YENİ MEDYA ve SİBER PROTESTO HAREKETLERİ

Doç. Dr. **Murat AKSER**

ÖZET

İnternette İslam dinine ve Türkiye'ye hakaret eden sitelere Türk hackerlar tarafından saldırılar yapılmaktadır. Bu yazı, hacker saldırılarını, siber-terörden ayrı olarak tanımlamayı amaçlamaktadır. Aktivist söylemci hacker, geçici olarak bir toplumsal durumu protesto amacıyla sitenin görünümünü değiştirir ve kalıcı zarar vermemektedir. Ayyıldız Grubu veya Bozkurt Grubu Türk askerlerinin şehit haberleri, Danimarka karikatür krizi, Türk-Yunan ve Mavi Marmara saldırısı gibi durumlara protesto amacıyla müdahale etmektedir. Yaptıkları hasar geçicidir, söylemleri evrensel barış ve kardeşlik üzerine kuruludur. Bu nedenle siber terör değil, aktivist söylemsel hackerlerdi.

Anahtar Kelimeler: İnternet, Hackleme, Yeni Medya, Siberalem.

GİRİŞ

İnternet üzerinde çeşitli ağlar ve siberalanlarda faaliyet göstermekte olan Türk kökenli siberaktivist hacker grupları dünya çapında belli bir görünürlüğe ve faaliyet alanına sahipler. Hiç beklenmeyen siber eylemin yarattığı geniş çaplı korku nedeni ile Türk hacker hareketlerinden Batılı medya korkuyor ve onları terörist olarak adlandırıyor. 11 Eylül olayları sonrası dünyada İslam'a karşı hakaret içeren batılı sitelerin sayısındaki artışın karşısında Türk hackerlar tarafından düzenlenen saldırılar sonucu zaman içinde bu tür siteler internetten yok oldular. Bu çalışma Türk hackerlar tarafından yapılan bu tarz saldırılara ait endişelere karşı terörist olmayan, özünde düzensiz olan, kalıcı zarar vermeyen, bilgi ve veriyi kamuyla paylaşmayı amaçlayan bu aktiviteleri kavramsal olarak tanımlamayı, sınıflandırmayı ve açıklığa kavuşturmayı amaçlıyor. Aktivist hackerlar, daha çok sitelerin görünümünü geçici olarak değiştirmek ve verileri açığa çıkarma türü faaliyetlerde bulunuyorlar. Ayyıldızlar veya Bozkurtlar gibi vatansever isimler kullanıyorlar. Söylemsel faaliyetleri Türk - Yunan ilişkileri, Türk askerlerinin şehit haberleri, Türk-Sırp futbol karşılaşmaları, Danimarka karikatür krizi ve Mavi Marmara saldırısı gibi olaylar ile ateşlenebiliyor. En fazla seyirci kitlesine ulaşabilmek için SONY gibi uluslararası markaların sitelerine saldırıyorlar. Verdikleri zarar finansal olmuyor ancak fikri mesajlarını Siber aktivismi siber terör olarak tanımlamaktan vazgeçmeli ve ideolojik hacker saldırılarının söylemsel faaliyet analizi yapılmalıdır.

Siberterörizm: Tanımlar

Siber-terör, radikal faaliyetler ile teknoloji arasındaki bir kesişme noktasıdır. Günümüzde birçok terörist grubun asıl amacı, etnik veya dine dayalı farklılıkları körükleyen kendi kimliklerini tüm diğerlerine üstün gören bir şiddet alanı yaratmaktır. Geçmişte, düşman tanımlanabiliyor veya coğrafi olarak kuşatılıyor, hapsedilebiliyor ve yok edilebiliyordu. Ama şimdi terör faaliyeti yapan düşmanı ayırt edebilecek keskin sınırlar bulunmamakta çünkü teknolojinin nimetlerinden faydalanabiliyorlar. Bu yeni yüzü ile terörizm daha tehlikeli; çünkü başlangıç noktası kesin değil ve herhangi bir ulus-devlet ile ilişkisi yok. Bugünün teröristleri saldırmak için uçaklara, bombalara ve diğer patlayıcıları kuşanmış silahlı orduya ihtiyaç duymuyor. Bir ülkenin belki de bir kıtanın ekonomik, politik ve askeri kaynaklarını barındıran ve hayati önem taşıyan bilgisayar sistemlerine virüs gönderebiliyorlar. İnternet üzerindeki terörist örgütlerin varlıklarının artması ve siber-uzaydaki terör günümüzün en önemli sorunlarından biri. Potomac Enstitüsünde çalışan terör uzmanı Yonah Alexander biyolojik, kimyasal, nükleer gibi geleneksel olmayan silahlara karşı bir saldırı olabileceği konusunda uyarıda bulunuyor ve siber-terörizm ile "suçlular güç kaynaklarına ve hava trafiğine bir tuşa basarak zarar vermeye çalışacaklar." (Alexander, Swetman, 2001: 4). Siber-terörizmin yarat-

