketlerin kârını arttırma amaçlı kullanılan toplumu etkileme yöntemleri olmuştur. Bu çalışmada üzerinde duracağımız kötü anlam kazanmış bağlam ise bilişim alanıdır.

Toplum mühendisliği bilişim alanındaki bağlamıyla düşünüldüğünde, kabaca, toplum mühendisliği yöntemlerinin bilişim alanında uygulanması olarak ifade edilebilir. Burada, kötü niyetli kişiler, bu yöntemleri erişim haklarının olmadığı kişisel bilgilere erişebilmek için bireyleri manipule etmede kullanmaktadır. Bu noktada, bu alandaki toplum mühendisleri, bilgi güvenliğindeki en zayıf halka olan bireyleri kullanarak erişim haklarının olmadığı bilgileri hedef alırlar. Toplum mühendisliği saldırıları çoğunlukla teknolojiden çok psikolojiden yararlanmaktadır [1]. Toplum mühendisliği günümüzde insanları aldatma sanatı olarak ifade edilmektedir [20].

3.2 Saldırılar

Genel olarak toplum mühendislerinin ilk yaptıkları şey saldırılarını gerçekleştirecekleri kişi ve kurumlarla bir güven ilişkisi kurmak olur. Daha sonra bu güven mekanizması kullanılarak çeşitli yardımcı bilgilere erişmeye çalışırlar. Edinilen bu yardımcı bilgileri de genellikle sistemde güvenlik kontrolü sırasında karşılaşacakları bir sorunun cevabı veya bir şifre veya bunlara benzer bir şey olabilmektedir. Bu aşamadan sonrası ise sadece bilgiye erişmek olacaktır. Dahası, toplum mühendisliği kötü amaçlı yazılımlardan daha zarar vericidir. Çünkü sadece sisteminizi değil sizi hedef alır. Bunları bir örnek üzerinde inceleyebiliriz. Bir şirketin insan kaynaklarında yeni işe başlamış bir çalışanın hikayesi [20]:

> ***Yardımsever Andrea***
> *-İnsan kaynakları, Andrea Colhaun.*
> *-Andrea, merhaba, ben Alex; Şirket Güvenliği'nden*
> *-Evet?*
> *-Bugün işler nasıl?*
> *-İyi. Sizin için ne yapabilirim?*
> *-Yeni başlayanlar için bir güvenlik semineri düzenliyoruz ve deneme için birkaç kişiyi bir araya getirmemiz gerekiyor. Geçen ay işe başlayan herkesin adlarına ve telefon numaralarına ihtiyacım var. Bana bu konuda yardımcı olabilir misiniz?*
> *Tabi ki olabilirdi.*

Bu saldırı incelendiğinde yapılan şey yeni başlamış birinin bilgisizliğinden yararlanıp, ihtiyaç edinilen bilgiye kolayca erişilmiştir. Bunların dışımda toplum mühendisliğinde; bir çalışan gibi davranmak, yetkili biri gibi davranmak, yardıma ihtiyacı olan biri gibi davranmak, e-posta ekiyle truva atı göndermek, bedava yazılıma truva atı gizlemek, kurbana içine truva atı gizlenmiş bir CD vermek (Oyun CD'sine mesela), kullanıcının yeniden MSN adresini ve

şifresini girmesini sağlayacak sahte bir pencere kullanmak (Fake Mail) gibi birçok yöntem sıralanabilir. Bunlarla birlikte, sahte öykülerle kandırma ve e-dolandırıcılık gibi farklı tekniklerle gerçekleştirilen saldırılar olmaktadır. Birçok farklı tipteki aldatmaca, günümüzde çevrimiçi güvenliği tehdit eden bir sorun haline gelmektedir. Bu tehditler parolaları ele geçirmekten finansal işlemleri yönlendirmeye kadar varabilir. Toplum mühendisliği saldırılarının temelindeki en büyük tehdit parolalar içindir. Kazara veya aldatmaca ile parolanın ele geçirilmesi tüm sistemi yıkacak sorunlara yol açabilir. Sistemlere sızmak için onları kullanan kişileri kandırmak giderek büyüyen bir yöntemdir fakat yeni değildir [1].

