# RedHack Özelinde Siber Olaylar ve Siber Suçlar

**Yazan: Yiğit Turak**

**08 Şubat 2014**

İçindekiler

Kısaltmalar ve Tanımlar

| **Kısaltma / Tanım** | **Açıklama** |
|---|---|
| DDoS | Dağıtık servis engelleme saldırısı (Distributed denial of service) |
| CERT | Siber Olaylarla Mücadele Birimi (Cybercrime Emergency Response Team) |
| XSS | Çapraz kod çalıştırma (Cross Site Scripting) |
| USOM | Ulusal Siber Olaylara Müdahale Merkezi |
| SOME | Siber Olaylara Müdahale Ekibi |
| Kaba kuvvet atak | Belirli koşullar çerçevesinde rastgele üretilen değerler ile yapılan ataktır. Özellikle kullanıcı girişlerinde şifreleri tespit edebilmek için yapılır. |
| Sözlük atak | Belirli bir sözcük listesindeki değerleri sırayla deneyerek yapılan ataktır. Özellikle kullanıcı girişlerinde şifreleri tespit edebilmek için yapılır. |
| Stuxnet | ABD ve İsrail'in, İran'ın nükleer çalışmalarını sekteye uğratmak için kullandığı solucan yazılımdır. |
| DNS | Alan adı sunucusu (DomainName Server) |

**Özet**
Bilişim teknolojilerinin hızla gelişmesi, bilginin anında tüm dünya ile paylaşılabilmesi bazı klasik suçların daha kolay işlenmesine imkân vermesinin yanında, yeni tip suçların da ortaya çıkmasını sağlamıştır. Günümüzde internetin sağladığı imkânlar sayesinde birçok insanın istediği bilgiye saniyeler içerisinde ulaşması veya bu bilgiyi paylaşabilmesi, insanların merak duygusunu ve bilginin özgür olması gerektiği düşüncesini tetiklemiştir. Bireylerin bu istek ve merakla, kişisel olarak veya bir araya gelerek çeşitli eylemlerde bulunmaya başladığı görülmüş ve siber suç kavramının ortaya çıkmasına neden olmuştur. Bilişim suçlar Türkiye'de, RedHack grubunun özellikle siyasi gündeme göre yapmış olduğu siber eylemeler neticesinde bu konuda farkındalığın artması gerektiğini ortaya koymuştur. Bununla beraber, bilişim teknolojilerine olan bağımlılığın giderek artması, devletin de birçok hizmetini elektronik ortama taşıması ve RedHack'in eylemleri neticesinde elde ettiği gizli bilgileri tüm dünyanın erişimine sunması, siber alanı da ulusal güvenliğin önemli bir parçası konumuna getirmiştir. Bu yüzden siber güvenlik ve RedHack son yıllarda en fazla tartışılan konulardan birisi haline gelmiştir. Ancak RedHack grubunun deşifre edilememesi, üyesi olduğu düşünülen kişiler hakkında farklı iddianameler hazırlanması Türkiye'de Bilişim Suçları konusuna gereken önemin verilmemesinden kaynaklandığını düşünmekteyim. Bu alandaki bilgi birikimine katkıda bulunmak amacıyla bu çalışmanın ilk bölümünde hacker kavramı ve RedHack grubu ele alınacak, ikinci bölümünde hacktivizm ve siber güvenlik politikaları, son bölümde ise RedHack eylemleri hukuki yönden incelenecektir.

**Anahtar Kelimeler:** RedHack, Hacktivizm, Siber Suç, Siber Güvenlik, Bilişim Hukuku

# 1 Giriş

Ülkelerin bilişim teknolojilerine ve özellikle internete olan bağımlılıkları her geçen gün artmaktadır. Dünya nüfusunun yaklaşık üçte ikisinin internet bağlantısı, %20'sinin sosyal ağlara üyelikleri ve Türkiye nüfusunun %49'unun aktif internet erişimi bulunmaktadır. Yine dünya nüfusunun %85'i cep telefonu kullanmakta ve bunların %15'i cep telefonlarıyla alışveriş yapmaktadırlar. Bu rakamlar bilişim teknolojilerine olan bağımlılığın ne derece arttığını göstermektedir. Bilişim teknolojileri, hayatı kolaylaştırma adına sağladıkları imkânların yanında, güvenlik boyutunda da yeni kaygıların gelişmesine sebep olmuştur.

Bu yeni dünyada, fiziksel temasa veya mağdurla aynı yerde bulunmaya gerek duymadan internet dükkânlarına erişimlerin engellenmesi, bilgilerin çalınması, hırsızlık, dolandırıcılık gibi suç fiilleri mümkün hale gelmiştir. Bunun yanında, bilişim teknolojileri suç gruplarının veya terör örgütlerinin iletişim becerilerini artırmış, propaganda imkânlarını güçlendirmiş ve yeni faaliyet sahalarının ortaya çıkmasını sağlamıştır. Belirli siyasi ve ideolojiyi görüşü benimsemiş, bu doğrultuda bilişim sistemlerine karşı eylemlerini gerçekleştiren topluluklar, bu toplulukların üye ve taraftar sayısı gün geçtikçe hızla artmaktadır. Toplulukların dünyadaki en bilindik örneği "V for Vandetta" maskesi ile de tanınan Anonymous grubudur. Türkiye'de ise özellikle Taksim Gezi Parkı protestoları ile popülerliği en üst seviyeye yükselten RedHack grubudur.

1997 yılında kurulmasına rağmen 2012 yılında Ankara Emniyet Müdürlüğü'ne karşı yaptığı eylem ile adını duyuran RedHack grubu; sahip olduğu bilişim sistemlerini, bilgi ve becerilerini kullanarak, kendi ideolojileri doğrultusunda hedef aldıkları sistemlerin içerisine sızıp propaganda mesajları bırakmak, gizli bilgileri ele geçirip basın ve sosyal ağlar vasıtasıyla yaymak, sistemleri erişilemez kılmak gibi eylemlerde bulunmaktadırlar. Ancak RedHack grubunun bir türlü deşifre edilememesi, üyesi olduğu iddia edilip gözaltına alınan kişiler hakkında bilişim suçları, terör örgütü gibi farklı iddianameler hazırlanması Türkiye'de Bilişim Suçları konusunun tam olarak netleştirilemediğini belirtmektedir.

Bu çalışmadaki ana amaç RedHack özelinde Bilişim Suçları ve Siber Güvenlik konusunu incelemektir. Çalışma içerisinde öncelikle, hacker kavramını, türlerini ve RedHack grubundan bahsedilmiştir. Çalışmanın ikinci bölümünde hacktivizm kavramı, dünyadaki örnekleri, RedHack grubunun eylemleri ve siber güvenliği sağlamak için uygulanan politikalardan bahsedilmiştir. Çalışmanın son bölümünde ise RedHack grubunun eylemlerinin bilişim suçları, bilişim araçları vasıtasıyla işlenen klasik suçlar, örgütlü suçlar ve terör suçları alanlarında hukuki incelemesine yer verilmiştir.

# 2 HACKER VE REDHACK

Gün geçtikçe daha fazla duymaya başladığımız hacker kavramını, çeşitlerini ve özellikle ülkemizdeki aktiviteleri ile gündemde sıkça yer alan RedHack topluluğunu bu bölümde inceleyeceğiz.