tığı potansiyel tehdit kitlesel medyada, politikada, güvenlik güçlerinde ve bilgi teknolojileri sektöründe geniş çapta tartışılageldi. Bu korku özellikle kamuda körüklenmekte; çünkü modern zamanın en büyük korkulardan ikisi siber-terörizm çağında belirlendi. Siberterörde korku şiddetli mağduriyet (can-mal kaybı) ve huzursuzluk hissiyle birlikte bilgisayar teknolojisi ile ne zaman nerede ortaya çıkacağı beli olmadan kendini gösterir (Weimann, 2004).

Siber-âlem (internet ve cep telefon ağları) teröristler için oldukça çekici bir alan teşkil eder. Çünkü daha ucuz ve geleneksel terörizm metotlarından daha kimliksiz. Hedeflerin çeşitliliği ve büyüklüğü oldukça geniş ve siber-terörist kendini hiç belli etmeden yönetim sağlayabilir ki bu özellikle tercih sebebidir. "Siber-terörizm geleneksel terörizm standartlarına göre çok daha az fiziksel çalışma, psikolojik yatırım, ölüm riski ve seyahat zorunluluğu gerektiriyor. Bu durum terörist örgütler için insan çekmeyi, kazanmayı kolaylaştırıyor." (Wiemann, 2004: 5). Siberterörizm geleneksel terörist örgütlenmelere oranla daha fazla insana etki etmeye başladığından beri kamuda daha fazla varlık gösteriyor ve medyanın daha fazla dikkatini çekiyor ki teröristlerin istediği de buydu.

Ancak, bu yeni tip terörizme olan aşırı ilgiye rağmen şaşırtıcı bir şekilde bu teröristlerin karakteristik özellikleri ve esas internet kullanım amaçları bilinmiyor. Bu nedenle, "siber-terörizm" üzerine bu yapılan ilk önemli tanımlamadır.

Siber-terörizm, terörizm ile siber alemin kesişme noktasıdır. "Yasal olmayan saldırılar ve bilgisayarlara, ağlara ve bilgi depolarına, devletin veya insanlarının toplumsal durumlarını veya siyasal konumlarını göz korkutarak ve baskı altında tutmak için yapılan saldırılar" (Denning, 2000: 1) olarak tanımlanıyorlar. Ek olarak, insanlara veya mülke yapılan bir saldırı şiddet ile sona ermeli veya en azından korkuyu sağlayabilmek adına yeterli zararı vermeli ki onun adına siber-terörizm denilebilsin. Stratejik olarak önemli bir altyapıya yapılan ciddi saldırılar da siber-terörizm olarak adlandırılabilir. Ancak saldırılar stratejik önemi olmayan hizmetlere duraksatıyor veya kurum imajına yönelik ideolojik söylem içeren sorun yaratan aktivizm ise siber-terörizm kategorisinde sayılmıyor. Siber-teröristlerin kullanabileceği metotlar oldukça geniş:

- saldırılan ağı çökertmeye ya da o ağ üzerinde kontrol kurmaya izin veren muhtelif çeşitlerde saldırılar;

- bilgiye zarar vermeye ya da yeniden düzenlemeye ya da bilgisayar sistemlerindeki işlemi engelleyen ağ kurtlarını (worm) da barındıran bilgisayar virüsleri;

-mantıksal bombalar; programların içine yerleştirilen ve bazı zamanda aktive edilen bir kod;

-tehlikeli sistemlerin sahibi hakkında bilgi sahibi olmadan gerçek hareketleri öldürmeye izin veren "Truva Atları" (kendini bilgisayar kullanıcısın şifreleri dahil

tüm bilgilerini İnternetten virüslü bir site üzerinden farklı hedeflere gönderen Truva atları (Trojan) şu anda oldukça yaygın); Yani siber-terör ağlar arası bilgi değiş tokuşuna engel olmak için hazırlanır. (Golubev, 2001: 4).