3.2.1 Sahte Öykülerle Kandırma (Pretexting)

Bu teknik daha çok güvenlik bilgilerinin sağlanacağı kişileri dil dökerek kandırmak, kendisini bir başkasıymış gibi tanıtmak ve gerekli bilgileri almak üzerine kuruludur. Ulaşılmak istenen bilgiyi doğrudan değil de, öncelikle o bilginin elde edilmesi için gerekli temel bilgileri elde etmek ve sonrasında bunları kullanarak elde eder. Çok temel bilgiler (doğum tarihi, kimlik numarası, doğum yeri, anne adı vb.) ulaşmanın kolay olduğunu düşünürsek bunları kullanarak bir çok şey yapılabilir. 1996'da sağlık mahremiyetine yapılan saldırıları tespit etmek için bir deney yapılmıştı [1]. Çalışanlar yetkisiz aramalar konusunda eğitilmişti. Örneğin aramanın nereden geldiğine bağlı olarak yetkili bir talep olup olmadığı tespit edilmeye çalışılmıştı. Bir hafta içinde 30 aldatma isteği tespit edilmişti.

Bir şirketin santralini atlatmanın ve insanların güvenini kazanmanın yolu pazarlama eğitimlerinde öğretilmektedir. Mitnick bu konuda bir uzman sayılabilir [20]. Yıllarca bu yöntemleri kullanarak şirketlerin güvenliklerini aldatmıştır. Sahte öykülerle kandırma yöntemi uzun zaman şirketler için kullanılmıştır. Son zamanlarda ise bireylere karşı kullanılma oranı giderek artmaktadır [1].

3.2.1 E-dolandırıcılık (Phishing)

Günümüzde en hızlı büyüyen çevrimiçi suç olarak e-dolandırıcılık bulunmaktadır. En sık yaşanılan biçimlerinden biri, e-mail yolu ile görünüşte tanıdığınız bir siteye yönlendirilerek parolanızın çalınmasıdır. Bu saldırı tekniği e-mail dışında telefon, web sitesi veya başka herhangi bir sistem üzerinden gerçekleştirilebilir. Türkçe'de e-dolandırıcılık olarak ifade edilebilen bu aldatmaca dolandırıcılığın çevrimiçi yapılan biçimidir. Bankanızdan gelen bir e-mail gibi görünerek kişisel bilgilerinizin ele geçirilmesidir. E-dolandırıcılık saldırıları 2003'ten itibaren başlamıştır. İlk örnekler taklit siteler olmuştur. Şimdilerde saldırganlar psikolojiyi daha etkin kullanmaktadırlar [1].

E-dolandırıcılık, şirketler için birçok yönden sahte öykülerle kandırmacadan daha zorlu bir problemdir. Şirket çalışanları yerine müşterileri hedef alan bu yöntem şirketler için başa çıkılması daha güç bir problem halini almıştır. Dolandırıcılar genel olarak iç kontrolün zayıf olduğu ve yüklü miktarda parayı hızlıca dışarıya taşıyacakları ve şüpheli ödemeleri kontrol etmesi zaman alacak bankaları veya kurumları tercih ederler [1].

Sahte öykülerle kandırma veya e-dolandırıcılık gibi tekniklerin dışında, bunlardan biçimsel olarak farklılaşan saldırı teknikleri bulunmaktadır. Bunlar; ilgi çekici yazılımlar, beliren pencereler, çöp karıştırma, casusluk ve gizli dinleme gibi teknikler olabilmektedir. İlgi çekici yazılımlar ile kullanıcıların bu yazılımları bilgisayarlarına yüklemesi sağlanmaktadır. Yazılım yüklendikten sonra truva atı ile sisteme sızma gerçekleştirilmektedir. Beliren pencere beklenmedik bir anda ekranın herhangi bir yerinde oluşarak, kullanıcın dikkatini dağıtabilmektedir. Toplum mühendisleri bu dikkatsizlikten faydalanarak hedefe istenilen eylemleri yaptırabilmektedir. Örneğin, bir internet bağlantısı kesintisi ile kullanıcı adı ve parolanın tekrar girilmesi ile kişisel bilgiler ele geçirilebilir. Çöp karıştırma tekniği, saldırganın kişisel bilgilerin geçmiş olabileceği herhangi bir belgeye veya sistem üzerindeki bir dosyaya ulaşmak için ulaşabildiği her yeri karıştırması olarak ifade