## 2.1 HACKER NEDİR VE TÜRLERİ NELERDİR?

Dünya literatürüne 1950'li yıllarda giren ve Türkçe'ye "*bilgisayar korsanı*" olarak çevrilen *hacker* kavramı 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 anlamına gelmektedir. Hacker topluluklarında kullanılan anlamı ise "teknolojinin orijinal, alışılmışın dışında, ustalıkla, yasadışı olarak ve özgün bir tarzda kullanan kimse" anlamına gelmektedir.
Basında ve halk arasında bilişim sistemlerine sızan, zarar veren, sistemin çalışmasına engel olan kişiler hacker olarak adlandırılsa da, aslında yaptıkları saldırı çeşitleri ve amaçlarına göre 7 farklı türü vardır.

1. **Beyaz Şapkalı Hacker:** Firmalarda güvenlik uzmanları olarak çalışan, sistemlere kötü niyetli bir saldırgan gözüyle sızmaya çalışan ve tespit ettiği güvenlik zafiyetlerini raporlayarak kapatılmasını sağlayan kişilerdir.
2. **Siyah Şapkalı Hacker:** Bilişim sistemlerinin güvenlik zafiyetlerini tespit edip bunlardan yararlanarak sistemlerin içerisine sızan, sistemin bütünlüğünü bozan, çalışmasına engel olan, gizli bilgileri ele geçiren kişilerdir.
3. **Script Kiddie:** Bu kişiler çoğunlukla sistemlere ve kişilere saldırmaya, hasar vermeye ve ele geçirdikleri bilgileri kötü amaçla kullanmaya çalışırlar. Özellikle internette kolayca bulunabilen çeşitli hazır programları ve araçları nasıl yapılacağını adım adım anlatan dokümanları okuyarak kullanırlar. Kullandıkları programın nasıl çalıştığını bilmezler ve teknik dokümanlardan anlamazlar.
4. **Hacktivist:** Kendi bakış açılarına göre güncel siyasi ve politik olaylara bilişim sistemlerini kullanarak tepki veren kişilerdir. Kendilerine göre karşı görüşlü bilişim sistemlerine girerek kendi isimlerini ve görüşlerini yazarlar veya bu bilişim sistemlerinin çalışmasını engelleyici faaliyetlerde bulunurlar.
5. **Devlet Destekli Hacker:** Devletlerin son zamanlarda kurmaya başladıkları siber ordular içerisinde yer alan, ülkenin bilişim sistemlerini koruyan ve gerektiği zaman devletin çıkarları doğrultusunda başka sistemlere sızan veya engelleyen kişilerdir.
6. **Ajan Hacker:** Firmalar tarafından rakip şirketlerin gizli bilgilerini, ticari sıralarını ele geçirmek için para ödeyerek tuttukları kişilerdir. Son yıllarda talep artışı sebebiyle hızları giderek artmaya başlamıştır.
7. **Siber Teröristler:** Siyasi ve politik açıdan kendilerini motive ederek, bilişim sistemlerine yaptıkları saldırılar ile toplumlar içerisinde korku ve kaos ortamı oluşturmaya çalışan kişilerdir.

## 2.2 REDHACK NEDİR?

R.H.A (Red Hackers Association) yani REDHACK 1997 Mayıs ayında "somut koşulların somut tahlili" ilkesinden yola çıkan teknoloji sektörünün bilişim ve iletişim kollarında alın teri döken yoldaşlar tarafından Türkiye'de kurulmuştur. Eylemlerine yön verecek esas merkez Türkiye olup; esas görevi, Türkiye Devrimci Hareketi'ne devrimin bilişim alanında, yardımcı olabilmek, Türkiye ve dünya proletaryasına ve ezilen halklara bir nebze olsun dayanışma gösterebilmektir.

RedHack topluluğunun 2006 yılında Atılım gazetesine verdiği röportajda kendilerini şu şekilde tanıtmaktadırlar; "O dönemde hack (kırmak) eylemleri, sadece şoven eylemlerle sınırlıydı. Bir kısım hacker zevki için veya popülist egoist kişiliklerini tatmin etmek için hacke başvuruyordu. Bir kısım hacker ise parasal durumlarından kaynaklı bu işe girişmişti. Yukarıda bahsettiğimiz hiçbir tanım, bizim kişiliğimize ve duruşumuza uymuyordu. Çünkü, bizlerin programlama ve hacking bilgisi dışında bir de dünya görüşümüz vardı. Bu, insanlığın ortak kurtuluşu olan bilimsel bir görüştü. Ve biz de bu görüş etrafında nasıl birleşebilirizi

araştırdık. Hackingi dünyanın kurtuluşuna; eşit, adil, sömürüsüz bir dünya kurulmasına nasıl sokabiliriz, diye düşündük. "Aynılar aynı yerdedir, ayrılar ayrı yerdedir" esprisinden hareketle Redhack'i Türkiye ve Kürdistan devrimine hizmet etmesi için, devrimci dayanışmanın bir ürünü olarak kurduk."

### 2.2.1 Topluluğun Yapısı

Kemik kadro olarak adlandırılan topluluğun ana kadrosu 12 kişiden oluşmaktadır. Kendilerini örgüt olarak anan RedHack grubu, topluluk içerisinde her devrimci görüşten kişiye yer vermekte olup, grup içerisinde kimse kimsenin ne olduğunu, nerde oturduğunu, adını, yaşını, hatta cinsiyetini bile bilmemektedir.

Topluluğun kendisine ait bir tüzüğü olup içerisinde; amaçları, üyelik kabul koşulları, üyelerin görev ve sahip olduğu haklar, üyelikten ayrılma, komite ve büroların yapısı ve mali kaynaklarından bahsedilmektedir.

"Halk için hack" sloganını benimsemiş olan RedHack topluluğu gelirlerini esasta illegal olmak üzere, devrimci duruşun rehberlik ettiği bir şekilde yeteneklerinden yararlanarak elde eder. Ayrıca toplulukta yer alan kişilerin yeteneklerine göre çeşitli komite ve bürolar yer almaktadır.

-Merkez Komite

-Siyasal Büro

-Basın ve Informasyon Bürosu

-Teknik Büro

-Enternasyonal Büro

-Hack Bürosu

-Askeri Komite

-Alt Grup Komitesi

### 2.2.2 Saldırı Yöntemleri

Saldırı çeşitliliğinin sınırsız olduğu bilişim alanında profesyonel kişi veya topluluklar tek bir tür yerine birkaç yöntemin bir arada kullanıldığı karışık ataklar yapmaktadır. RedHack grubu tarafından hiçbir zaman nasıl saldırı yaptıkları, ne tür yöntemler kullandıkları gibi bilgiler paylaşılmamaktadır. Bilgi Güvenliği alanındaki tecrübelerim ve eylemler konusunda yaptığım araştırmalar neticesinde bazı atak yöntemlerini tespit ettim.

RedHack'de ülkemizdeki özellikle web sitesi hackleme olarak adlandırılan eylemlerinde çapraz kod çalıştırma (XSS), SQL cümleciği sokuşturma (SQL injection) ve yama zafiyetleri gibi yöntemleri bir arada kullanarak saldırılar yapmaktadır. E-mail veya kullanıcı hesabı hackleme gibi eylemlerinde ise kaba kuvvet atak, sözlük atak gibi türler kullanmaktadır. Yakın zamanda yaptığı bazı eylemlerinde hem web sitelerin hacklenmesi hem de kullanıcı hesaplarının ele geçirilmesi ataklarını bir arada kullanarak bunların sosyal medyada yayılmasını sağlamışlardır. Bu saldırıların dışında bazı sistemlere ise dağıtık servis engelleme saldırıları (DDoS) düzenlemiş ve hizmet kesintilerine sebep olmuşlardır.