Kitlesel medya ve film sektörü, siber saldırı korkusunun canlandırılmasına sebep oldu. 2003 Temmuz'unda, Washinton Post ilk sayfa manşetinde şunu yayınladı: "Uzmanlar Al Qaeda Feared tarafından düzenlenen siber saldırılar için kan akıtma aracı olarak internet kullanımının eşiğindeki teröristler olduklarını söylüyor." Film sektöründen *Golden Eye*, *Swordfish*, *Die Hard 4.0* gibi filmler ve popüler televizyon dizisi *24* yalnızca bazı örnekler. Kitlesel medya hackleme olaylarını siber-terörizm olarak etiketlemeye eğilimli. Bu nedenle "hackleme" ve "siber-terörizm" arasında bir ayrım yapmak önemli. Hackleme "online ve gizlenerek gizli olanı açığa çıkarmak, kendi çıkarı için kullanmak veya başka bir yolla bilgisayar işletim sistemleri ve diğer yazılım açıklarından yararlanmak için arama yapan aktiviteler" olarak tanımlanıyor. Diğer yandan, hackerlar yalnızca kargaşa ile öç almak isterken siber-teröristler öldürmeyi ve dehşet yaratmayı amaçlıyor. Terörist grupların hackerları taraflarına çekip istihdam etmeleri halinde, hackleme ile siber-terörizm arasındaki fark o kadar da net olmamaktadır. Bu durumda hackerlar siber-teröristlere dönüşebilirler ve bu dönüşüm para ile veya prestij ile sağlanabilir. Genç ve eğitimli insanlar olarak terörist grupların oyunlarına gelebiliyorlar, bu yeni jenerasyon siber-terörizmin davranışlarını uygulayabilme yeteneğine sahip olacaktır.

11 Eylül sonrası dönemde Amerikan Hükümeti siber-terörizmi bir problem olarak görüp ciddi bir biçimde ele aldı ve internete katı kurallar getirdi. 11 Eylül'den sonraki 45 günde Amerikan Kongresi yeni anti-terörizm kanunu ile tüm ülkeyi koruyan bir kurumsal yaklaşıma geçti. "Siber-terörizm" kanunda adı geçen yeni bir tanım olmuştur. Kanuna göre siber-terörizmin açılımı "ulusal savunmayı yönetmek veya ulusal güvenliği sağlamak için bir devlet kurumu tarafından kullanılan bilgisayar sisteminde hasar oluşması ve vatandaşlar, tüzel kişiler veya hükümet yetkilileri de dahil olmak üzere korunan bir bilgisayarın ağlarına çeşitli nedenlerle zarar verilmesi" olarak kaydedildi

2002 yılında, Siber Güvenliği Arttırma Kanunu, İç Güvenlik Kanunu'na dâhil edildi. Bu kanun, başkalarının hayatlarını düşüncesizce tehlike altında bırakan kötülükçü bilgisayar hackerlarını ömür boyu hapis cezası ile cezalandırıyor ve internet bağlantısında sürmekte olan bir saldırı varsa ya da "ulusal güvenlik menfaatini tehdit eden ani bir saldırı" varsa mahkeme izni olmadan sınırsız olarak gözetim altında tutma izni veriyor (Cullagh, 2002). Bu, ayrıca devletin şahsa ait özel bilgilerine ulaşımını ve gözetleme gücünü artırırken terörist aktivitelerin tanımını genişletiyor.