edilebilir. Casusluk ve gizli dinleme, e-mail, cd veya ücretsiz yazılımlar gibi herhangi bir kanaldan bilgisayarınıza casus yazılımların yüklenmesidir. Bu casus yazılımlar vasıtasıyla, klavyenizden girdiğiniz tüm veriler takip altına alınabilmektedir. Son zamanlarda bankaların kullandığı sanal klavyelere karşı da bir tehlike oluşmaya başlamaktadır. Bu güvenlik önlemini aşmak amacıyla ekran görüntüsü almak gibi teknikler ortaya çıkmıştır. Veya ağ bağlantınıza sızılarak, ağ üzerinden akan tüm verileriniz takip altına alınabilmektedir. Bu saldırı teknikleri artırılabilir. Fakat asıl dikkat edilmesi gereken, tüm bu teknikler ile bilgisayar sistemleri yerine kullanıcıların hedef alınması ve farklı bir biçimde aldatılmasıdır [3].

3.3 Genel Değerlendirme ve Önlemler

Toplum mühendisliği saldırılarından korunmak için alınacak temel önlemleri listeyebiliriz. Bunlar, kurum çalışanlarının yetkiler konusunda eğitilmesi, kişisel verilerin paylaşımı konusunda dikkatli davranılması için bireylerin bilgilendirilmesi olabilir. Veya telefon konuşmasında şüphelendiğiniz kişiyi geri aramak için bir numara istemeniz, talep edilen şeyin uygunluğu, aciliyete vurgu yapan kişilerden şüphelenilmesi. soru sorulduğunda karşı tarafın rahatsız olup olmadığına dikkat edilmesi, bilmediğiniz e-postaları ve eklerini açmamak, internetten bedava adı altında bulduğunuz her programı bilgisayarınıza kurmamak gibi birçok önlemden bahsedilebilir. Fakat bunların en temelinde bireylerin zayıflıkları olduğunu unutmamak gerekiyor. Dikkat edeceğiniz üzere tüm toplum mühendisliği saldırılarında ve önlemlerde temel kriter psikoloji olmaktadır. Dolayısıyla bireylerin kendilerini korumayı öğrenmeleri gerekmektedir. En iyi korunma yöntemi nelerden kaçınmanız, nelere dikkat etmeniz gibi konularda bilgilenmektir. [20]

Bilişsel psikoloji nasıl düşündüğümüz, nasıl karar verdiğimiz veya nasıl hatırladığımız gibi konularla ilgilenir. Saklanması gereken bir bilgi ile o bilgiyi saklamak için gerekli bilgi arasındaki denge çok kritik olmaktadır. Sistem tasarımcıları bu konuda zayıf kalmaktadır. Dolayısıyla psikoloji ve güvenlik arasındaki bu köprü üzerine daha çok eğilmek gerekmektedir. Bununla ilgili olarak George Miller'in bir araştırması bulunmaktadır. Bu araştırma kısa süreli belleğin eş zamanlı olarak kaç farklı seçenekle başa çıkabildiği üzerinedir. Bu çalışma seçenek sayısının yedi civarında (artı-eksi iki) olduğunu göstermiştir. Birçok sistem tasarımcısı ise seçenek sayısını beş civarında belirlemektedir. Çalışmalar bunun doğru bir tasarım olmadığını göstermiştir [1].