# 3 HACKTİVİZM VE SİBER GÜVENLİK

Özellikle ülkemizde RedHack grubunun yaptığı eylemler ile birlikte dilimize giren *hacktivizm* ve *dijital hacktivizm* kavramları ve bu hacktivist hareketlerin yanı sıra Stuxnet olayından sonra ülkelerin siber güvenlik konusunu gündeme almaları ve bu konuya ülkelerin bakış açılarının incelenmesi gerekmektedir.

## 3.1 DİJİTAL HACKTİVİZM VE EYLEMLER

**Hacktivizm**, yani bilgi özgürlüğü temelli "hacker etiği"nde kökünü bulan politik amaçlar için hack faaliyetleri olup, bu faaliyetlerde bilişim sistemlerin temel alınması ise **dijital hacktivizm**dir. Anonim, özel, devlet ve diğer iktidar odaklarının şeffaf olması gerektiğini savunarak bu faaliyetleri yürüten kişi ve topluluklara ise **hacktivist** denir. Tüm hacktivistlerin temel amacı, bilginin kimsenin tekelinde olmadığını gösterebilmektedir. Bu amaçla doğrultusunda kurulmuş hem ülkemizde hem de dünyada bir çok grup vardır.
Hacktivizm ile ilgili yaptığım araştırmalarda "Hack Kültürü ve Hacktivizm" isimli derlemede Pınar Demirkan'ın kaleme aldığı açıklama;

*"Hacktivizm kısaca; bilgisayar teknolojisinin veya programlama sistemlerinin toplumsal bir soruna yönelik tepki gösterme amaçlı kullanılmasıdır. Fakat şu şekilde daha afili alternatif tanımları mevcuttur: Alexandra Samuel'e göre hacktivizm; hack ve aktivizm kelimelerinin portmantosu ve yasal açıdan belirsiz araçların politik sonuçlar peşinden sessiz bir şekilde kullanılmasıdır. Prof. Dorothy 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."*

### 3.1.1 Dünyadaki Redhack Benzeri Yapılanmalar

Red Hack, anonymous, siber saldırı gibi kelimeleri sosyal medyada ve haberlerde sık sık duymaya başladık. Ülkemizdeki RedHack grubunun sık sık yaptığı eylemlerle siber güvenlik alanında insanlarımızın farkındalığı artmaya başladı ancak RedHack gibi dünyada yer alan ve çarpıcı eylemlere imza atan diğer hacktivist grupların neler olduğunu bilmemiz gerekmektedir. Dünyadaki RedHack benzeri topluluklar ve bazı eylemleri:

- **Anonymous:** RedHack topluluğundan temel farkı üyelerin siyasi ve toplumsal görüşlerinin homojen olarak dağılmış olmasıdır. Arap Bahar'ına destek anlamında Mısır ve Tunus harekatları, Türkiye'de Digiturk ve RTÜK'e DDoS saldırısı, Suriye Başbakanlığına ait e-mail yazışmalarının deşifre edilmesi gibi eylemlerde bulunmuşlardır.
- **Cyber-Warriors (Akıncılar):** Türk milliyetçi-muhafazakar kimliğinde, farklı bir tepkiyle devlet ve kamusal düzen adına hizmet veren siber hacktivist topluluktur. Cyber - Warrior ve Red Hack aynı eylem biçim ve tekniklerini kullanmaktadırlar. Akıncılar, devlet organlarını ve kamusal düzeni siber ortamda korumaya çalışan ve dahi devlet kuruluşlarına bilgi sağlayan siber aktivistlerdir. Aynı eylem biçimlerini kullanan iki karşıt topluluktan; Cyber-Warrior, Emniyet Teşkilatından destek hatta plaket alırken; Red Hack hakkında terör örgütü şüphesi ile hukuki süreç başlatılmıştır.
- **LulzSEC:** 50 günlük bir eylem planı yapan ve şirketleri, hükümetleri, genellikle toplumun ta kendisini ve bütün bu yapılar arasında kalan her şeyi, sırf yapabildiklerini göstermek ve insanları eğlendirmek için, yaptıklarını belirttiler. ABD'li yayıncı kuruluş PBS networkünü, Sony Pictures sitesini, FBI ile bağlantılı InfraGard sitesini ve Nintendo'nun networkünü çökerten gruptur.
- **The Jester:** Kendilerini yasallık sınırında eylemlerde bulunan ve gri şapkalı hacktivistler olarak tanımlamaktadırlar. Taliban, Wikileaks, Anonymous gibi grupların sitelerine saldıran topluluk LulzSEC grubuna yaptığı saldırı ile grup üyelerini deşifre etmiştir.
- **Milw0rm:** Hindistan'daki nükleer araştırma merkezindeki bilgisayarlara sızmayı başararak adını duyuran grup silahsızlanma ve anti-nükleer bir görüşü benimsemektedir. Ayrıca İngiliz yer sağlayıcı firma olan Easyspace firmasını hackleyerek 300 websitesine anti-nükleer mesajlar koymuştur.
- **Telecomix:** İnternet topluluğundan oluşan, ifade özgürlüğünü savunan ve sansüre ve kişisel hayata müdahaleye karşı direnen Telecomix, Suriye'deki telekomünikasyon kuruluşlarının ağlarını hackleyip ve gözetleme ağının önemli bir kısmını açığa çıkarmışlardır.

- **Electronic Disturbance Theater:** Meksika yerlilerinin başkaldırısına destek amaçlı internet üzerinden harekete geçmiş ve FloodNet adlı bir yazılım oluşturmuştur. Bu yazılımın amacı sanal oturumlar ile karşı taraftaki internet sitesini geçici bir süreliğine işlevsiz hale getirmekti.

3.1.2 Redhack'in Türkiye'deki Eylemleri

Dünyadaki belli başlı hacktivist grupların eylemlerinde genel olarak gördüğümüz ortak nokta güncel politik konulara karşı tepkilerdir. Türkiye'de de RedHack bu konuda en aktif ve kendini kanıtlamış topluluktur. Aşağıdaki tabloda göreceğimiz eylemlerin hepsi genel olarak iktidara ve insani konulara karşı duyarsız kalan kurum ve kuruluşlara karşı olmuştur.