Avrupa ülkeleri benzer biçimde siber-alemi kontrol eden kuralları uygulamaya koymuştur. Örneğin, Avrupa Konseyince 23 Kasın 2001'de kabul edilen siber-suç Anlaşması siber-suçlara ilk yasal ve usulen bakış açısı getirilen anlaşmadır (Con-

vention, 2001). Bu sözleşme ulusal ve hükümetler arası seviyede bilgisayar üzerinden işlenen yasadışı faaliyetleri önlemeyi amaçlayan yaptırımları şart koşuyor.

Devletler bazında internetin teröristler için çekici bir alan olarak kullanılabileceği korkusunun temelleri bulunmaktadır. Çünkü internet:

- kolay erişim sunuyor,

- kural, sansür veya hükümet kontrolünün çok az ve hatta bazen hiç barındırmıyor,

-dünyaya yayılmış potansiyel seyirci kitlesi var,

-iletişimde anonimlik sağlayabiliyor,

-hızlı bilgi akışı var,

-karşılıklı etkileşim mümkün,

-sanal varlık ucuz bir yolla yaratabilip korunabilmekte,

-faklı medya türleri içerebilmesi (metin, grafik, ses kaydı ve video yapma olanağı ve kullanıcılara film, şarkı, kitap, poster vs. yükleme kapasitesi)

-haber kaynağı olarak İnterneti gittikçe daha fazla kullanan geleneksel kitlesel medyanın gazetedeki yerini şekillendirme olanağı.

2000 sonrası ortaya çıkan internet toplumunun bilgi teknolojilerine karşı artan bağımlılığı teröristlere siber-alemi kullanma şansı vererek yeni hassasiyetler yarattı. "Bir ülke ne kadar çok teknoloji ile geliştiriliyorsa o kadar çok altyapısına siber-saldırı uğranması riskini taşır." (Weimann, 2004: 2).

Bugünün siber-terörizmine bağlı gerçeklere dayanarak bakıldığında siber-terörizm üzerine kanun koyucular tarafından algılanan tehdit orantısız olarak abartılabilmektedir. Ulusların kritik altyapı sistemlerine yapılan bazı aktivist söylemsel siber-saldırılar teröristler tarafından liderlik edilmeyen ve siber-terör derecesinde zarar vermeyen faaliyetlerdir. Bu kavram karışıklığının daha önceden ciddiyetle irdelenmemesinin sebepleri çeşitlidir;

İlk olarak, siber-terörizm şu anda gündemde insanların hayallerinde orantısız bir tehlike olarak görülmekte ve bu özelliği ile bir dizi popüler film, TV şovları ve romanlarda yer almaya devam ediyor.

İkincisi, kitlesel medya hackleme ve siber-terörizm arasındaki farkı belirlemekte başarısız oluyor ve birçok hackleme aktivitelerini siber-terörizm eylemi olarak adlandırıyorlar.

Üçüncü sebep ise toplumsal bilinçsizliktir. Siber-terörizm birçok insanın tamamıyla anlayamadığı, bu nedenle korku eğilimi duydukları iki alanda meydana getiriliyor-teknoloji ve terörizm. Dördüncüsü, siyasetçilerin bu korkuya zaman

zaman kendi gündemlerini ilerletmek için yaptıkları açıklamalar ile katkıda bulunmasıdır. Beşinci faktör ise siber-terörizmin anlaşılmaması ve kamu zihninde karmaşaya ve binlerce efsane oluşmasına yol açan farklı anlamlar barındırması.

Türk Hackerlerin Ayrıcalıklı Durumu

Bu çalışmaya, şu araştırma soruları sorularak başlanılmıştı: Türk hackerlerinin söylemsel faaliyetleri siber-terörizm olarak adlandırılabilir mi? Bu faaliyetleri ne şekilde batıdaki muadillerinden ayrılır? Bu eylemlerin ardında nasıl bir söylem vardır? Türk hacker faaliyetlerini terör faaliyetleri olarak adlandırmak siber hackleme aktivitelerinin tamamının siber terör sayılıp sayılamayacağına dair tartışmaya tekrar düşmemize neden olmaktadır. Siber terör, tıpkı terör eylemlerinin konvansiyonel türleri gibi bir ülkenin devlet ya da özel kurum web-sitesini hackleyip yurttaşlarını etkileyerek farkındalık, çaresizlik ve korku yaratmayı amaçlar. Ancak, saldırganların doğrudan amacı korkutma yahut paniğe yol açma olmaz ise ve Türk hackerlar durumunda olduğu üzere yalnızca farkındalık yaratmak olsa da bu hala siber terörizm olarak adlandırılabilir mi? Bizim görüşümüz şudur ki; bu tür hackleme faaliyetleri siber terör aktiviteleri değil, aktivist söylemsel hackleme faaliyetleridir.