Bu alanda yaşanan sıkıntılar çoğunlukla tasarlanan sistem ile bireyler arasındaki uyumsuzluğu göstermektedir. Bireyler amaçlarına uygun hareket ederken, amacı gerçekleştirmelerinden sonra ortalığı derleyip toparlamadan gidebilirler. Buna örnek olarak ATM'leri düşünebiliriz. Para çekmeye odaklanmış birey, önce parayı sonra kartı veren ATM'de parayı aldıktan sonra kartını unutabilir. Bireyler arasındaki farklılıklar da tasarlanan sistemin kullanılabilirliğini etkilemektedir. Örnek olarak sistemlerin çoğu erkekler için tasarlanırken, bu sistemleri kullanan kadınların sayısı erkeklerden fazla olabilmektedir. Yapılan bir araştırma insanları iki grup altında sınıflandırmaya çalışmıştır. Bu gruplardan biri simgesel çıkarımlar yapma eğilimi gösterenleri, diğeri ise dil ve aynı anda birden fazla işlem yapma becerileri olanları temsil etmektedir. Bu çalışmanın sonuçlarına bakıldığında ilk gruptakilerin çoğunlukla erkek, ikinci gruptakilerin ise çoğunlukla kadın olduğu gözlenmiştir [1].

Sistem tasarımlarında öne çıkan bir güvenlik problemi de, parola belirleme konusudur. Parolanın hem hatırlanabilir hem de başkaları tarafından kolay tahmin edilemeyecek bir şekilde belirlenmesi gerekmektedir. Parola belirlenirken, isim, soy isim, doğum tarihi gibi tahmin edilmesi kolay olan veriler girmek en çok yapılan hatalardan biridir. İnsanlar sıklıkla kullanmadıkları veya sıklıkla değiştirdikler şeyleri hatırlamakta zorlanırlar. Güvenlik önlemleri alırken parola tek bir çözüm yolu değildir. Buna alternatif olarak bir uzaktan kumada gibi fiziksel araçlar kullanılabilir. Veya parmak izi tanıma

sistemleri olabilir. Parola gibi bir güvenlik önlemi alınıyorsa, kullanım limitleri koyulabilir. ATM'ler bunlara bir örnektir. Kartınızın şifresini üç defa yanlış girdiğiniz takdirde kartınız bloke olur veya kartınıza el koyulur. Sistem tasarlanırken sizden hatırlanması veya tahmin edilmesi zor bir parola seçmeniz ve o parolayı herhangi bir yere yazmamanız beklenir. Bu durum başlı başına bir paradokstur [1].

E-dolandırıcılık saldırılarına karşı alınabilecek güvenlik önlemleri farklı düzeylerde farklı tipteki araçlar olabilmektedir. Bunlara bir çok örnek verilebilir. Parola mengeneleri bunlardan bir tanesidir. Bu araç, tarayıcı üzerinde bulunan bir eklentidir. Kullanıcının giriş yapacağı sitenin alan adı ile gireceği parolayı harmanlayarak kendi içerisinde yeni bir parola üretip kullanmaktadır. Kullanıcı her defasında aynı parolayı kullansa bile farklı sitelerde farklı yeni parolalar üretileceğinden güvenlik arttırılmış olacaktır. Size tanıdıkmış gibi gelen bir site, gerçekte başka bir alan adına sahip olacağından üretilecek yeni parola doğru olmayacağı için bu tip bir e-dolandırıcılık saldırı önlenebilecektir. Bir başka örnek geçmişte kullanılmış kullanıcı bazlı sertifikalar veya özel uygulamalar olabilir. Geçmişte bankaların özel uygulamalarının olduğu floopy diskler ile herhangi bir bilgisayar bankaların terminalleri olarak kullanılabilmiştir. Bu yöntem günümüzde de benzer bir şekilde varlığını sürdürmektedir ve oldukça başarılı bir güvenlik mekanizması sağlamaktadır. Veya bir başka önlem yapılan işlemleri güvenli hale getirmek için bilgilerin şifrelenmesini sağlayan sertifikalardır. Bilgisayarınızda kullandığınız tarayıcınızı bir parola deposu haline getirebileceğiniz eklentiler bulunmaktadır. Rastgele parolalar üretmekte ve bunları belleğinde saklamaktadır. URL doğru olduğu sürece sizin adınıza giriş yapabilmektedir. Parolaların şifrelenmemiş bir şekilde saklanması durumunda güvenlik açığı oluşturabilmektedir. Bir başka araç bankaların favorisi olan sanal klavyelerdir. Dolandırcılar, henüz çok yaygın olmasa da, sanal klavye kullanımı sırasında ekran görüntüsü alabilecek yazılımlarla şifreleri ele geçirmeye çalışmaktadır. Bu gibi yöntemlerin dışında toplum mühendisliğinin asıl hedefi olan bireyleri veya müşterileri eğitmek de önlemlerden biri olabilmektedir [1].