| **Tarih** | **Saldırı Şekli** | **Olay** |
|---|---|---|
| 27/02/12 | Websitesi hackleme | Ankara Emniyet Müdürlüğü'nün internet sitesinin çökertilerek, çok sayıda ihbar ve iç yazışmanın internet ortamında yayınlanması |
| 20/04/12 | Websitesi hackleme | İçişleri Bakanlığı sitesine ait bir alt sayfaya mesaj bırakılması |
| 27/04/12 | DNS sunuculara DDoS atak | İnternet servis sağlayıcılarından TTNET'in yaklaşık 2 saat süreyle internet hizmetinin aksatılması |
| 02/05/12 | Personel yardımıyla iç sisteme sızma | Kara Kuvvetleri Komutanlığı'nın sistemine girerek bazı TSK personelinin bilgilerinin ifşa edilmesi |
| 03/05/12 | Websitesi hackleme | MEB'ıı "Okul sütü-Akıl küpü" adıyla başlattığı süt dağıtım projesinin ilk gününde yüzlerce öğrencisinin zehirlenerek hastanelere kaldırılmasını protesto amacıyla 3 süt firmasının hacklenmesi |
| 14/05/12 | Websitesi hackleme | Anneler Günü nedeniyle "kadına yönelik şiddete" dikkat çekme amacıyla Aile ve Sosyal Politikalar Bakanlığı'nın internet sitesinin hacklenmesi ve ana sayfasına bildiri konulması |
| 29/05/12 | DDoS atak | Türk Hava Yolları'nın internet sitesine greve destek amacıyla bir siber saldırı gerçekleştirilmesi |
| 03/07/12 | Websitesi hackleme | Dışişleri Bakanlığı'nın dosya paylaşım sitesinin hedef alınması |
| 16/07/12 | Websitesi hackleme | Eylemlerini destekleyen akademisyen ve gazetecilerin tehdit edilmesi üzerine Ankara Emniyet Müdürlüğü'nün web sitesinden daha önce ele geçirdikleri 77 megabyte boyutundaki ihbarların bulunduğu txt dosyasının tamamının yayınlanması |
| 29/10/12 | Websitesi hackleme | Diyanet İşleri Başkanlığı'nın ana sayfasını hackleyerek hükümete ve Fethullah Gülen cemaatine yönelik bir dizi eleştirinin yayınlanması |
| 02/11/12 | Websitesi hackleme | Kamu İhale Kurumu (KİK)'e saldırarak AKP'yi 1 kuruşa ihaleye çıkarma eylemi |
| 07/12/12 | Websitesi hackleme | Maliye Bakanlığı sitesini hackleyerek memura "temsili olarak" zam yapılması eylemi |
| 25/12/12 | Sosyal medya saldırısı | Pedofili (çocuk tacizcileri) kişileri yakalatma ve hesaplarını kapatma eylemi |

| | | |
|---|---|---|
| 08/01/13 | Websitesi hackleme | Yüksek Öğretim Kurumu (YÖK) sitesini 2. kez hackleme ve ele geçirdiği yolsuzluk belgelerini yayınlama |
| 26/02/13 | Trojan saldırısı | Ankara Büyükşehir Belediye Başkanı Melih Gökçek hakkındaki belgelerin yayınlanması |
| 22/03/13 | Websitesi hackleme | Ankara Büyükşehir Belediyesi'nin sitesinin hacklenmesi |
| 23/03/13 | Websitesi hackleme | İsrail gizli servisi MOSSAD'ın sitesinin Anonymous grubunun işbirliğinde çökertilmesi eylemi |
| 05/05/13 | Websitesi hackleme | İstanbul Valiliği'nin Taksim'de 1 Mayıs gösterilerine izin vermemesi ve göstericilere sert müdahalesi sebebiyle İstanbul Valiliği'nin resmi sitesinin hacklenmesi |
| 11/05/13 | DDoS atak | Hatay Reyhanlı'da yaşanan patlama sonrasında ulusal yas ilan edilmesini isteyerek Hatay Valiliğinin sitesinin çökertilmesi |
| 22/05/13 | İç sisteme sızma | Reyhanlı Patlamasıyla ilgili Askeri İstihbarat Belgelerinin yayınlanması |
| 26/05/13 | E-mail hesabı hackleme | Avrupa Birliği Bakanı Egemen Bağış'ın bazı mail yazışmalarının yayınlanması |
| 31/05/13 | Websitesi hackleme | Taksim Gezi Parkı yıkımını protesto amaçlı "Hak yersen hack yersin" sloganıyla Gaziantep Büyükşehir Belediyesi web sitesinin hacklenmesi |
| 01/06/13 | E-mail hesabı hackleme | Gezi Parkı eylemlerinde milletvekillerinin duyarsızlığını gerekçe göstererek milletvekili ve eşlerinin cep ve ev telefon numaralarının yayınlaması eylemi |
| 08/06/13 | Bilinmiyor | Gezi Parkı protestolarında polisin sert tutum göstermesi gerekçe gösterilerek İstanbul ili emniyet müdürlerinin cep telefonlarının yayınlanması eylemi |
| 17/06/13 | Bilinmiyor | Tarım Bakanı ve iş adamları arasında yapılan toplantı kaydının yayınlanması eylemi |
| 28/06/13 | Websitesi ve Kullanıcı hesabı hackleme | İstanbul İl Özel İdaresi'nin web sayfasının hacklenmesi ve kullanıcı bilgilerinin twitter'da yayınlanarak sistemde takipçileriyle birlikte değişiklikler yapılması eylemi |
| 02/07/13 | DDoS atak | Sivas İl Özel İdaresi'nin Sivas Katliamını anmak maksadıyla web sayfasının hacklenmesi ve erişimin tamamen kapatılması |
| 03/07/13 | Websitesi ve Kullanıcı hesabı hackleme | Diyanet İşleri Başkanlığının web sayfasının hacklenmesi ve kullanıcı bilgilerinin twitter'da yayınlanarak sistemde takipçileriyle birlikte değisiklik yapılması eylemi |
| 14/08/13 | Websitesi ve Kullanıcı hesabı hackleme | ASKİ, Adana Büyükşehir Belediyesi Su ve Kanalizasyon İdaresi'nin hacklenmesi ve kullanıcı bilgilerinin twitter'da yayınlanarak sistemde takipçileriyle birlikte değişiklikler yapılması eylemi |
| 14/10/13 | Websitesi hackleme | Türkiye Kamu İşletmeleri Birliği web sitesinin hacklenmesi ve bayram |

| | | |
|---|---|---|
| | | mesajı bırakılması eylemi |
| 10/01/14 | XSS açığı ile Websitesi hackleme | Türkiye Büyük Millet Meclisinin web sitesinin hacklenmesi eylemi |

## 3.2 SİBER GÜVENLİK POLİTİKALARI

Dünyanın ve ülkemizin siber güvenlik konusuna bakış açısı ve bu alan için belirledikleri politikalar incelenecektir.

### 3.2.1 Ulusların Siber Güvenliğe Bakışları

Siber güvenlik, bilişim teknolojilerinin yaygınlaşması ve internet kullanımının artmasıyla beraber ulusal güvenlik stratejilerinde yer almaya başlamıştır. Bu kapsamda başta gelişmiş ülkeler olmak üzere pek çok ülke ve NATO, AB gibi uluslararası kuruluşlar siber güvenlik stratejileri üretmiştir. 19 ülkenin ulusal siber güvenlik stratejileri üzerinde yapılan inceleme sonucunda strateji belgelerinde şu ortak hedeflere değinildiği görülmektedir (Eric Luiijf ve Alexander Klimburg):

• Güvenli, saldırılara karşı dayanıklı ve güvenilir bir siber alanın sağlanması.
• Bilişim sistemleri vasıtasıyla ekonomik ve sosyal refahın, güvenli iş ortamı ve ekonomik büyümenin teşvik edilmesi.
• Bilişim ve iletişim teknolojilerinin barındırdığı risklerin kontrol altında tutulması.
• Bilişim altyapılarının dirençli hale getirilmesi.

Klimburg, NATO desteği ile oluşturduğu Ulusal Siber Güvenlik Temel Kılavuzun'da, ulusal siber güvenlik düşünülürken göz önünde bulundurulması gereken beş alan olduğunu belirtmektedir. Mevcut siber güvenlik stratejilerine bakıldığında bu alanların işlendiği görülmektedir.