Yöntem olarak bu eylemlerin eleştirel söylem analiziyle incelenmesi faaliyetlerin aktivist yönüne işaret edecektir. Bu çalışmada örnek vaka, Türk hacker grubu Ayyıldız ekibinin faaliyetleridir. Bu grubun web-sitesi siber faaliyetlerinin ardındaki söyleme dair bir öngörü sağlamaktadır.

a. Grup Kimliği

Ayyıldız Grubu üyelerinin kullandığı takma adlar adı genellikle Türk milliyetçiliğinin mitolojisindeki Ayyıldız, Bozkurt gibi isimlerden etkilenmektedir. Ayyildiz.org sitesi beş ayrı dilde faaliyet göstermektedir: Türkçe, İngilizce, Almanca, Fransızca ve Arapça. Bu diller popüler diller olmakla birlikte, Türk kökenli göçmenler çoğunlukla bu dillerin konuşulduğu ülkelerde yaşamaktadır ve bu hizmet onların da siteye erişimini kolaylaştırmaktadır.

Ayyıldız ekibi dünyanın tüm bölgelerinden gelen hackerler tarafından oluşturulmuştur. Birçoğu gelişmekte olan ülkelerdeki yazılım mühendislerine yurttaşlık veren sanayileşmiş ülkelerdendir. Örneğin Batuhan (Avustralya), Barbaros (Kanada), Atakan (ABD), Kahraman (Fransa), Çağabey (İsviçre) ülkeleri üzerinden ekibe katılmıştır. Sitelerindeki manifestolarında kendilerini Türk ordusunun 1920'lerdeki İstiklal Savaşını andıran biçimde konumlamaktadırlar. Grubun kurucu üyelerinden biri olan Batuna, 2008'de hayatını kaybetmiştir ancak grup hala operasyona devam etmektedir, hatta operasyonlarına dair özel baskı ve el altından dağıtılan bir kitap bile yayınlamışlardır.

b. Saldırı Faaliyetleri ve Biçimleri

Bir siteye müdahale ederek görünümünü değiştirmek Türk hackerlerinin en genel özelliğidir. Kullanılan semboller, Türk bayrağı veya Türkiye Cumhuriyeti'nin kurucusu Mustafa Kemal Atatürk'ün fotoğrafı gibi belirgin milliyetçi sembollerdir. Ayrıca grup, İslam dinine karşı düşmanlık yapan sitelere karşı İslam'ı savunmak ve ırkçılık yapan sitelere karşı yurtdışında yaşayan Türkleri ve yurtdışındaki Türkiye imajını savunmak türü faaliyetler göstermektedir.

Dini toleranssızlık örneğinde, grup 2006 yılında Danimarkalı karikatür krizinde Danimarka'daki pek çok nefret söylemi içeren web-sitesini zarar vermek ya da yok etmek amacı ile değil yalnızca İslam'ı ve Türkleri yanlış tanıttığı için protesto etmek amacı ile hacklemiştir. Benzer şekilde Birleşmiş Milletler sitesini Filistin-İsrail sorunları ve Lübnan'a düzenlenen İsrail saldırılarına tepki olarak hacklemiştir. Hatta ekip saldırılarının başka bir sebebi olarak şunu ekledi: "Birleşmiş Milletler, Afrikalı insanların ölümlerini izliyor". Ayyıldız grubu web-sitelerinde, savunmalarına iki tane daha sorunu faaliyet alanı olarak gördüklerini belirtmiştir. Bunlardan biri Ermeni soykırımının kabul edilmesi ve ikincisi Kürt TV kanalı Roj TV'deki Türkiye aleyhtarı yayınlarının Danimarka'da desteklenmesi.