Önümüzdeki yıllarda güvenlik ve psikoloji arasındaki ilişkinin büyük bir araştırma alanı olacağı düşünülmektedir. Bilgisayar bilimleri uzun yıllardır çalışılan bir alan olsa da, aklın anlaşılması henüz çok yeni ve bakir bir alandır. Beynin karmaşıklığı düşünüldüğünde bu alanda yapılacak çok şey olduğu söylenebilir [1].

4. Toplum Mühendisliği Yanılsaması Olarak Hacktivizm

Hacktivizm ve Toplum Mühendisliği bugüne kadar bilişim alanında, gerek bu disiplindeki kişiler gerekse bu disiplin dışındaki kişiler tarafından sürekli karıştırılan iki kavram olmuştur. Bu çalışmada hacktivizm konusundaki negatif algı değiştirilmeye çalışılmış ve hacktivizm olarak bilinen toplum mühendisliği kavramı ortaya konulmaya çalışılmıştır. Dolayısıyla toplum mühendisleri tarafından yapılanlar saldırı, hackerlar tarafından yapılanlar ise eylem olarak ifade edilmişlerdir. Bu temel fark, toplum mühendisliğindeki saldırıların amacının kişisel bilgilere erişim ve bunlar üzerinden kişisel çıkarlar(bilgileri satarak para kazanma, dolandırma vb.) sağlanması iken, hacktivizmde ise bir sistemi geçici olarak işlevsiz hale getirerek toplumsal bir soruna dikkat çekmek istenmesinden kaynaklanmaktadır. Toplum gözünde hackerlara olan negatif algı, Bu iki kavramın birbirine karıştırılması ve toplum mühendislerinin yaptıklarının hacktivism eylemleri olarak ifade edilmesinden doğmaktadır.

Ricardo Dominguez ve Stefan Wray, Meksika Hükümeti'ne “İnternet savaşı” açtıklarını deklare edene kadar, aktivist kimliklerini broşür dağıtmak veya politik slogan atmak gibi geçmişten gelen yöntemlerle Zapatista istyanlarına destek olarak kazanmışlardır. Daha sonra New Yorklular zulümden sorumlu tuttukları kişilerin veya kurumların sitelerine eylemde bulunmak için “sanal katılım” düzenlemişlerdir. Bu eylemler sırasında

şiarları, “Devrim dijital ortama aktarılacaktır” olmuştur. Ve Stefan Wray'ın “Bunu elektronik sivil itaatsizliğin bir biçimi olarak görmekteyiz” ifadesi ile hacktivizmin, artık toplumsal hareketlerin bir parçası ve bir eylem biçimi olduğu görülmektedir [21].

Hacktivistler interneti politik eylemleri için kullanmaktadır. Kendilerini gerçek dünyadaki eylemlerin internet ortamındaki temsilcileri olarak görmektelerdir. Örnek olarak, 1998'de İngiliz hackerlar, 300 web sitesini hackleyerek nükleer karşıtı içerikler yayınlamışlardır. 1990'ların ortalarından önce hackerların politik bağlantısını gösteren az sayıda kanıt olsa da, hacktivizm giderek büyüyen bir hacker kültürüdür [2]. Bugüne kadar yapılan eylemler ve saldırılar incelendiğinde, toplum mühendisleri daima kişisel bilgileri elde etmeyi amaçlarken, hackerlar eylemlerinde toplumsal sorunlara dikkat çekmeyi merkeze koymuşlardır. “*Gerçek Hacker'lar sanal bilgiler vasıtasıyla kişisel çıkarlar peşinde koşan, virüs yazan, veri hırsızlığı ya da soygunculuk yapan, kısaca devletlerin hayatın her alanında, elleri altlarındaki basın-yayın organlarıyla bize göstermek istedikleri suçlular değillerdir*” [4].