#### 3.2.1.1 Askeri Siber Operasyonlar

Ülkenin sahip olduğu bilişim altyapısının korunmasına yönelik olarak siber savunma olmaktadır. Siber savunma istihbarat odaklı olup CERT tarzı, acil durumlara hızlı müdahaleye imkân sağlayan bir organizasyonel yapı gerektirmektedir. Siber savunma yukarıda bahsedildiği gibi pasif ve aktif savunma biçimlerini içermektedir. Aktif savunma yöntemleri saldırganın saldırı maliyetini arttırarak caydırıcılığı arttırmayı hedeflemektedir. İkinci önemli askeri beceri, düşman unsurların bilişim altyapılarına stratejik nitelikli siber operasyonlar yapabilmektir. Üçüncü önemli askeri beceri, savaş halinde düşmanın sahip olduğu bilişim altyapılarına yönelik siber saldırı gerçekleştirebilmektir. Dördüncü beceri, geleneksel askeri yapıların, bilişim teknolojilerinin sunduğu imkânlardan yararlanılarak modernize edilmesi yoluyla kapasite ve etkinliğin arttırılmasıdır.

#### 3.2.1.2 Siber Suçlarla Mücadele

Mücadelenin ilk aşaması ulusal ve uluslararası hukuki altyapının oluşturulmasıdır. Bu görev adalet bakanlıkları aracılığıyla yürütülmeli ve insan hak ve hürriyetlerini gereğinden fazla kısıtlamayan, caydırıcılığı olan ve polis birimlerine mümkün olduğunca rahat bir çalışma ortamı sağlayan bir hukuki altyapının tesisi için çalışmalıdır. Siber suçların küresel özelliği nedeniyle diğer ülkelerin hukuk sistemleri ile bu alanda işbirliği mekanizmaları geliştirmeye çaba göstermelidir. Polis birimlerindeki personelin, dijital delilleri daha iyi analiz edilebilmesi ve araştırmalarını daha verimli yapılabilmesi için adli bilişim konusunda uzmanlaşması sağlanmalıdır.

#### 3.2.1.3 İstihbarat Faaliyetleri

Günümüzde istihbarat faaliyetleri sadece devlet kurumları arasında değil, ticari sırların çalınması amacıyla özel şirketler arasında da gerçekleşmektedir. ABD istihbarat yetkilileri, 2009 yılında ABD firmalarının yaklaşık 50 milyar dolar değerinde fikrî mülkiyet hırsızlığına maruz kaldığını iddia etmektedir (Robinson, 2012). Bunun gibi siber casusluk operasyonlarının hedefi olmamak için karşı istihbarat faaliyetleri önem arz etmektedir.

#### 3.2.1.4 Kriz Yönetimi ve Yedekleme

Kriz yönetimi becerileri siber saldırılara maruz kaldıktan sonra hasar tespiti, saldırılara karşılık verme, gerekli noktalara acil müdahale ve hasar gören sistemlerin tekrar ayağa kaldırılması gibi kritik fonksiyonlar ihtiva etmektedir. Kritik altyapıların korunması öncelikli olarak ulusal çapta bir risk analizinin yapılarak, risk faktörlerinin düzenli olarak güncellenmesini gerektirmektedir.

#### 3.2.1.5 Siber Diplomasi ve İnternetin Yönetimi

Siber alan yeni yeni şekillenmekte olduğundan, özellikle güçlü devletler bu yeni alana ilişkin kuralların kendi ulusal çıkarlarıyla paralel olması için sürekli girişimlerde bulunmaktadırlar. Bu sebeple, ulusal menfaatlere

ters bir takım gelişmelerin yaşanmaması için siber diplomasiye önem verilmelidir. Diğer bir konuysa internet ve internete yön veren politika ve standartlardır. İnternet, kuruluşundan bu yana herhangi bir devletin veya özel kuruluşun doğrudan etkisi altına girmemiştir. Merkezi bir yapının olmayışı her türlü fikrin özgürce ifade edildiği bir ortamın oluşmasına katkı sağlamakla birlikte, internetin güvenliğini olumsuz yönde etkilemektedir. İnterneti daha güvenilir bir hâle getirmek içinse şirketler ve bağımsız kuruluşlarca güvenli iletişim protokollerinin ve standart işlemlerin geliştirilmesi yönünde çalışmalar yapılmaktadır. Bu çalışmalar internetin geleceğinin şekillenmesinde etkili olabileceğinden, ulusal güvenlik açısından bu çalışmalara katkı yapmak ve gelişmelerin dışında kalmamak gerekmektedir.

### 3.2.2 Türkiye'nin Siber Güvenlik Politikası

Ülkemizde siber güvenlik stratejisi çalışmalarının çok fazla bir geçmişi bulunmamaktadır. Siber güvenliğin tesisi açısından göze çarpan önemli faaliyetlerin başında bu alanı düzenleyen bazı kanunların kabulü gelmektedir. 2004 yılında kabul edilen 5070 sayılı Elektronik İmza Kanunu, 2008 yılında kabul edilen haberleşme sektörünü düzenlemeyi hedefleyen Elektronik Haberleşme Güvenliği Yönetmeliği bunlardan ilklerindendir (Ünver ve Canbay, 2010). Bunların yanında 2006 yılında 28242 sayılı Resmi Gazete'de yayınlanan 2006/38 sayılı Yüksek Planlama Kurulu Kararında bulunan Bilgi Toplumu Stratejisi ve Eki Eylem Planında "Güvenlik ve Kişisel Bilgilerin Mahremiyeti" başlığı altında iki eylem sayılmıştır. Bunların ilki, bilgi güvenliğine ilişkin yasal düzenlemelerin yapılmasını; ikincisi, bilgisayar olaylarına acil müdahale merkezinin kurulmasını ve kamu kurumlarının bilişim güvenliğinin sağlanmasına yönelik faaliyetleri planlamaktadır. Bu kapsamda, yukarıda CERT olarak anılan yapıya eşdeğer, Bilgisayar Olaylarına Müdahale Ekibi (TR-BOME), TÜBİTAK Bilişim ve Bilgi Güvenliği İleri Teknolojiler Araştırma Merkezi (BİLGEM) bünyesinde kurulmuş ve faaliyete geçirilmiştir.

Siber güvenliğe ilişkin olarak makro planda atılmış en somut adım 2012/3842 sayılı "Ulusal Siber Güvenlik Çalışmalarının Yürütülmesi, Yönetilmesi ve Koordinasyonuna İlişkin Karar" başlıklı Bakanlar Kurulu Kararıyla gerçekleşmiştir. Kararın kamuoyunda en çok konuşulan hükmü "siber güvenlikle ilgili alınacak kararları belirlemek, hazırlanan plan, program, rapor, usul, esas ve standartları onaylamak ve bunların uygulanmasını ve koordinasyonunu sağlamak amacıyla" bir Siber Güvenlik Kurulu'nun kurulması olmuştur. Kurul Ulaştırma, Denizcilik ve Haberleşme Bakanlığı başkanlığında Dışişleri, İçişleri, Milli Savunma, Ulaştırma, Denizcilik ve Haberleşme Bakanlığı müsteşarları, Kamu Düzeni ve Güvenliği Müsteşarlığı, Milli İstihbarat Teşkilatı Müsteşarı, Genelkurmay Başkanlığı Muhabere Elektronik ve Bilgi Sistemleri Başkanı, Bilgi Teknolojileri ve İletişim Kurumu Başkanı, TÜBİTAK Başkanı, Mali Suçları Araştırma Kurulu Başkanı, Telekomünikasyon İletişim Başkanı ile Ulaştırma, Denizcilik ve Haberleşme Bakanınca belirlenecek bakanlık ve kamu kurumlarının üst düzey yöneticilerinden oluşmaktadır. Kurulun ilk toplantısı 24 Aralık 2012'de yapılmıştır.