Grubun diğer bir saldırısı ise Almanya'ya olmuştur. Bu saldırıların sebebi Almanya'da yaşayan Türklere gösterilen ırkçı tutumdur. Benzer şekilde Avusturya hükümetinin 500 sitesine Türk elçiliğine yapılan saldırı nedeniyle ve Avusturya polisinin tutumu ile PKK'ya verilen desteğinin sonucu olarak hacklenmiştir. Grup bu faaliyetleri Viyana Kuşatması olarak adlandırır.

Bulgar web-siteleri Osmanlı anıtlarını yok etmeleri ve Türk karşıtı ırkçı ATAKA Partisi'nin ayrımcı politikaları, Bulgar ve Balkan Türkleri üzerindeki baskılar, PKK desteği ve bir Türk balıkçının bir Bulgar sahil görevlisi tarafından öldürülmesinin nedeni ile hacklenmiştir.

Grup, Suudi Arabistan gibi bir İslam ülkesine de müdahale etmiştir. Suudi hükümet ve üniversite siteleri hacklenir. Suudi Arabistan, Amerikan emperyalizmi ile ortak hareket etmek ile suçlanır, kar amacıyla Hristiyanlara İslam topraklarını yönetmek için izin vermek ve bir Türk genci olan Sabri BOGDAY hakkında ölüm cezasının onaylanması grubun tepkisine neden olmuştur.

En ağır saldırı ise Yunanistan'a karşıdır. Ayyıldız ekibi sitelerinde bu ülkeyi bir numaralı hedef ilan etmiştir. Yunanistan'ın PKK terörist kamplarına desteği, Makedonya'da yaşayan Türklere baskı uygulanması, Yunan sahil görevlisinin Türk bir balıkçıyı yakması, Yunanistan'ın Kıbrıs politikasının Yunanistan'ın Ermeni soykırımının ispatlanmasını desteklemesi ve tarih boyunca Türklere karşı süren düşmanlık nedenler arasındadır. Ayyıldız Grubu, Yunan Parlamentosu, medya organizasyonları ve hükümet sitelerine saldırmıştır. Grup ayrıca Türk hükümeti

sitesinde sızarak casusluk yapan Yunan siber terörist gruplarını da ihbar etti. Bu hareket tarzı Ayyıldız Grubu gibi Türk hacker ekiplerinin aktivist söylemci faaliyetlerinin protestocu ve korumacı olduğunu ve terörist olmadığını gösterir.

Örneğin, Ayyıldız ekibinin evrensel temalar üzerindeki faaliyetleri kendini gösteriyor ki İsrail hükümeti sitelerine saldırdıklarında onları "uluslararası hukukun daimi ihlali ve ABD'nin Orta Doğu'daki görünen yüzüne karşı hareketlerdir"(Ayyıldız Ekibi web-sitesi). Grup bu saldırıyı başka hacker grupları alt kademesinde bir ordu gibi kullanarak düzenlemiştir. Grup 1920'lerdeki Kurtuluş Savaşı'nı andıran bir organizasyon şeması ile rütbe vererek hackerleri kumanda etmiştir. Bu katmanlı hackleme faaliyetleri Türkiye karşıtı söylemi olan MSN İtalya ve İtalyan Hava Kuvvetleri web-sitelerine karşı kullanılmıştır. Ayyıldız Grubu İtalya saldırılarının nedeni olarak bu ülkenin PKK desteğini ve Türkiye'nin AB üyeliğine engel olmasını gösterir.

c. Grubun Söylemi ve Mesajı

Bu saldırılarda söylemlerinin farklı katmanları vardır;

1. Bu saldırılar söylemsel bir karşı eylem tarafından tetiklenmiştir. Türklüğü ya da İslam gururunu incitecek ve bu faaliyetlerin olduğu ülkelerin devletleri gerekli tedbirleri almadığı zaman grup müdahale etmiştir. Danimarka'daki karikatür olayı ve İsrail-Lübnan krizi buna örnektir.

2. Saldırılar aktif olarak PKK faaliyetleri ve Ermeni Soykırımı iddiaları karşısında tavır almayan ülkelere karşı da uygulanmaktadır.