5. Sonuç

Hackerlar, yaşadığımız yabancılaşma sürecini tersine çevirmeye çalışan insanlardır. Artık üreten değil tüketen olduğumuz bu toplumda teknolojinin bilgisinden giderek uzaklaşarak bilmeden anlamadan sadece kullanan konuma geliyoruz. Bu kısır döngüyü kırmaya çalışan hackerlar, toplumsal çıkarları göz önünde bulundurmuşlardır. Çünkü üretimden tüketime geçen konumumuz sebebiyle yaşadığımız yabancılaşma bireyler üzerinde bir gözetim, denetim ve tüketim toplumu olarak tekrar tekrar karşımıza çıkmaktadır [6].

Daha önce bahsedildiği gibi Hacktivizm bir kültürdür. Ve bu kültür daha fazla özgürlük için bilginin, teknolojinin/tekniğin bilgisinin keşfedilmesini ve paylaşılmasını gerektirir. Bilginin önemi ve değeri gittikçe artmakta devletler ve şirketler onu ellerinde tutmak istemektedirler. Bilginin özgür olması bu gücün herhangi birinin elinde olmaması demektir. Hackerlar; militarize edilmiş, askeri sanayileri geliştirmekte kullanılan bilgiyi tüm insanlık için kullanılabilir hale getirmeye çalışan kimselerdir. Hacker, bilginin mülkiyetiyle varolan egemen sınıfların egemenlik alanlarına müdahele ederek, bilginin ekonomi politiğini sekteye uğratır ve bilgiyi anonimleştirir [4]. Bilginin korunabilmesi için hackerların çok net bir kuralı vardır: Ne olursa olsun, bilgi özgür olmalıdır [6].

Kaynaklar

[1] Ross J. Anderson, Security Engineering: A Guide to Building Dependable Distributed Systems.

[2] Maura Conway, Hackers as Terrorists? Why it Doesn’t Compute.

[3] Ashish Thapar, Social Engineering: An attack vector most intricate to tackle!

[4] McKenzie Wark, Bir Hacker Manifestosu

[5] www.tdk.gov.tr

[6] Hack Kültürü ve Hacktivizm, Alternatif Bilisim Dernegi, Temmuz 2013.

[7] Yogita Negi, Pragmatic Overview of Hacking & Its Counter Measures.

[8] Orhan Dökdemir: Sanal Âlemin Klavyeli Asileri: REDHACK. Destek Yayınevi. Şubat 2013. İstanbul.

[9] https://stallman.org/articles/on-hacking.html

[10] Pekka Himanen, Linus Torwalds, Manuel Castells, The Hacker Ethic and the Sipirit of the Information Age.

[11] http://www.gnu.org/

[12] http://www.youtube.com/watch?v=3isJzz7HKl8

[13] http://www.scientology.org/

[14] Steve Mansfield-Devine, Anonymous: serious threat or mere annoyance?

[15] Christos Douligeris, Aikaterini Mitrokotsa, DDoS attacks and defense mechanisms: classification and state-of-the-art.

[16] https://twitter.com/TheRedHack/statuses/423833940210626560

[17] https://twitter.com/RedVideos/statuses/423844534653841408

[18] Karl Popper: Political Philosophy, Internet Encyclopedia of Philosophy, http://www.iep.utm.edu/popp-pol/

[19] Slava Gerovitch, "New Soviet Man" Inside Machine: Human Engineering, Spacecraft Design, and the Construction of Communism.

[20] Kevin David Mitnick & William L. Simon, Aldatma Sanatı, Çeviri: Nejat Eralp Tezcan, ODTÜ Yayincilik.

[21] Amy Harmon, "Hacktivists" of All Persuasions Take Their Struggle to the Web, The New York Times, 31 October 1998.