Bunun yanında kararda, ulusal siber güvenliğin sağlanması için politika, strateji ve eylem planlarının hazırlanması görevinin Ulaştırma Bakanlığına verildiği belirtilmiştir. Bu madde uyarınca Ulaştırma Bakanlığı, ilgili kurum ve kuruluşların da görüşünü alarak bir siber güvenlik eylem planı hazırlamıştır. Ancak eylem planı bu makalenin kaleme alındığı tarihte henüz kamuoyuyla paylaşılmamıştır. Siber güvenliğe ilişkin önemli hususları içerdiği belirtilen eylem planının uygulamaya geçirilebilmesi durumunda bu alanda önemli bir mesafenin alınacağı yetkililerce ifade edilmektedir.

### 3.2.3 Ulusal Siber Olaylarla Müdahale Merkezi

2012/3842 sayılı "Ulusal Siber Güvenlik Çalışmalarının Yürütülmesi, Yönetilmesi ve Koordinasyonuna İlişkin Karar" başlıklı Bakanlar Kurulu Kararında; Ulaştırma, Denizcilik ve Haberleşme Bakanlığına verilen görevler arasında "ulusal bilgi teknolojileri ve iletişim altyapısı ve sistemleri ile veritabanlarının güvenliğini sağlamaya, kritik altyapıları belirleyerek bunlara yönelik siber tehdit ve saldırı izleme, müdahale ve önleme sistemlerini oluşturmaya, ilgili merkezleri kurmaya, kurdurmaya, bu sistemlerin denetimi, işletimi ve sürekli güçlendirilmesine yönelik" çalışmalar yapmak sayılmaktadır. Bu kapsamda Telekomünikasyon İletişim Başkanlığı bünyesinde, Ulusal Siber Olay Merkezi (USOM) adı verilen bir yapının oluşturulmasına eylem planında yer verilmiş ve karar çerçevesinde 27 Mayıs 2013 tarihinde Telekomünikasyon İletişim Başkanlığında Ulusal Siber Olaylara Müdahale Merkezi (USOM) kurulmuştur. USOM, siber güvenliğe ilişkin olaylarda daha çok ulusal koordinasyon ve uluslararası işbirliği birimi olarak faaliyet gösterecek, Sektörel ve Kurumsal Siber Olaylara Müdahale Ekipleriyle (SOME) bir arada siber güvenliğin sağlanmasına yönelik faaliyetler yürütecektir.

# 4 REDHACK'İN TOPLUMSAL VE HUKUKİ İNCELEMESİ

Ülkemizde bilişim suçları çok yeni bir kavram olmakla birlikte, 5237 sayısı Türk Ceza Kanunumuzda bu tür suçlar 2 farklı başlık altında değerlendirilmiş ve yer verilmiştir. Elektronik ağlar vasıtasıyla işlenen klasik suçlardan genellikle o suçların bahsedildiği kısımda ağırlaştırıcı faktör olarak belirtilmiştir. Mesela bilişim vasıtalarını kullanarak işlenen dolandırıcılık suçu "nitelikli dolandırıcılık" başlığı altında mütalaa edilmiş ve ağırlaştırıcı sebep olarak kabul edilmiştir. Elektronik ağlara has suçlarsa TCK'da Onuncu Bölüm olarak Bilişim Alanında Suçlar başlığı altında ele alınmıştır. Ancak ülkemizin siber suçlara ilişkin mevzuatı ve bu mevzuatta görülen bazı problemler vardır.

TCK 141. maddede tanımı yapılan hırsızlık suçu için 142. maddede işlenen suçun nitelikli hırsızlık olma koşulları sıralanmış olup 2. fıkra e bendinde "bilişim sistemlerinin kullanılması vasıtasıyla" şeklinde bölüm yer almaktadır.

TCK 157. maddede tanımı yapılan dolandırıcılık suçu için 158. maddede işlenen suçun nitelikli dolandırıcılık olma koşulları sıralanmış olup 1. fıkra f bendinde "bilişim sistemlerinin, banka veya kredi kurumlarının araç olarak kullanılması suretiyle" şeklinde bölüm yer almaktadır.

TCK Onuncu Bölüm'de bilişim sistemine girme ve içerisinde kalma fiilini tanımlayan 243. maddeyle başlamaktadır. Maddenin birinci fıkrasında "bir bilişim sisteminin bütününe veya bir kısmına, hukuka aykırı olarak giren ve orada kalmaya devam eden kimseye" ceza verileceğine hükmetmektedir. Dolayısıyla bilişim sistemine sadece girme fiili ceza kapsamından çıkartılmakta, cezalandırma için sistemde kalma şartını da getirmektedir. Kanun koyucu muhtemelen kazara gerçekleşen yetkisiz erişimleri kapsam dışında tutmaya çalışmış olmakla beraber, kişinin bu madde kapsamında cezalandırılması için sistemde ne kadar kalması gerektiği konusu yoruma bırakılmıştır. Bunun yanında sisteme hukuka uygun olarak girip, hukuka aykırı olarak kalmaya devam edenler veya yetkisini aşanlar hakkında da belirsizlik bulunmaktadır.

Maddenin ikinci fıkrasında "yukarıdaki fıkrada tanımlanan fiillerin bedeli karşılığı yararlanılabilen sistemler hakkında işlenmesi halinde, verilecek ceza yarı oranına kadar indirilir" hükmü yer almaktadır. Bu fıkrada "bedeli karşılığı yararlanılabilen sistemler" ibaresinden ne kastedildiği açık olmamakla beraber bunun, kayıtlı müşterilerine internet üzerinden belli hizmetler sunan firmalara ait sistemler olduğu anlaşılmaktadır. Kanun, saldırıya hedef olma ihtimali daha fazla olan bu sistemlere karşı gerçekleştirilecek yetkisiz girme ve kalmaya devam etme fiiline verilecek cezayı yarı oranında azaltmaktadır. Aslında daha fazla risk barındıran sistemlere ilişkin daha fazla caydırıcılık olması gerekirken bu fıkrada tam tersi bir durum söz konusudur. Kaldı ki böyle bir sisteme saldırı neticesinde müşterilerin kişisel ve finansal bilgilerinin kötü maksatlı kişilerin eline geçmesi gibi korunması gereken ciddi bir risk bulunmaktadır. Diğer yandan bir önceki fıkrada aslında "yetkisiz girme ve kalmaya devam etme" şeklinde tek bir fiilden bahsedilirken ikinci fıkranın "yukarıdaki fıkrada tanımlanan fiillerin" ibaresiyle başlaması kanun metninde yapılan değişikliğin biraz aceleye geldiği düşüncesini uyandırmaktadır. Üçüncü fıkrada ise bu fiil neticesinde istemeden verilerin yok olması halini hükme bağlamaktadır.

TCK 244. maddede bilişim sisteminin işleyişinin engellenmesi ve bozulması; bilişim sistemindeki verilerin bozulması, yok edilmesi, değiştirilmesi veya erişilmez kılınması; sisteme veri yerleştirilmesi, var olan verilerin başka bir yere gönderilmesi suçları hükme bağlanmaktadır.

TCK 245. madde kredi kartı dolandırıcılıklarına ilişkin hükümler içermekte ve son madde olan TCK 246. madde ise bu suçların işlenmesi suretiyle yararına haksız menfaat sağlanan tüzel kişiler hakkında bunlara özgü güvenlik tedbirlerine başvurulacağını belirtmektedir.