3. Saldırıyı yapanlar, saldırıları tanımlamak üzere Osmanlı askeriyesinde olduğu üzere kuşatmaya dair terimlerden oluşan, Avrupa'nın ortaçağ kalelerinin kuşatılmasını anımsatan bir dil kullanır. Yahut tekzip, düzeltme, kelimesi örneğin soykırım gibi suçlamaların yanlış olduğunu göstermek, doğru yorumu ortaya koymak için kullanılır.

4. Grup saldırılarının geçici ve zarar vermeyen söylemsel eylemler olduğunu özellikle vurgular. Bu faaliyetlerin terörist saldırılar olmadıkları maddi ya da başka türde hiçbir kayıp oluşturmadıklarını belirtirler. Ayrıca, Ayyıldız Ekibi, çocuk pornosu gibi illegal eylemleri engellemekle övünmektedir.

d. Grubun Etkileri

Ayyıldız Ekibi' nin batı devletine ve özel kurum sitelerine saldırılarından sonra, kurumsal ve kişisel olarak gelen cevaplar saldıranları genellikle "İslami Terörist Saldırı" ya da "Türk teröristleri devlet sitesine saldırdı" şeklinde yansıttılar (Borst 2008: 130). Bu hack eylemleri otuz dakika civarı sürdü ve eylemciler 'Trojan' ya-

hut "Logic Bomb" yüklemediler ama web sitelerinin IP'lerini kontrol ettiler. Web adminleri IP'yi değiştirdi ve ardından orijinal sayfalar geri yüklendi. Finansal ya da maddi kayıp meydana gelmedi. Şok ve sitelerin kullanıcılarıyla sahiplerinden gelen erişememeye dair tepkiler ise geçiciydi. Öte yandan ise, hackerlerin amacı olabilecek en geniş kitleye ulaşmak ve hedef kitleye Türklük ve İslam konusundaki cehaletleri konusunda bir ders verebilmektir. Herhangi bir zarar verilmemiş ve evrensel kardeşlik mesajı verilmiştir.

SONUÇ

Türk Siber Hack Grupları için, siber terörün tanımı geçerli değildir. Yeni çeşit bir siber eylem tanımı yerine aktivist söylemsel hackleme tanımlaması, bu saldırıların kaygılarını belirtmesi açısından daha doğru bir tanım olacaktır.

Son Not:

Doç. Dr. Murat AKSER, Öğretim Üyesi, Kadir Has Üniversitesi, İletişim Fakültesi, Yeni Medya Bölümü Başkanı.

KAYNAKÇA

YONAH, A., SWETMAN, M. S. (2000) *Cyber Terrorism and Information Warfare: Threats and Responses*. Transnational Publishers.

AYYİLDİZ TEAM WEBSİTE. http://ayyildiz.org Borst, Stefan "Türken-Gang hackt die EU (Turkish network attacks European Union)" *Focus* 29, (2008): 130.

COLARIK, A. M. (2006), *Cyber Terrorism: Political and Economic Implications*. Idea Group, U.S.

Convention on Cybercrime, Budapest, 23.9.2001.

CULLAGH, D. (2002), *"House Considers Jailing Hackers For Life,"*

http://news.com.com/House+considers+jailing+hackers+for+l ife/2100- 1001_3-965750.html., November 14, 2002.

DENNING, D. E. (2000), *"Cyberterrorism,"* Testimony before the Special Oversight Panel on Terrorism Committee on Armed Services U.S. House of Representatives, May 23,.

GOLUBEV., V. (2004) *"Cyberterrorism: Concept, Terms, Counteraction,"* Computer Crime Research Center, August 3.

GOMEZ, J. (2003) *"Careful: Someone Is Watching You Surf,"* Bandwidth Magazine, November-December.

http://www.commsday.com.au/magazine/asian_century/nov_d ec2003_03.htm.

VERTON, D. (2003) *Black Ice: The Invisible Threat of Cyber-terrorism*. Osborne/McGraw-Hill, U.S.

WEIMANN, G. (2004) *"Cyberterrorism: How Real Is the Threat?"* Special Report No.119, United States Institute of Peace, December.

WEİMANN, G. *Terror on the Internet: The New Arena, the New Challenges*. United States Institute of Peace, U.S.