### 4.1.1 Bilişim Suçları Açısından Değerlendirilmesi

RedHack grubunun yaptığı eylemler bölümünde yaptığı saldırılar ve türlerini TCK'nın onuncu bölümünde yer alan Bilişim Suçları maddeleri ışığında incelediğimiz zaman 3 temel suç görülmektedir:

1. Çeşitli atak tipleri kullanarak bilişim sistemlerinin içerisine sızmayı başardıkları suçlar TCK 243. maddede yer alan "Bilişim sisteminin bütününe veya bir kısmına, hukuka aykırı olarak giren ve orada kalma" bölümü ile eşleşmektedir.

2. Yaptıkları DDoS saldırılarındaki amaç, yöntem ve sonuçlar değerlendirildiği zaman, işlenen suç TCK 244. maddesi 1. fıkrasında yer alan "Bir bilişim sisteminin işleyişinin engellenmesi veya bozulması" bölümü ile eşleşmektedir.

3. Özellikle en çok yaptıkları saldırı türü olan bir bilişim sisteminin içerisine girip verileri değiştirmeleri veya içeride eriştikleri verileri kendilerine ait bloglarda yayınlamaları TCK 244 2. fıkrada yer alan "Bir bilişim sistemindeki verileri bozma, yok etme, değiştirme veya erişilmez kılma, sisteme veri yerleştirme, var olan verileri başka bir yere gönderme" ile eşleşmektedir.

TCK 244. madde ile uyuşan suçları RedHack sıklıkla kamu kurum veya kuruluşlarına karşı işlemektedir. Aynı maddenin 3. fıkrasında bu durum suçun cezasının artırıcı sebebi olarak belirtilmektedir.

Örneğin, RedHack 3 Temmuz 2013 tarihinde Diyanet İşleri Başkanlığının websitesindeki zafiyetlerden yaralanarak bilişim sisteminin içerisine girmeyi başarmış, burada elde ettikleri kullanıcı hesap bilgilerini sosyal ağlar aracılığıyla başka insanlarla paylaşmış, sistemdeki verileri değiştirmiş ve değişmesine sebep olmuştur. Bu eylemin amacı sisteme erişip verileri değiştirmek ve bilgileri paylaşmak olması ışığında Bilişim Suçları açısından değerlendirildiği zaman TCK'nin 244. maddesinin 2.fıkrasında yer alan suçlar kapsamında olup 6 aydan 3 yıla kadar hapis cezası ile cezalandırılması gerekmektedir. Diyanet İşleri Başkanlığının bir kamu kurumu olması da göz önünde bulundurulduğu zaman TCK'nin 244. maddesinin 3. fıkrasına göre söz konusu cezanın yarı oranda artırılması gerekmektedir.

### 4.1.2 Bilişim Vasıtasıyla İşlenen Klasik Suçlar Açısından Değerlendirilmesi

"Geleneksel" ya da "klasik" suçlar olarak tanımlanan, ancak bir bilişim sistemi aracılığıyla işlenen suçlar; e-posta yoluyla işlenen tehdit veya hakaret suçu, yine bilgisayar veya İnternet siteleri üzerinden işlenen cinsel taciz, halkı kin ve düşmanlığa tahrik etme gibi suçlar örnek olabilir. Teknolojik imkanların müthiş bir hızla artması ve gelişmesi ile birlikte, artık insan öldürme suçuna kadar her suç bilişim yoluyla işlenebileceği için, bu gruptaki suçların sınırını belirlemek mümkün değildir. Ayrıca bilişim sistemlerinin kullanılması ile işlendiği zaman nitelikli halen gelen hırsızlık ve dolandırıcılık suçları da vardır. Örneğin, bir bilişim sistemine bağlanmış kasanın veya kapının açılması suretiyle ziynetlerin çalınması bilişim vasıtasıyla işlenen hırsızlık suçu kapsamındadır.

RedHack grubunun eylemlerinden önce özellikle sosyal ağlar üzerinden yayınladıkları mesajlar ve bildirilerde kişileri tehdit etmekte ve onlara şantaj yapmaktadır. Bu eylemler TCK 106 ve 107. maddelerde suç olarak belirtilmiş olup, tehdit için mağdurun şikâyeti üzerine, altı aya kadar hapis veya adlî para cezası, şantaj için bir yıldan üç yıla kadar hapis ve beşbin güne kadar adlî para cezası ile cezalandırılması gerekmektedir.

### 4.1.3 Örgütlü Suçlar ve Terör Suçları Açısından Değerlendirilmesi

TCK 220.maddesi 1-8 fıkralarında suç işlemek amacıyla örgüt kurma suçunun tanımı ve cezaları yer almaktadır. RedHack grubu tüzüğü ile organizasyon yapısını belirlemiş olması, faaliyetleri içerisinde suç işlemiş olması sahip olduğu araç ve gereçler ile suç işlemeye elverişli olması sebebiyle örgütlü suçlar kapsamında değerlendirilebilir. Bunun yanı sıra TCK 220'nin en önemli kriteri olan suç işlemek amacıyla örgütün kurulmuş olduğunu belirtmesi ve RedHack'in gerek tüzüğünde gerekse basın ve sosyal ağlar aracılığıyla eylemlerinde illegal yöntemleri esas olarak kabul etmesi TCK 220. maddesine göre suç işlemek amacıyla örgüt kurmadan dolayı yargılanma yolu açıktır.

3713 sayılı Terörle Mücadele Kanunu'n 1. maddesinde terör "cebir ve şiddet kullanarak; baskı, korkutma, yıldırma, sindirme veya tehdit yöntemlerinden biriyle, Anayasada belirtilen Cumhuriyetin niteliklerini, siyasî, hukukî, 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. Aynı kanunun 4.maddesinde terör amacıyla işlenen suçlar belirtilmiş olup, TCK 243 ve 244. Maddelerdeki suçları TMK 1.maddede yer alan tanıma uygun olarak işleyenlerin terör suçu işlediği tanımlanmıştır.

Ankara Cumhuriyet Başsavcılığı; RedHack grubunun tüzük ve ambleminin olması, örgüt kategorisine girmesi ve bazı kamu kurumlarının sistemlerini hackleyerek polis muhbirlerinin isimlerini deşifre etmesi terör örgütü olduğunu kanıtladığını savunmuştur. Ayrıca iddianamede e-devlet uygulamaları hakkında bilgiler verilerek, "Yazılı ve görsel basına yansıyan haberlerden de görüleceği üzere artık tüm dünyada e-devlet uygulamalarına yapılan siber saldırılar, devlet otoritesini zaafa uğratan, temel hak ve hürriyetleri yok eden, devletin iç ve dış güvenliği ile kamu düzenini bozan' eylemler olarak kabul edildiğinden terör olarak değerlendirilmektedir" denilmiştir. Grup üyelerinin Ankara Emniyeti'ne düzenledikleri siber saldırı da bazı muhbirlerin kimliklerini açıkladıkları ve bunun da Terörle Mücadele Kanunu'nca (TMK) suç sayıldığının anlatıldığı iddianamede, Redhack isimli grubun terör örgütü gibi organize olduğu, şehir merkezlerinde yazılama ve afişleme olaylarını gerçekleştirdikleri de ifade edildi. İddianamede, şu ifadelere yer verildi: "Yapılan eylemlerin fotoğraflarını dijital ortamda internet üzerinde yayımladıkları, kendilerinin ve kendileriyle aynı düşünceye sahip grupların gerçekleştirdiği yerleşik olan düzen içerisinde kanunların suç saydığı eylemlere müdahale eden kurum ve kuruluşların internet ortamında yayınlanan sitelerine saldırı yaptıkları, saldırılar neticesinde ele geçirdikleri bilgi ve belgeleri internet üzerinde yayınladıkları kurdukları internet sitelerinde örgütün tanıtımını yaptıkları, internet ortamında gerçekleştirdikleri eylemler ile kendileri gibi yapıya sahip THKP/C, THKO, TKP/ML, DHPK/C MLKP ve PKK gibi Marksist – Leninist – Maoist sol ve bölücü örgütlerin tamamına dijital anlamda destek verdikleri belirlenmiştir."

Terörle Mücadale Yasası (TMY) ile görevli Ankara Başsavcı Vekilliği, birçok devlet kurumunun internet sitesine yönelik eylemleriyle gündeme gelen RedHack'e yönelik, "silahlı terör örgütü" suçlaması konusunda fikir değiştirmiştir. Daha önce Ankara Emniyeti'nin sitesine yönelik siber saldırı nedeniyle RedHack üyesi olduğu iddia edilen kişiler için "silahlı terör örgütü üyeliğiyle" dava açan savcılık, RedHack'in YÖK, Dışişleri Bakanlığı gibi kurumların sitelerine yaptığı saldırılarla ilgili yürüttüğü soruşturmada ise görevsizlik kararı vermiştir. Dosyayı normal savcılığa gönderen TMY Savcılığı, gerekçesinde RedHack'in "yasadışı örgüt" olduğunu, ancak eylemlerinin "şiddet içermediğini" kaydetmiştir.

# 5 SONUÇ

Hem ülkemizde hem de dünyada bilişim altyapılarına ve internete olan bağımlılığımız artmakta ve buna bağlı olarak siber alandaki tehditler de giderek artmaktadır. Siber tehdidi doğru ölçebilmek ve strateji geliştirebilmek için öncelikle gözlem, takip, analiz ve tahmin kapasitesi olan birimlere ihtiyaç vardır. Ayrıca siber güvenliğin sadece internet güvenliğini değil tüm iletişim altyapılarını kapsayan geniş bir kavram olması nedeniyle sonraki adım olarak çok sektörlü bir yaklaşımla ulusal siber güvenlik politikasının belirlenmesi gerekmektedir. Ülkemizin ciddi bir siber saldırıya maruz kalmaması için pasif savunma alanında yapılanların yanında aktif savunmaya da yönelik tedbirler alınmalıdır.

Bu kapsamda ülkemizde 2012/3842 sayılı "Ulusal Siber Güvenlik Çalışmalarının Yürütülmesi, Yönetilmesi ve Koordinasyonuna İlişkin Karar" başlıklı Bakanlar Kurulu Kararıyla Siber Güvenlik Kurulu kurulmuştur. Bu karar doğrultusunda Telekomünikasyon İletişim Başkanlığı bünyesinde, Ulusal Siber Olay Merkezi (USOM) adı verilen bir yapının oluşturulmasına eylem planında yer verilmiş ve Telekomünikasyon İletişim Başkanlığında Ulusal Siber Olaylara Müdahale Merkezi (USOM) kurulmuştur. USOM, Sektörel ve Kurumsal Siber Olaylara Müdahale Ekipleriyle (SOME) bir arada siber güvenliğin sağlanmasına yönelik faaliyetler yürütecektir. Özellikle ulusal güvenliğe tehdit olacak iletişim, finans ve enerji sektörlerine ait Sektörel ve Kurumsal SOME'lerin bir an önce faaliyetlerine başlamaları gerekmektedir.

Siber suçlarla mücadeleye yönelik hukuki altyapımız pek çok ülkeyle kıyaslandığında gelişmiş gözükse de, RedHack iddianamelerinde ve davalarında da görüldüğü gibi bir takım önemli eksiklikleri bulunmaktadır. Bu sebeple TCK ve CMK'da, siber suçlarla daha etkin mücadeleye imkân verecek düzenlemelerin yapılması gerekmektedir. Bu konuda önemli bir eksik de siber teröre ilişkin ilgili mevzuatta bir tanımın yapılmamış olmasıdır. Siber terörle hukuk devleti çerçevesinde mücadele edebilmek için kavramın tanımının yapılması ve bu tür faaliyetlere yönelik yaptırımların belirlenmesi gerekmektedir.

Siber suçlar ile mücadelede alanında uzman kişilerden oluşan bir ekibin İçişleri Bakanlığı bünyesinde oluşturulması gerekmektedir. Çünkü RedHack gibi işinde uzman toplulukları veya kişilerin saldırılarının doğru şekilde analiz edilmesi, oluşan kayıt izlerinin anlamlandırılabilmesi ve incelemeler sonrası eylemde bulunan kişi veya toplulukların ve yerlerinin tespit edilmesi gerekmektedir. Şu aşamada bu alan ülkemizde yetersiz kaldığı için RedHack grubu Emniyet Müdürlükleri, Bakanlıklar, kamu kurum ve kuruluşları başta olmak üzere birçok yere siber saldırılar düzenlemekte, devlet sırlarını açığa çıkarmakta ve işledikleri bilişim suçları için cezalandırılamamaktadır.

Çalışma içerisinde toplumun hacktivist gruplara ve RedHack grubuna bakış açısı, devletin şeffaflaşması konusundaki katkısı ve sosyal ağların yapılan eylemleri meşrulaştırması konularına yer verilememiştir. Bu konular ile yaptıkları eylemlerin hukuksal incelemelerinin sentezlenmesi ileriki çalışmalara konu olmalıdır.

KAYNAKÇA

[1] Wikipedia - RedHack: <http://tr.wikipedia.org/wiki/RedHack>

[2] Atılım Gazetesi – Kızılhack: Hedefimiz Ezenler: <http://web.archive.org/web/20100507133839/http://www.atilim.org/atilim/modules.php?name=Guncel&file=article&sid=16899>

[3] Ankara Strateji Enstitüsü – Türkiye'nin Siber Güvenlik Politikası: <http://www.ankarastrateji.org/haber/turkiye-nin-siber-guvenlik-politikasi-991/>

[4] Resmi Gazete – Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı: <http://www.resmigazete.gov.tr/eskiler/2013/06/20130620-1-1.pdf>

[5] Mediterranean Journal of Social Sciences - Hactivism in Turkey: The Case of Redhack [Vol 4 No 9 October 2013]

[6] McAfee Blog Center – 7 Types of Hacker Motivations: <http://blogs.mcafee.com/consumer/family-safety/7-types-of-hacker-motivations>

[7] Google Docs – RedHack Tüzük: <https://sites.google.com/site/kizilhackerlar/tuzuk>

[8] Digitalage – Hacktivizm ve Siber Terör: <http://www.digitalage.com.tr/makale/hacktivizm-ve-siber-teror/>

[9] SANS Institute InfoSec Reading Room - The Jester Dynamic: A Lesson in Asymmetric Unmanaged Cyber Warfare: <http://www.sans.org/reading-room/whitepapers/attacking/jester-dynamic-lesson-asymmetric-unmanaged-cyber-warfare-33889?show=jester-dynamic-lesson-asymmetric-unmanaged-cyber-warfare-33889&cat=attacking>

[10] Alexander Klimburg (Ed.), National Cyber Security Framework Manual, NATO CCD COE Publication, Tallinn 2012.

[11] Telecomix - Türk Vatandaşlarına çağrı Adımız Telecomix: <https://resources.telecomix.ceops.eu/documents/circumvention/2013-06-18-Turk_Vatandaslarina_cagri.pdf>

[12] Sosyal Medya Macerası – Hacktivizm: Anonymous, RedHack, Cyber-Warrior: <http://sosyalmedyamacerasi.blogspot.com.tr/2013/02/Hacktivizm-RedHack-Anonymous.html>